

Teoria dos Números:
um passeio com primos e outros números
familiares pelo mundo inteiro

Fabio E. Brochero Martinez
Carlos Gustavo T. de A. Moreira
Nicolau C. Saldanha
Eduardo Tengan

<http://livrariavirtualimpa.br>

Prefácio

O tema deste livro é a chamada *Teoria dos Números*, que é a parte da Matemática que se dedica ao estudo dos números inteiros e seus amigos. Não há dúvidas de que o conceito de inteiro é um dos mais antigos e fundamentais da ciência em geral, tendo acompanhado o homem desde os primórdios de sua história. Assim, é de certa forma surpreendente que a Teoria dos Números seja atualmente uma das áreas de pesquisa mais efervescentes da Matemática e que, mais do que nunca, continue a fascinar e desafiar as atuais gerações de matemáticos.

Diferentemente de muitas outras áreas da Matemática, a Teoria dos Números se distingue muito menos por seus métodos mas mais sim por seus problemas, cujo tema comum subjacente é o de número inteiro. Assim, por exemplo, enquanto um analista utiliza-se de métodos analíticos para resolver seus problemas e um algebrista empregue métodos algébricos para atacar questões algébricas, em Teoria dos Números um mesmo problema pode requerer para a sua solução a utilização simultânea de métodos algébricos, analíticos, topológicos, geométricos e combinatórios, além de uma boa dose de imaginação! Talvez seja este aspecto multidisciplinar, aliado à simplicidade de seus conceitos e ao seu caráter fundamental, que torna a Teoria dos Números um dos ramos mais populares em toda a Matemática, cativando pessoas de formação totalmente diversas. Em particular, os quatro autores são matemáticos de áreas diferentes umas das outras e nenhum deles é propriamente um especialista em teoria dos números.

A escolha dos temas abordados neste livro pretende justamente ilustrar esta personalidade múltipla da Teoria dos Números. Assim, o leitor encontrará aqui, além dos tópicos já consagrados como próprios da Teoria dos Números, tais como divisibilidade, congruências, primos, raízes primitivas e reciprocidade quadrática, diversos outros na interface com

PREFÁCIO

outras disciplinas como Análise, Álgebra e até mesmo Computação: por exemplo, estudamos entre outros o comportamento assintótico de funções aritméticas, a aritmética do anel de inteiros algébricos bem como alguns dos testes de primalidade mais eficientes atualmente conhecidos.

A grande maioria dos resultados são clássicos (= vistos em classe) e nossa única contribuição original (além dos erros) é quanto à sua apresentação. Naturalmente a escolha de quais temas foram abordados e quais foram deixados de fora é mais um reflexo do gosto e da experiência pessoal de nós autores do que uma meticulosamente calculada amostragem dos diversos aspectos da teoria. Ainda sim, acreditamos que cada um dos aspectos mais relevantes tenha sido coberto em pelo menos algum trecho do livro, de modo que o leitor não se sentirá frustrado, tenha ele inclinações mais para uma área do que outra!

Devo ler este livro?

Bem, naturalmente esta é um questão que só você pode responder! Mas vejamos algumas das “iguarias” que você estará perdendo se decidir que não:

1. os teoremas caracterizando quais naturais são respectivamente somas de dois, três e quatro quadrados perfeitos (capítulo 4);
2. duas demonstrações da famosa lei de reciprocidade quadrática, um dos resultados favoritos de Gauß (capítulos 2 e 6);
3. o recentemente descoberto algoritmo AKS, que demonstrou que o problema de decidir se um número inteiro é ou não primo pode ser resolvido em tempo polinomial (capítulo 7);
4. o teorema de Lucas-Lehmer, que fornece uma condição necessária e suficiente para que um número da forma $2^p - 1$ seja primo, e cujo algoritmo correspondente é responsável pelos maiores primos explicitamente conhecidos atualmente (capítulo 7);
5. a utilização de frações contínuas para a obtenção das melhores aproximações racionais de números reais e os teoremas de Khintchine, que quantificam estas melhores aproximações para quase todo número real (capítulos 3 e 8);
6. o teorema da fatoração única em ideais primos no anel de inteiros algébricos de uma extensão finita de \mathbb{Q} (capítulo 6);
7. uma introdução à teoria de curvas elípticas, que é um dos temas centrais na Teoria dos Números contemporânea (capítulo 9).

Este livro incorpora a maior parte de um livro anterior [105] sobre números primos escrito por dois dos autores para o Colóquio Brasileiro de Matemática de 1999.

Por falar em primos, incluímos o apêndice A, intitulado “O teorema dos números primos”, escrito por Jorge Aarão. Este apêndice é basicamente a sua dissertação de mestrado, apresentada em 1988 no IMPA, sob a orientação de José Felipe Voloch. Nele são provados o teorema dos números primos e o teorema dos números primos em progressões aritméticas (que implica o teorema de Dirichlet). Trata-se de uma das melhores referências que conhecemos sobre o assunto. Somos muito gratos ao Jorge por ter-nos permitido incluir esse texto em nosso livro.

Gostaríamos também de agradecer ao Nivaldo Nunes de Medeiros por suas ótimas sugestões de problemas.

Mas a quem exatamente se destina este livro? Na verdade, este livro foi escrito tendo em mente leitores com bagagens técnicas diversas e em diversos estágios de seu desenvolvimento matemático, seja o leitor aluno de graduação, pós-graduação, matemático profissional ou apenas um curioso aficionado em Matemática. Assim, a exposição não segue um tempo uniforme: ela pode variar desde um largo ou andante, nos capítulos iniciais, até um prestíssimo em certos trechos da segunda parte. Ainda sim, fizemos um genuíno esforço para manter a exposição o mais auto-contida possível, mesmo quando fazemos uso de ferramentas um pouco mais avançadas, que acreditamos porém acessíveis à maioria dos alunos de graduação em cursos de Ciências Exatas (por exemplo).

Para facilitar a adoção deste livro em cursos de graduação e pós-graduação, dividimos o livro em duas partes: “Fundamentos” e “Tópicos adicionais bacanas”. A primeira cobre o programa mais ou menos tradicional em cursos de Teoria Elementar dos Números, incluindo temas como divisibilidade, congruências, raízes primitivas, reciprocidade quadrática, equações diofantinas e frações contínuas. Na segunda parte, os capítulos são mais ou menos independentes entre si, e vários trechos podem ser utilizados em seminários, projetos de iniciação científica ou como tópicos especiais em cursos. Em todo caso, excetuando-se os dois primeiros capítulos, cujos resultados são utilizados constantemente ao longo de todo o texto, a leitura não precisa ser “linear”: o leitor é completamente livre para excursionar pelos diversos temas que o atraírem e apreciar a paisagem nesta, esperamos, agradável viagem.

Exemplos e Problemas Propostos

Exemplos e exercícios são uma parte importante no aprendizado de qualquer novo assunto e não poderia ser diferente neste livro. Mas, como mencionamos no início, isto é ainda mais verdade em Teoria dos Números, cujo pilar central unificador são exatamente os problemas. Há mais de 80 exemplos e 200 exercícios, de dificuldades as mais variadas, incluindo desde cálculos rotineiros até problemas desafiantes extraídos de diversas Olimpíadas de Matemática ao redor do mundo. Para estes, utilizamos as seguintes abreviações:

- AusPol: Olimpíada Austro-Polaca de Matemática
- IMO: International Mathematical Olympiad
- OBM: Olimpíada Brasileira de Matemática
- OIbM: Olimpíada Ibero-americana de Matemática

O número razoavelmente grande de problemas de olimpíadas neste livro está provavelmente relacionado ao fato de todos os autores serem ex-olímpicos. Exortamos veementemente o leitor a tentar resolver o maior número possível de problemas. Exercícios matemáticos são de certa forma como exercícios físicos: você não ficará em forma se só olhar outros fazendo... E além disso, problemas matemáticos são como esporte amador: você não tem nada a perder ao tentar, além de serem muito divertidos! Mas não se preocupe se não conseguir resolver alguns problemas deste livro: muitos deles são (ou foram) difíceis para nós também.

Confessamos que não resolvemos cada qual dos exercícios, assim pode haver pequenos erros na maneira em que eles são apresentados, e neste caso é parte do exercício obter uma formulação correta. Caso o leitor encare isto com um lapso da parte dos autores, queremos então lembrar os seguintes versos de Goethe:

“Irrtum verläßt uns nie, doch ziehet ein höher Bedürfnis
Immer den strebenden Geist leise zur Wahrheit hinan.”¹

¹Erros nunca nos abandonam, ainda sim uma necessidade maior empurra gentilmente nossos espíritos almejantes em direção da verdade.

Terminologia Frequente e Notações

Utilizamos a já consagrada notação \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} para denotar os conjuntos dos números naturais (incluindo o zero), inteiros, racionais, reais e complexos. Além disso, ao longo de todo o livro utilizaremos a seguinte terminologia:

1. CLARAMENTE: Nós não estamos com vontade de escrever todos os passos intermediários.
2. LEMBRE: Nós não deveríamos ter que dizer isto, mas...
3. SEM PERDA DE GENERALIDADE: Nós não faremos todos os casos, então vamos fazer só um e deixar você adivinhar o resto.
4. VERIFIQUE: Esta é a parte chata da prova, então você pode fazê-la na privacidade do seu lar, quando ninguém estiver olhando.
5. ESBOÇO DE PROVA: Estamos com muita preguiça de fazer os detalhes, então só listamos alguns passos que fazem parte do argumento.
6. DICA: A maneira mais difícil dentre as várias maneiras de se resolver um problema.
7. ANALOGAMENTE: Pelo menos uma linha da prova acima é igual à prova deste caso.
8. POR UM TEOREMA ANTERIOR: Nós não nos lembramos de como era o enunciado (na verdade, não temos certeza se provamos isto ou não), mas se o enunciado está correto, o resto da prova segue.
9. PROVA OMITIDA: Acredite, é verdade.

Julho de 2010

Fabio, Gugu, Nicolau e ET

“Young men should prove theorems, old men should write books.”

G. H. Hardy

“To get a book from these texts, only scissors and glue were needed.”

J.-P. Serre

(comentário ao receber o prêmio Steele por seu livro
“Cours d’Arithmétique”)

Prefácio da segunda edição

Ficamos muito felizes com a boa recepção que nosso livro encontrou. Aproveitamos a ocasião desta reimpressão para corrigir alguns pequenos erros, vários deles apontados por leitores. Em particular, reescrevemos a seção dedicada ao algoritmo de Agrawal-Kayal-Saxena para testar a primalidade de um inteiro, atualizamos a lista de primos, incluímos uma breve discussão sobre a relação entre frações contínuas e a dinâmica da transformação de Gauss e adicionamos algumas figuras para facilitar a compreensão do texto. Além disso, o índice remissivo foi revisado e ampliado.

Outubro de 2011

Fabio, Gugu, Nicolau e ET

Prefácio da terceira edição

Novamente aproveitamos a ocasião da reimpressão para corrigir alguns pequenos erros e atualizar tabelas de primos. Entre outras mudanças, incluímos discussões sobre equações diofantinas lineares, sobre a conjectura de Artin e sobre a solução negativa do décimo problema de Hilbert, que mostra que não há um algoritmo geral que resolva qualquer equação diofantina polinomial. A prova do Lema de Hensel foi trocada por uma ligeiramente mais elementar; foi adicionada uma prova trigonométrica da lei de reciprocidade quadrática; na seção sobre a equação de Pell alguns enunciados e demonstrações foram reformulados, e finalmente o capítulo sobre inteiros algébricos foi revisto - aproveitamos em particular para incluir o célebre teorema de Pólya-Vinogradov.

Maior de 2013

Fabio, Gugu, Nicolau e ET

Conteúdo

I	Fundamentos	1
0	Princípios	3
0.1	Princípio da Indução Finita	3
0.2	Princípio da Casa dos Pombos	10
1	Divisibilidade e Congruências	15
1.1	Divisibilidade	15
1.2	mdc, mmc e Algoritmo de Euclides	18
1.3	O Teorema Fundamental da Aritmética	26
1.4	Congruências	34
1.5	Bases	38
1.6	O Anel de Inteiros Módulo n	41
1.7	A Função de Euler e o Teorema de Euler-Fermat	48
1.8	Polinômios	58
1.9	Ordem e Raízes Primitivas	68
2	Equações Módulo m	80
2.1	Equações Lineares Módulo m	80
2.2	Congruências de Grau 2	87
2.2.1	Resíduos Quadráticos e Símbolo de Legendre	88
2.2.2	Lei de Reciprocidade Quadrática	90
2.2.3	Uma demonstração trigonométrica	95
2.3	Congruências de Grau Superior	100
3	Frações Contínuas	108
3.1	Reduzidas e Boas Aproximações	119
3.2	Boas Aproximações são Reduzidas	121

3.3	Frações Contínuas Periódicas	125
3.4	Os Espectros de Markov e Lagrange	126
4	Equações Diofantinas	133
4.1	Ternas Pitagóricas	134
4.2	Equações Diofantinas Quadráticas e Somas de Quadrados	138
4.2.1	Somas de Dois Quadrados	142
4.2.2	Somas de Quatro Quadrados e o Problema de Waring	145
4.2.3	Somas de Três Quadrados	148
4.2.4	Teorema de Minkowski	152
4.3	Descenso Infinito de Fermat	155
4.3.1	Equação de Markov	158
4.3.2	Último Teorema de Fermat	159
4.4	Equação de Pell	166
4.4.1	Solução Inicial da Equação de Pell	173
4.4.2	A Equação $x^2 - Ay^2 = -1$	176
4.4.3	Soluções da Equação $x^2 - Ay^2 = c$	179
4.4.4	Soluções da Equação $mx^2 - ny^2 = \pm 1$	181
5	Funções Aritméticas	188
5.1	Funções Multiplicativas	188
5.2	Função de Möbius e Fórmula de Inversão	193
5.3	Algumas Estimativas sobre Primos	200
5.3.1	O Teorema de Chebyshev	200
5.3.2	O Postulado de Bertrand	204
5.3.3	Outras estimativas	206
5.4	A Função φ de Euler	212
5.5	A Função σ	217
5.6	Números Livres de Quadrados	219
5.7	As Funções ω e Ω	219
5.8	A Função Número de Divisores $d(n)$	221
5.9	A Função Número de Partições $p(n)$	225
5.10	A Função Custo Aritmético $\tau(n)$	231
II	Tópicos adicionais bacanas	238

6	Inteiros Algébricos	240
6.1	Inteiros de Gauß e Eisenstein	240
6.2	Extensões Quadráticas e Ciclotômicas	254
6.3	Alguns Resultados de Álgebra	263
6.3.1	Polinômios Simétricos	263
6.3.2	Extensões de Corpos e Números Algébricos	264
6.3.3	Imersões, Traço e Norma	269
6.4	Inteiros Algébricos	275
6.5	Ideais	283
6.5.1	Fatoração Única em Ideais Primos	292
6.6	Grupo de Classe e Unidades	296
7	Primos	308
7.1	Sobre a Distribuição dos Números Primos	308
7.1.1	O Teorema dos Números Primos	308
7.1.2	Primos Gêmeos e Primos de Sophie Germain	310
7.1.3	Outros Resultados e Conjeturas sobre Primos	319
7.2	Fórmulas para Primos	324
7.3	Testes de Primalidade	329
7.3.1	O teste probabilístico de Miller-Rabin	332
7.4	Testes determinísticos	336
7.4.1	Testes de Primalidade Baseados em Fatorações de $n - 1$	337
7.4.2	Teste de Agrawal, Kayal e Saxena	340
7.5	Primos de Mersenne	350
7.6	Sequências Recorrentes e Testes de Primalidade	355
7.7	Aspectos Computacionais	363
7.7.1	O Algoritmo de Multiplicação de Karatsuba	363
7.7.2	Multiplicação de Polinômios Usando FFT	364
7.7.3	Multiplicação de Inteiros Usando FFT	368
7.7.4	A Complexidade das Operações Aritméticas	372
7.8	Tabelas	374
8	Aproximações Diofantinas	382
8.1	Teoria Métrica das Aproximações Diofantinas	382
8.2	Aproximações Não-Homogêneas	384
8.3	O Teorema de Khintchine	390
8.3.1	O Caso Unidimensional	390
8.3.2	O Teorema de Khintchine Multidimensional	394

8.4	Números de Liouville	399
9	Introdução às Curvas Elípticas	402
9.1	Curvas Elípticas como Curvas Projetivas	
	Planas	402
9.2	A Lei da Corda-Tangente	405
9.3	Curvas Elípticas como Rosquinhas	408
III	Apêndices	418
A	O Teorema dos Números Primos	
	(por Jorge Aarão)	420
A.1	Os Conceitos Básicos	422
	A.1.1 A Função Zeta de Riemann	422
	A.1.2 A Função $\psi(x)$	428
A.2	Teoremas Tauberianos e o Teorema dos Números Primos .	431
	A.2.1 Teoremas Tauberianos	431
	A.2.2 O Teorema dos Números Primos	437
A.3	Caráteres de Grupos, L -Séries de Dirichlet e o Teorema em Progressões Aritméticas	437
	A.3.1 A Função $\psi(x; q, \ell)$	437
	A.3.2 Caráteres	439
	A.3.3 L -séries de Dirichlet	442
A.4	O Lema de Landau	448
A.5	Bibliografia	449
B	Sequências Recorrentes	451
B.1	Sequências Recorrentes Lineares	452
B.2	A Sequência de Fibonacci	454
B.3	A Recorrência $x_{n+1} = x_n^2 - 2$	456
B.4	Fórmulas Gerais para Recorrências Lineares	457
C	Qual o próximo destino?	473
C.1	Alguns comentários e sugestões	473
	C.1.1 Fundamentos	473
	C.1.2 Leis de Reciprocidade	474
	C.1.3 Inteiros p -ádicos	474
	C.1.4 Geometria Diofantina	476
C.2	Sugestões Bibliográficas	476

C.2.1	Textos Gerais	476
C.2.2	Textos sobre Teoria Analítica dos Números	476
C.2.3	Textos sobre Aproximações Diofantinas	477
C.2.4	Textos sobre Teoria Algébrica dos Números	477
C.2.5	Textos sobre Curvas Elípticas e Geometria Dio- fantina	478
Bibliografia		480
Índice Remissivo		492

Parte I

Fundamentos

Capítulo 0

Princípios

Neste capítulo preliminar veremos duas propriedades básicas dos números naturais, o *Princípio da Indução Finita* e o *Princípio da Casa dos Pombos*.

0.1 Princípio da Indução Finita

Seja $P(n)$ uma propriedade do número natural n , por exemplo:

- n pode ser fatorado em um produto de números primos;
- $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$;
- a equação $2x + 3y = n$ admite solução com x e y inteiros positivos.

Uma maneira de provar que $P(n)$ é verdadeira para todo natural $n \geq n_0$ é utilizar o chamado *Princípio da Indução Finita* (PIF), que é um dos axiomas que caracterizam o conjunto dos números naturais. O PIF consiste em verificar duas coisas:

1. (Base da Indução) $P(n_0)$ é verdadeira e
2. (Passo Indutivo) Se $P(n)$ é verdadeira para algum número natural $n \geq n_0$, então $P(n + 1)$ também é verdadeira.

Na base da indução, verificamos que a propriedade é válida para um valor inicial $n = n_0$. O passo indutivo consiste em mostrar como utilizar a validade da propriedade para um dado n (a chamada *hipótese de indução*) para provar a validade da mesma propriedade para o inteiro

seguinte $n + 1$. Uma vez verificados a base e o passo indutivo, temos uma “cadeia de implicações”

$$\begin{array}{l}
 P(n_0) \text{ é verdadeira (base)} \xRightarrow{\text{passo indutivo}} P(n_0 + 1) \text{ é verdadeira} \\
 \xRightarrow{\text{passo indutivo}} P(n_0 + 2) \text{ é verdadeira} \\
 \xRightarrow{\text{passo indutivo}} P(n_0 + 3) \text{ é verdadeira} \\
 \vdots
 \end{array}$$

de modo que $P(n)$ é verdadeira para todo natural $n \geq n_0$.

Vejamos alguns exemplos.

Exemplo 0.1. *Demonstrar que, para todo inteiro positivo n ,*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

SOLUÇÃO: Observemos que $1 = \frac{1 \cdot 2}{2}$ donde a igualdade vale para $n = 1$ (base da indução). Agora suponha que a igualdade valha para $n = k$ (hipótese de indução):

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Somando $k + 1$ a ambos lados da igualdade, obtemos

$$1 + 2 + \cdots + k + (k + 1) = \frac{k(k+1)}{2} + (k + 1) = \frac{(k+1)(k+2)}{2},$$

de modo que a igualdade também vale para $n = k + 1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$. \square

Exemplo 0.2. *Demonstrar que, para todo número natural n ,*

$$M_n = n(n^2 - 1)(3n + 2)$$

é múltiplo de 24.

SOLUÇÃO: Veja que se $n = 0$ então $M_0 = 0$, que é um múltiplo de 24 (base da indução).

Agora, suponhamos que para certo inteiro k o número M_k é divisível por 24 (hipótese de indução) e vamos mostrar que M_{k+1} também é divisível por 24 (passo indutivo). Calculamos primeiramente a diferença

$$\begin{aligned} M_{k+1} - M_k &= (k+1)((k+1)^2 - 1)(3(k+1) + 2) - k(k^2 - 1)(3k + 2) \\ &= k(k+1)[(k+2)(3k+5) - (k-1)(3k+2)] \\ &= 12k(k+1)^2. \end{aligned}$$

Um dos números naturais consecutivos k e $k+1$ é par donde $k(k+1)^2$ é sempre par e $12k(k+1)^2$ é divisível por 24. Por hipótese de indução, M_k é divisível por 24 e temos portanto que $M_{k+1} = M_k + 12k(k+1)^2$ também é divisível por 24, como se queria demonstrar. \square

Uma variante do PIF é a seguinte versão (às vezes apelidada de *princípio de indução forte* ou *princípio de indução completa*), em que se deve mostrar

1. (Base da Indução) $P(n_0)$ é verdadeira e
2. (Passo Indutivo) Se $P(k)$ é verdadeira para todo natural k tal que $n_0 \leq k \leq n$, então $P(n+1)$ também é verdadeira.

Exemplo 0.3. A sequência de Fibonacci F_n é a sequência definida recursivamente por

$$F_0 = 0, \quad F_1 = 1 \quad e \quad F_n = F_{n-1} + F_{n-2} \quad \text{para } n \geq 2.$$

Assim, seus primeiros termos são

$$F_0 = 0, \quad F_1 = 1, \quad F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \quad \dots$$

Mostre que

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

onde $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ são as raízes de $x^2 = x + 1$.

SOLUÇÃO: Temos que $F_0 = \frac{\alpha^0 - \beta^0}{\alpha - \beta} = 0$ e $F_1 = \frac{\alpha^1 - \beta^1}{\alpha - \beta} = 1$ (base de indução). Agora seja $n \geq 1$ e suponha que $F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$ para todo k com

$0 \leq k \leq n$ (hipótese de indução). Assim,

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &= \frac{\alpha^n - \beta^n}{\alpha - \beta} + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \\ &= \frac{(\alpha^n + \alpha^{n-1}) - (\beta^n + \beta^{n-1})}{\alpha - \beta} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \end{aligned}$$

pois $\alpha^2 = \alpha + 1 \implies \alpha^{n+1} = \alpha^n + \alpha^{n-1}$ e analogamente $\beta^{n+1} = \beta^n + \beta^{n-1}$.

Observe que, neste exemplo, como o passo indutivo utiliza os valores de dois termos anteriores da sequência de Fibonacci, a base requer verificar a fórmula para os dois termos iniciais F_0 e F_1 e não apenas para o primeiro termo. \square

Exemplo 0.4. *Demonstrar que, para quaisquer naturais $n \geq m$, o coeficiente binomial*

$$\binom{n}{m} \stackrel{\text{def}}{=} \frac{n!}{m!(n-m)!}$$

é inteiro.

SOLUÇÃO: Procederemos por indução sobre a soma $m+n$. Se $m+n = 0$ então $m = n = 0$ e $\binom{0}{0} = 1$ é inteiro (base de indução). Para o passo indutivo, observe primeiramente que para $0 < m < n$ temos a seguinte identidade de binomiais

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

que segue diretamente das definições:

$$\begin{aligned} \binom{n-1}{m} + \binom{n-1}{m-1} &= \frac{(n-1)!}{m!(n-m-1)!} + \frac{(n-1)!}{(m-1)!(n-m)!} \\ &= \frac{((n-m)+m)(n-1)!}{m!(n-m)!} = \binom{n}{m}. \end{aligned}$$

Agora suponhamos que $\binom{n}{m}$ é inteiro para $m+n \leq k$ (hipótese de indução). Note que podemos supor também que $0 < m < n$, já que se $m = n$ ou $m = 0$ temos $\binom{n}{m} = 1$ e o resultado vale trivialmente. Assim, se $m+n = k+1$, temos que $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$ é inteiro também pois cada somando da direita é inteiro pela hipótese de indução. \square

Um terceiro disfarce do PIF é o chamado *princípio da boa ordenação* (PBO) dos números naturais, que afirma que todo subconjunto A não vazio de \mathbb{N} tem um elemento mínimo. (Você sabe dizer por que o princípio da boa ordem não vale para o conjunto \mathbb{Z} de todos os inteiros?)

Vejamos a equivalência entre os dois princípios. Assuma primeiramente o PBO e seja $P(n)$ uma propriedade para a qual $P(0)$ é verdadeira e $P(n)$ verdadeira implica $P(n+1)$ verdadeira. Seja B o conjunto dos n tais que $P(n)$ é falsa; devemos mostrar que $B = \emptyset$. Suponha que não; pelo PBO o conjunto B possui um menor elemento b . Como $0 \notin B$ (pois $P(0)$ é verdadeira por hipótese) temos que $b \geq 1$ e assim $b-1 \in \mathbb{N}$ e pela minimalidade de b temos que $b-1 \notin B$, ou seja, $P(b-1)$ é verdadeira. Mas por hipótese temos então que $P(b)$ também é verdadeira, o que é um absurdo, logo $B = \emptyset$.

Assuma agora o PIF e seja $A \subset \mathbb{N}$ um subconjunto não vazio. Defina agora o conjunto $B = \{b \in \mathbb{N} \mid a \notin A \text{ para todo } a < b\}$. Trivialmente $0 \in B$. Afirmamos que existe $k \in B$ tal que $k+1 \notin B$ e nesse caso k será o menor elemento de A . De fato, se isto não acontecer, teremos que $0 \in B$ e $k \in B$ implica que $k+1 \in B$. Logo, pelo PIF, $B = \mathbb{N}$ e $A = \emptyset$, o que é absurdo.

Exemplo 0.5. *Demonstrar que toda função $f : \mathbb{N} \rightarrow \mathbb{N}$ monótona não-crescente (isto é, $n \leq m \implies f(n) \geq f(m)$) é constante a partir de um certo número natural.*

SOLUÇÃO: Seja $A \subset \mathbb{N}$ a imagem de f . Pelo PBO, tal conjunto possui elemento mínimo a_0 . Seja n_0 um natural tal que $f(n_0) = a_0$. Como a função é monótona não-crescente então para todo $n \geq n_0$ temos que $f(n) \leq f(n_0)$, mas pela definição de a_0 temos $f(n) \geq a_0$. Logo $f(n) = a_0$ para todo $n \geq n_0$, como queríamos demonstrar. \square

Observação 0.6. *Dado um conjunto S , uma relação \prec em S é chamada de ordem parcial em S se ela satisfaz os seguintes axiomas:*

1. (Reflexividade) $a \prec a$ para todo $a \in S$.
2. (Anti-simetria) se $a \prec b$ e $b \prec a$ então $a = b$.
3. (Transitividade) se $a \prec b$ e $b \prec c$ então $a \prec c$.

Dizemos que \prec é uma ordem total se, dados quaisquer $a, b \in S$, ou $a \prec b$ ou $b \prec a$. Uma ordem total \prec em S é uma boa ordem se todo subconjunto A de S possui um elemento mínimo, isto é, um elemento $a \in A$ tal que $a \prec b$ para todo $b \in A$. É possível demonstrar que para todo conjunto S podemos definir uma ordem total em S que é uma boa ordem. Este fato usa o axioma da escolha (e na verdade é equivalente a ele) e está fora do propósito deste livro. Veja por exemplo [134].

Problemas Propostos

0.1. *Demonstrar por indução que para $n \geq 1$ natural*

$$(a) \quad 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

$$(b) \quad 1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

$$(c) \quad (1^5 + 2^5 + \cdots + n^5) + (1^7 + 2^7 + \cdots + n^7) = 2(1 + 2 + \cdots + n)^4.$$

$$(d) \quad \sin x + \sin 2x + \cdots + \sin nx = \frac{\sin \frac{(n+1)x}{2} \cdot \sin \frac{nx}{2}}{\sin \frac{x}{2}}.$$

0.2. *Seja F_n o n -ésimo termo da sequência de Fibonacci. Demonstrar que para todo natural $n \geq 1$ temos*

$$(a) \quad F_1 + F_2 + \cdots + F_n = F_{n+2} - 1.$$

$$(b) \quad F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n.$$

$$(c) \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

$$(d) \quad \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \cdots = F_{n+1}, \text{ onde na soma interpretamos } \binom{m}{k} = 0 \text{ se } k > m.$$

0.3. *Demonstrar que*

$$(a) \quad n^3 - n \text{ é um múltiplo de 6 para todo natural } n.$$

$$(b) \quad 5^n - 1 \text{ é múltiplo de 24 para todo número natural } n \text{ par.}$$

$$(c) \quad 2^n + 1 \text{ é múltiplo de 3 para todo natural ímpar } n.$$

0.4. Definimos a sequência $\{a_n\}$ por $a_1 = 2$ e para $n \geq 2$ o termo a_n é o produto dos termos anteriores mais um. Mostre que

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = 1 - \frac{1}{a_1 a_2 \cdots a_n}.$$

0.5. Mostre que $7^{2n} - 48n - 1$ é divisível por 48^2 para todo valor n .

0.6. Mostre que para todo natural $n \geq 4$

(a) $2^n < n!$.

(b) $2n^3 > 3n^2 + 3n + 1$.

0.7. Dado um inteiro positivo n , definimos $T(n, 1) = n$ e, para todo $k \geq 1$, $T(n, k+1) = n^{T(n, k)}$. Prove que existe $c \in \mathbb{N}$ tal que, para todo $k \geq 1$, $T(2010, k) < T(2, k+c)$. Determine o menor inteiro positivo c com essa propriedade.

0.8. Mostre que para todo n e k inteiros positivos

$$\binom{n}{n} + \binom{n+1}{n} + \binom{n+2}{n} + \cdots + \binom{n+k}{n} = \binom{n+k+1}{n+1}.$$

0.9. Demonstre a fórmula do binômio de Newton para n natural:

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

0.10. Encontrar com demonstração uma expressão para o multinômio

$$(x_1 + x_2 + \cdots + x_k)^n$$

em termos dos coeficientes multinomiais

$$\binom{n}{i_1, \dots, i_k} \stackrel{\text{def}}{=} \frac{n!}{i_1! \cdots i_k!}$$

onde $i_1 + \cdots + i_k = n$.

0.11. Considere n retas em posição geral em um plano, isto é, sem que haja duas retas paralelas ou três retas concorrentes em um mesmo ponto.

(a) Determine em função de n o número de regiões em que as retas dividem o plano.

- (b) *Demonstre que é possível colorir essas regiões com duas cores sem que duas regiões vizinhas tenham a mesma cor (duas regiões são vizinhas se elas possuem um segmento de reta em comum).*

0.12. *Sejam x_1, \dots, x_n números reais positivos. Neste exercício vamos provar que*

$$\frac{x_1 + \dots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}.$$

Tal desigualdade é conhecida como desigualdade das médias aritmética e geométrica.

- (a) *Utilize o PIF para mostrar a desigualdade das médias para $n = 2^k$.*
- (b) *Sejam x_1, \dots, x_n reais positivos fixados e $A = \frac{x_1 + \dots + x_n}{n}$ a média aritmética destes números. Suponha que a desigualdade valha para $n+1$ números reais positivos quaisquer; aplicando-a para x_1, \dots, x_n, A , conclua que a desigualdade vale também para quaisquer n números reais positivos.*
- (c) *Combinando os itens anteriores, prove a desigualdade para todo n natural.*

0.13. *Demonstrar que para cada número natural n existe um número natural M satisfazendo simultaneamente as seguintes duas condições:*

- (i) *M possui n dígitos pertencentes ao conjunto $\{1, 2\}$.*
- (ii) *M é divisível por 2^n .*

0.14 (IMO1987). *Mostre que não existe uma função $f: \mathbb{N} \rightarrow \mathbb{N}$ tal que $f(f(n)) = n + 1987$ para todo $n \in \mathbb{N}$.*

0.2 Princípio da Casa dos Pombos

É intuitivamente claro que se colocamos $n + 1$ objetos em n gavetas então haverá ao menos uma gaveta com mais de um objeto. Isto é exatamente o que afirma o chamado *Princípio da Casa dos Pombos* (PCP) ou *Princípio das Gavetas de Dirichlet*: se temos $kn + 1$ pombos e n casinhas, então existirá uma casinha onde haverá pelo menos $k + 1$ pombos. De fato, se em todas as casas houvesse no máximo k pombos, então o número de pombos não poderia ultrapassar kn .

O PCP parece bastante inocente, mas tem muitas aplicações interessantes, especialmente em argumentos de *existência* em que não se determina o objeto procurado explicitamente. Como exemplos falam mais do que 10^3 palavras, vejamos alguns.

Exemplo 0.7. *Do conjunto $A = \{1, 2, \dots, 99, 100\}$, escolhemos ao acaso 51 números. Demonstrar que entre os números escolhidos sempre existem dois que são consecutivos.*

SOLUÇÃO: Para provar isto, primeiro escolhamos gavetas adequadas ao problema. Distribuímos os números de A em 50 “gavetas” assim construídas:

$$\{1, 2\} \quad \{3, 4\} \quad \{5, 6\} \quad \cdots \quad \{99, 100\}.$$

Como há 50 gavetas das quais retiramos 51 números, sempre existirá uma gaveta da qual escolhemos dois números e estes, graças à nossa construção, serão consecutivos. Podemos generalizar este resultado considerando os números $\{1, 2, \dots, 2n\}$ e escolhendo dentre eles $n + 1$ números ao acaso.

□

Exemplo 0.8. *Do conjunto $A = \{1, 2, \dots, 99, 100\}$, escolhemos ao acaso 55 números. Demonstrar que entre os números escolhidos sempre existem dois tais que sua diferença é 9.*

SOLUÇÃO: Como no exemplo anterior o problema é descobrir como formar as gavetas. Consideremos as gavetas numeradas $0, 1, 2, \dots, 8$, onde o número n é colocado na gaveta i se, e só se, o resto na divisão de n por 9 é i . Como escolhemos $55 = 9 \times 6 + 1$ números, pelo PCP existirá uma gaveta j na qual há 7 ou mais números escolhidos. Mas em cada gaveta há no máximo 12 números (por exemplo, o conjunto $\{1, 10, 19, 28, 37, 46, 55, 64, 73, 82, 91, 100\}$ possui exatamente 12 elementos). Segue, como no problema anterior, que existirão dois números que serão “consecutivos” em tal conjunto, isto é, dois números cuja diferença é 9.

□

Exemplo 0.9. *Demonstrar que qualquer conjunto de n inteiros possui um subconjunto não vazio cuja soma dos elementos é divisível por n .*

SOLUÇÃO: Sejam a_1, a_2, \dots, a_n os elementos do conjunto, e definamos as “somadas parciais” $s_j = a_1 + \dots + a_j$ para $j = 1, \dots, n$. Se algum dos s_j é divisível por n o problema fica resolvido. Se nenhum é divisível por n , então os possíveis restos na divisão por n são $1, 2, \dots, n-1$ e como há n somadas parciais pelo PCP existem duas s_j e s_k com $j < k$ que deixam o mesmo. Portanto $s_k - s_j = a_{j+1} + \dots + a_k$ é divisível por n e $\{a_{j+1}, a_{j+2}, \dots, a_k\}$ é o subconjunto procurado.

Por outro lado, observemos que n é a quantidade mínima de elementos para que se verifique tal condição, no sentido em que existem conjuntos A com $n-1$ elementos tais que a soma dos elementos de todo subconjunto não vazio de A não é divisível por n . Por exemplo, $A = \{1, n+1, 2n+1, \dots, (n-2)n+1\}$ é um destes conjuntos (verifique!).

□

Exemplo 0.10. *Seja α um número real. Demonstrar que, para todo inteiro $n \geq 2$, existe um inteiro $0 < k < n$ tal que o módulo da diferença entre $k\alpha$ e seu inteiro mais próximo é menor ou igual a $\frac{1}{n}$.*

SOLUÇÃO: Vamos denotar por $\{x\}$ a *parte fracionária* do número real x , isto é, o único real que satisfaz $0 \leq \{x\} < 1$ e $x = m + \{x\}$ para algum $m \in \mathbb{Z}$.

Considere $\{k\alpha\}$ para $k = 1, 2, \dots, n-1$. Particione o intervalo $[0, 1)$ em n partes de tamanho $\frac{1}{n}$:

$$[0, 1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \left[\frac{2}{n}, \frac{3}{n}\right) \cup \dots \cup \left[\frac{n-1}{n}, 1\right)$$

Se $\{k\alpha\} \in [0, \frac{1}{n})$ ou $\{k\alpha\} \in [\frac{n-1}{n}, 1)$ para algum $k = 1, \dots, n-1$, o problema acabou. Caso contrário, pelo PCP haverá duas partes fracionárias $\{j\alpha\}$ e $\{k\alpha\}$ com $1 \leq j < k \leq n-1$ pertencentes a um mesmo intervalinho dentre os $n-2$ restantes. Sendo $x = (k-j)\alpha$, teremos

$$\{x\} = \begin{cases} \{k\alpha\} - \{j\alpha\} & \text{se } \{k\alpha\} \geq \{j\alpha\} \\ 1 + \{k\alpha\} - \{j\alpha\} & \text{se } \{k\alpha\} < \{j\alpha\} \end{cases}$$

e portanto $\{x\} \in [0, \frac{1}{n})$ ou $\{x\} \in [\frac{n-1}{n}, 1)$, assim $k-j$ satisfaz as condições do problema.

□

Problemas Propostos

0.15. *Escolhem-se 7 pontos no interior de um retângulo de dimensões 2×3 . Demonstrar que sempre é possível encontrar dois pontos tal que sua distância é menor ou igual a $\sqrt{2}$.*

0.16. *Escolhem-se 9 pontos no interior de um quadrado de lado 1. Demonstrar que é possível escolher 3 deles de tal forma que a área do triângulo que formam é menor ou igual a $\frac{1}{8}$.*

0.17. *Dadas 6 pessoas numa festa, demonstrar que necessariamente existem 3 pessoas que se conhecem mutuamente ou 3 pessoas que não se conhecem mutuamente. Suponha que a relação de conhecer é simétrica. Este é um caso particular do teorema de Ramsey, veja por exemplo [106].*

0.18. *Do conjunto $A = \{1, 2, \dots, 99, 100\}$ escolhemos 51 números. Demonstrar que, entre os 51 números escolhidos, existem dois tais que um é múltiplo do outro.*

0.19. *Dado um número irracional u , demonstrar que sempre é possível encontrar infinitos números racionais $\frac{p}{q}$, $p, q \in \mathbb{Z}$, de tal forma que*

$$\left| u - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Um problema mais difícil é demonstrar existem racionais $\frac{p}{q}$ de tal forma que

$$\left| u - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

Veja o teorema 3.13 e a seção correspondente para este e outros resultados relacionados à aproximação de números reais por números racionais.

0.20 (IMO1985). *Dado um conjunto M com 1985 inteiros positivos distintos, nenhum dos quais tem divisores primos maiores do que 23, mostre que há 4 elementos em M cujo produto é uma quarta potência.*

0.21 (OIbM1998). *Determinar o mínimo valor de n para o qual, de todo subconjunto de $\{1, 2, \dots, 999\}$ com n elementos, é possível selecionar quatro inteiros diferentes a, b, c, d tais que $a + 2b + 3c = d$.*

0.22. *Demonstrar que de qualquer conjunto de $2^{n+1} - 1$ números inteiros positivos é possível escolher 2^n elementos de tal forma que sua soma é divisível por 2^n .*

0.23 (IMO2001). *Sejam n_1, n_2, \dots, n_m inteiros com m ímpar. Denotemos por $x = (x_1, \dots, x_m)$ uma permutação dos inteiros $1, 2, \dots, m$, e definamos $f(x) = x_1 n_1 + \dots + x_m n_m$. Demonstre que existem duas permutações a e b tais que $f(a) - f(b)$ é divisível por $m!$.*

0.24. *Demonstrar que dados 7 números reais sempre é possível escolher 2 deles, digamos a e b , tais que*

$$\left| \frac{a-b}{1+ab} \right| < \frac{1}{\sqrt{3}}.$$

0.25 (IMO1991). *Seja $S = \{1, 2, \dots, 280\}$. Encontrar o menor inteiro n para o qual todo subconjunto de S com n elementos contém cinco números que são dois a dois primos entre si.*

0.26 (Erdős). *Mostrar que toda a sequência com $n^2 + 1$ números reais contém ou uma subsequência crescente com $n + 1$ termos ou uma subsequência decrescente com $n + 1$ termos.*

0.27. *Pintamos todos os pontos do plano de azul, verde ou preto. Mostrar que existe no plano um retângulo cujos vértices têm todos a mesma cor.*

0.28. *Em um tabuleiro 9×9 são colocados todos os números de 1 até 81. Mostre que existe um k tal que o produto dos números na k -ésima linha é diferente ao produto dos números da k -ésima coluna.*

0.29 (XII Vingança Olímpica). *Seja n um número inteiro positivo. Uma família \mathcal{P} de intervalos $[i, j]$ com $0 \leq i < j \leq n$ e i, j inteiros é dita unida se, para quaisquer $I_1 = [i_1, j_1] \in \mathcal{P}$ e $I_2 = [i_2, j_2] \in \mathcal{P}$ tais que $I_1 \subset I_2$, então $i_1 = i_2$ ou $j_1 = j_2$. Determine o maior número possível de elementos de uma família unida.*

Capítulo 1

Divisibilidade e Congruências

Neste primeiro capítulo veremos os tópicos básicos de Teoria dos Números, como divisibilidade, congruências e aritmética módulo n .

1.1 Divisibilidade

Dados dois inteiros d e a , dizemos que d *divide* a ou que d é um *divisor* de a ou ainda que a é um *múltiplo* de d e escrevemos

$$d \mid a$$

se existir $q \in \mathbb{Z}$ com $a = qd$. Caso contrário, escrevemos $d \nmid a$. Por exemplo, temos que $-5 \mid 10$ mas $10 \nmid -5$.

Eis algumas propriedades importantes da divisibilidade:

Lema 1.1. *Sejam $a, b, c, d \in \mathbb{Z}$. Temos*

- (i) (“ d divide”) *Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.*
- (ii) (Limitação) *Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.*
- (iii) (Transitividade) *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

DEMONSTRAÇÃO: Se $d \mid a$ e $d \mid b$, então podemos escrever $a = dq_1$ e $b = dq_2$ com $q_1, q_2 \in \mathbb{Z}$, logo $ax + by = d(q_1x + q_2y)$. Como $q_1x + q_2y \in \mathbb{Z}$,

temos $d \mid ax + by$. Para mostrar (ii), suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \geq 1$ e $|a| = |d||q| \geq |d|$. Finalmente, se $a \mid b$ e $b \mid c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto $a \mid c$. \square

Vejamos como utilizar estas propriedades para resolver alguns problemas de divisibilidade.

Exemplo 1.2. *Encontre todos os inteiros positivos n tais que $2n^2 + 1 \mid n^3 + 9n - 17$.*

SOLUÇÃO: Utilizando o “ $2n^2 + 1$ divide” para reduzir o grau de $n^3 + 9n - 17$, temos que

$$\begin{aligned} & \begin{cases} 2n^2 + 1 \mid n^3 + 9n - 17 \\ 2n^2 + 1 \mid 2n^2 + 1 \end{cases} \\ \implies & 2n^2 + 1 \mid (n^3 + 9n - 17) \cdot 2 + (2n^2 + 1) \cdot (-n) \\ \iff & 2n^2 + 1 \mid 17n - 34. \end{aligned}$$

Como o grau de $17n - 34$ é menor do que o de $2n^2 + 1$, podemos utilizar a “limitação” para obter uma lista finita de candidatos a n . Temos $17n - 34 = 0 \iff n = 2$ ou $|2n^2 + 1| \leq |17n - 34| \iff n = 1, 4$ ou 5 . Destes candidatos, apenas $n = 2$ e $n = 5$ são soluções. \square

Exemplo 1.3 (IMO1994). *Determine todos os pares (m, n) de inteiros positivos para os quais $\frac{n^3+1}{mn-1}$ é inteiro.*

SOLUÇÃO: Vamos tentar reduzir o grau em n utilizando o “ d divide”. Temos

$$\begin{aligned} mn - 1 \mid n^3 + 1 & \implies mn - 1 \mid (n^3 + 1) \cdot m - (mn - 1) \cdot n^2 \\ & \iff mn - 1 \mid n^2 + m. \end{aligned}$$

Da mesma forma,

$$\begin{aligned} mn - 1 \mid n^2 + m & \implies mn - 1 \mid (n^2 + m) \cdot m - (mn - 1) \cdot n \\ & \iff mn - 1 \mid m^2 + n \end{aligned}$$

e, finalmente,

$$\begin{aligned} mn - 1 \mid m^2 + n &\implies mn - 1 \mid (m^2 + n) \cdot m - (mn - 1) \\ &\iff mn - 1 \mid m^3 + 1 \end{aligned}$$

que é a mesma expressão com que começamos, trocando n por m . Assim, temos que a condição é simétrica em m e n e as divisibilidades acima são todas equivalentes entre si. Portanto podemos supor sem perda de generalidade que $m \geq n$. Utilizando a “limitação” temos

$$mn - 1 \mid n^2 + m \implies mn - 1 \leq n^2 + m \iff m(n - 1) \leq n^2 + 1.$$

Se $n \neq 1$ temos $m \leq \frac{n^2+1}{n-1} = n + 1 + \frac{2}{n-1}$. Como estamos assumindo $m \geq n$, se $n \geq 4$ temos apenas duas possibilidades: $m = n$ ou $m = n + 1$. Agora temos alguns casos a analisar.

- Se $m \geq n = 1$ devemos ter $m - 1 \mid 1^2 + m \implies m - 1 \mid m + 1 - (m - 1) \iff m - 1 \mid 2$ e portanto $m = 2$ ou $m = 3$, ambos os casos fornecendo soluções.
- Se $m \geq n = 2$ devemos ter $2m - 1 \mid 2^2 + m \implies 2m - 1 \mid 2(m + 4) - (2m - 1) \iff 2m - 1 \mid 9 \iff m = 2$ ou $m = 5$, ambos os casos fornecendo soluções.
- Se $m \geq n = 3$ devemos ter $3m - 1 \mid 3^2 + m \implies 3m - 1 \mid 3(m + 9) - (3m - 1) \iff 3m - 1 \mid 28 \iff m = 5$, que fornece uma solução.
- Se $m = n \geq 4$ devemos ter

$$\begin{aligned} n^2 - 1 \mid n^2 + n &\iff n - 1 \mid n \\ &\implies n - 1 \mid n - (n - 1) \iff n - 1 \mid 1 \end{aligned}$$

o que não é possível pois $n \geq 4$.

- Se $m = n + 1 \geq 5$ devemos ter

$$\begin{aligned} (n + 1)n - 1 \mid n^2 + (n + 1) \\ \iff n^2 + n - 1 \mid (n^2 + n + 1) - (n^2 + n - 1) \\ \iff n^2 + n - 1 \mid 2 \end{aligned}$$

o que novamente não é possível pois $n \geq 4$.

Logo as soluções (m, n) são $(1, 2)$, $(2, 1)$, $(1, 3)$, $(3, 1)$, $(2, 2)$, $(2, 5)$, $(5, 2)$, $(3, 5)$ e $(5, 3)$. \square

1.2 mdc, mmc e Algoritmo de Euclides

Dados dois números inteiros a e b com $a \neq 0$ ou $b \neq 0$, a cada um deles pode-se associar seu conjunto de divisores positivos, D_a e D_b respectivamente, e a intersecção de tais conjuntos $D_a \cap D_b$ é finita (pela “limitação”) e não vazia (já que 1 pertence à intersecção). Por ser finito, $D_a \cap D_b$ possui elemento máximo, que é chamado de *máximo divisor comum* (mdc) dos números a e b . Denotamos este número por $\text{mdc}(a, b)$ (alguns autores usam a notação (a, b)). Para $a = b = 0$ convencionamos $\text{mdc}(0, 0) = 0$. Quando $\text{mdc}(a, b) = 1$ dizemos que a e b são *primos entre si*.

Por outro lado, se denotamos por M_n o conjunto dos múltiplos positivos de n , dados dois números inteiros a e b com $a \neq 0$ e $b \neq 0$, então a intersecção $M_a \cap M_b$ é não vazia (já que $|ab|$ está na intersecção). Como os naturais são bem ordenados, $M_a \cap M_b$ possui elemento mínimo. Tal número é chamado *mínimo múltiplo comum* (mmc) de a e b e o denotaremos por $\text{mmc}(a, b)$ (alguns autores escrevem $[a, b]$).

Para calcularmos o mdc e o mmc de maneira eficiente, vamos descrever o chamado *algoritmo de Euclides* ou *algoritmo das divisões sucessivas*. Primeiramente, vamos relembrar o conceito de *divisão euclidiana*, ou *divisão com resto*, que é uma das quatro operações que toda criança aprende na escola. Sua formulação precisa é: dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ com

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|.$$

Tais q e r estão unicamente determinados pelas duas condições acima (veja o argumento a seguir) e são chamados o *quociente* e *resto* da divisão de a por b . O resto r é também denotado por $a \bmod b$.

Para $x \in \mathbb{R}$, definimos o *piso* ou *parte inteira* $\lfloor x \rfloor$ de x como sendo o único $k \in \mathbb{Z}$ tal que $k \leq x < k + 1$; definimos o *teto* $\lceil x \rceil$ de x como o único $k \in \mathbb{Z}$ tal que $k - 1 < x \leq k$. Por exemplo, temos $\lfloor \sqrt{2} \rfloor = 1$, $\lceil \sqrt{2} \rceil = 2$, $\lfloor 10 \rfloor = \lceil 10 \rceil = 10$, $\lfloor -\pi \rfloor = -4$ e $\lceil -\pi \rceil = -3$. Podemos agora mostrar a existência de q e r satisfazendo as duas condições acima: basta tomar

$$q = \begin{cases} \lfloor a/b \rfloor & \text{se } b > 0 \\ \lceil a/b \rceil & \text{se } b < 0 \end{cases} \quad \text{e} \quad r = a - bq \quad \text{em ambos os casos}$$

e é fácil verificar que $0 \leq r < |b|$ a partir das definições das funções piso e teto. Por outro lado, se $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \leq r_1, r_2 < |b|$,

então temos que $r_2 - r_1 = b(q_1 - q_2)$ é um múltiplo de b com $|r_2 - r_1| < |b|$, portanto $r_2 - r_1 = 0$ e assim $q_1 = q_2$ também, o que prova a unicidade.

Podemos agora descrever o *algoritmo de Euclides* para calcular o mdc, que se baseia na seguinte simples observação:

Lema 1.4 (Euclides). *Se $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.*

DEMONSTRAÇÃO: Basta mostrar que $D_a \cap D_b = D_b \cap D_r$, já que se estes conjuntos forem iguais em particular os seus máximos também serão iguais. Se $d \in D_a \cap D_b$ temos $d \mid a$ e $d \mid b$, logo $d \mid a - bq \iff d \mid r$ e portanto $d \in D_b \cap D_r$. Da mesma forma, se $d \in D_b \cap D_r$ temos $d \mid b$ e $d \mid r$, logo $d \mid bq + r \iff d \mid a$ e assim $d \in D_a \cap D_b$. \square

O algoritmo de Euclides consiste na aplicação reiterada do lema acima onde q e r são o quociente e o resto na divisão de a por b (note que o lema vale mesmo sem a condição $0 \leq r < |b|$). Como os restos formam uma sequência estritamente decrescente, o algoritmo eventualmente para quando atingimos o resto 0.

Exemplo 1.5. *Calcule $\text{mdc}(1001, 109)$.*

SOLUÇÃO: Realizando as divisões sucessivas, temos

$$1001 = 109 \cdot 9 + 20$$

$$109 = 20 \cdot 5 + 9$$

$$20 = 9 \cdot 2 + 2$$

$$9 = 2 \cdot 4 + 1$$

$$2 = 1 \cdot 2 + 0.$$

Assim, temos $\text{mdc}(1001, 109) = \text{mdc}(109, 20) = \text{mdc}(20, 9) = \text{mdc}(9, 2) = \text{mdc}(2, 1) = \text{mdc}(1, 0) = 1$. \square

Exemplo 1.6. *Sejam $m \neq n$ dois números naturais. Demonstrar que*

$$\text{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{se } a \text{ é par,} \\ 2 & \text{se } a \text{ é ímpar.} \end{cases}$$

SOLUÇÃO: Suponha sem perda de generalidade que $m > n$ e observe a fatoração

$$a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-2}} + 1)(a^{2^{m-3}} + 1) \dots (a^{2^n} + 1)(a^{2^n} - 1).$$

Logo $a^{2^m} + 1 = (a^{2^n} + 1) \cdot q + 2$ com $q \in \mathbb{Z}$ e assim

$$\text{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \text{mdc}(a^{2^n} + 1, 2)$$

que é igual a 2 se $a^{2^n} + 1$ for par, isto é, se a for ímpar, e é igual a 1 caso contrário. \square

Além de servir de ferramenta computacional para o cálculo do mdc, a divisão euclidiana tem consequências teóricas importantes. O próximo teorema mostra que é sempre possível escrever o mdc de dois números como combinação linear destes (com coeficientes inteiros).

Teorema 1.7 (Bachet-Bézout). *Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com*

$$ax + by = \text{mdc}(a, b).$$

Portanto se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid \text{mdc}(a, b)$.

DEMONSTRAÇÃO: O caso $a = b = 0$ é trivial (temos $x = y = 0$). Nos outros casos, considere o conjunto de todas as combinações \mathbb{Z} -lineares de a e b :

$$I(a, b) \stackrel{\text{def}}{=} \{ax + by : x, y \in \mathbb{Z}\}.$$

Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$ (há pelo menos um elemento positivo, verifique!). Afirmamos que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d , de modo que $m = dq + r$ e $0 \leq r < d$. Temos

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

Mas como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e portanto $d \mid m$.

Em particular, como $a, b \in I(a, b)$ temos que $d \mid a$ e $d \mid b$, logo $d \leq \text{mdc}(a, b)$. Note ainda que se $c \mid a$ e $c \mid b$, então $c \mid ax_0 + by_0 \iff c \mid d$. Tomando $c = \text{mdc}(a, b)$ temos que $\text{mdc}(a, b) \mid d$ o que, juntamente com a desigualdade $d \leq \text{mdc}(a, b)$, mostra que $d = \text{mdc}(a, b)$. \square

Corolário 1.8. *Sejam $a, b, c \in \mathbb{Z}$. A equação*

$$ax + by = c$$

admite solução inteira em x e y se, e somente se, $\text{mdc}(a, b) \mid c$.

DEMONSTRAÇÃO: Se a equação admite solução inteira, então $\text{mdc}(a, b)$ divide o lado esquerdo, logo deve dividir o direito também. Reciprocamente, se $\text{mdc}(a, b) \mid c$, digamos $c = k \cdot \text{mdc}(a, b)$ com $k \in \mathbb{Z}$, pelo teorema acima existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = \text{mdc}(a, b)$ e multiplicando tudo por k obtemos que $x = kx_0$ e $y = ky_0$ são soluções da equação dada. \square

Dados um inteiro $n > 2$ e inteiros a_1, a_2, \dots, a_n , não todos nulos, definimos recursivamente

$$\text{mdc}(a_1, a_2, \dots, a_n) = \text{mdc}(\text{mdc}(a_1, a_2, \dots, a_{n-1}), a_n).$$

É fácil mostrar por indução em n que este número é um divisor positivo comum de a_1, a_2, \dots, a_n . Também podemos provar por indução em n que existem inteiros x_1, x_2, \dots, x_n tais que $a_1x_1 + a_2x_2 + \dots + a_nx_n = \text{mdc}(a_1, a_2, \dots, a_n)$. De fato, pelo teorema anterior, existem u e v inteiros tais que $\text{mdc}(\text{mdc}(a_1, a_2, \dots, a_{n-1}), a_n) = \text{mdc}(a_1, a_2, \dots, a_{n-1})u + a_nv$, e, se existem inteiros y_1, y_2, \dots, y_{n-1} com $a_1y_1 + a_2y_2 + \dots + a_{n-1}y_{n-1} = \text{mdc}(a_1, a_2, \dots, a_{n-1})$, temos

$$\begin{aligned} \text{mdc}(a_1, a_2, \dots, a_n) &= \text{mdc}(\text{mdc}(a_1, a_2, \dots, a_{n-1}), a_n) = \\ &= \text{mdc}(a_1, a_2, \dots, a_{n-1})u + a_nv = a_1x_1 + a_2x_2 + \dots + a_nx_n, \end{aligned}$$

onde $x_j = y_ju$ para $1 \leq j \leq n-1$ e $x_n = v$. Em particular, se d é um divisor comum de a_1, a_2, \dots, a_n então $d \mid \text{mdc}(a_1, a_2, \dots, a_n)$.

O corolário anterior se generaliza então da seguinte forma: dado $c \in \mathbb{Z}$, a equação

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c$$

admite solução inteira em x_1, x_2, \dots, x_n se, e somente se, $\text{mdc}(a_1, a_2, \dots, a_n) \mid c$.

Temos uma outra importante consequência do teorema anterior:

Proposição 1.9. *Se $\text{mdc}(a, b) = 1$ e $a \mid bc$, então $a \mid c$.*

DEMONSTRAÇÃO: Como $\text{mdc}(a, b) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1 \implies a \cdot cx + (bc) \cdot y = c$. Do fato de a dividir cada termo do lado esquerdo, temos que $a \mid c$. \square

Lembramos que um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de p são 1 e p e um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e n . Observemos que 1 não é nem primo nem composto.

Claramente, se p é primo e $p \nmid a$ temos $\text{mdc}(p, a) = 1$. Usando a proposição anterior e indução temos o seguinte resultado:

Corolário 1.10. *Seja p um número primo e sejam $a_1, \dots, a_m \in \mathbb{Z}$. Se $p \mid a_1 \cdots a_m$, então $p \mid a_i$ para algum i , $1 \leq i \leq m$.*

O próximo lema resume algumas propriedades úteis do mdc:

Lema 1.11. *Temos*

1. *Se p é primo, então $\text{mdc}(a, p)$ é 1 ou p .*
2. *Se k é um inteiro, então $\text{mdc}(a, b) = \text{mdc}(a - kb, b)$.*
3. *Se $a \mid c$, então $\text{mdc}(a, b) \mid \text{mdc}(c, b)$.*
4. *Se $\text{mdc}(a, b) = 1$, então $\text{mdc}(ac, b) = \text{mdc}(c, b)$.*

DEMONSTRAÇÃO: O primeiro item é claro e o segundo é apenas uma reformulação do lema 1.4. Para provar o terceiro item, observe que $\text{mdc}(a, b) \mid a$ e $a \mid c$ implicam que $\text{mdc}(a, b) \mid c$. Como também temos $\text{mdc}(a, b) \mid b$, concluímos que $\text{mdc}(a, b) \mid \text{mdc}(b, c)$ por Bachet-Bézout. Finalmente, para mostrar o último item, note primeiro que $\text{mdc}(c, b) \mid \text{mdc}(ac, b)$ pois $\text{mdc}(c, b)$ divide simultaneamente ac e b . Reciprocamente, para mostrar que $\text{mdc}(ac, b) \mid \text{mdc}(c, b)$, podemos escrever $ax + by = 1$ com $x, y \in \mathbb{Z}$ por Bachet-Bézout. Assim, $\text{mdc}(ac, b)$ divide $ac \cdot x + b \cdot cy = c$ e também divide b , logo divide $\text{mdc}(c, b)$. \square

Vejamos como podemos usar as propriedades acima para solucionar o seguinte

Exemplo 1.12. *Sejam $a_n = 100 + n^2$ e $d_n = \text{mdc}(a_n, a_{n+1})$. Calcular d_n para todo n .*

SOLUÇÃO: Aplicando a propriedade 2 temos que

$$d_n = \text{mdc}(100 + n^2, 100 + (n + 1)^2) = \text{mdc}(100 + n^2, 2n + 1).$$

Como $2n + 1$ é ímpar, $\text{mdc}(4, 2n + 1) = 1$ e pelas propriedades 4 e 2 temos que

$$\begin{aligned} d_n &= \text{mdc}(400 + 4n^2, 2n + 1) \\ &= \text{mdc}(400 + 4n^2 - (2n + 1)(2n - 1), 2n + 1) \\ &= \text{mdc}(401, 2n + 1). \end{aligned}$$

Como 401 é primo, então $\text{mdc}(401, 2n + 1) = 401$ se $2n + 1 = 401k$ (com $k = 2r + 1$ inteiro ímpar) e $\text{mdc}(401, 2n + 1) = 1$ caso contrário, ou seja,

$$d_n = \begin{cases} 401 & \text{se } n = 401r + 200 \text{ com } r \in \mathbb{Z} \\ 1 & \text{caso contrário.} \end{cases}$$

□

A próxima proposição conecta o mdc e o mmc de dois inteiros e pode ser utilizada, juntamente com o algoritmo de Euclides, para o cálculo eficiente do mmc.

Proposição 1.13. *Sejam a e b dois números naturais, então*

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = a \cdot b.$$

DEMONSTRAÇÃO: Escreva $d = \text{mdc}(a, b)$ e $a = a_1d$ e $b = b_1d$ onde $a_1, b_1 \in \mathbb{Z}$ são tais que $\text{mdc}(a_1, b_1) = 1$. Temos $\text{mmc}(a, b) = al$ para algum $l \in \mathbb{Z}$; além disso, $b \mid \text{mmc}(a, b) \iff b_1d \mid a_1dl \iff b_1 \mid a_1l$. Como $\text{mdc}(a_1, b_1) = 1$, isto implica que $b_1 \mid l$ pela proposição 1.9. Pela definição de mínimo múltiplo comum, temos que l deve ser o mínimo número divisível por b_1 , assim concluímos que $l = b_1$ e portanto $\text{mmc}(a, b) = b_1a$. Logo $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = d \cdot b_1a = a \cdot b$. □

Dados um inteiro $n > 2$ e inteiros a_1, a_2, \dots, a_n , não todos nulos, definimos recursivamente

$$\text{mmc}(a_1, a_2, \dots, a_n) = \text{mmc}(\text{mmc}(a_1, a_2, \dots, a_{n-1}), a_n).$$

É fácil mostrar por indução em n que este número é um múltiplo positivo comum de a_1, a_2, \dots, a_n , e que, se m é um múltiplo comum de a_1, a_2, \dots, a_n , então $\text{mmc}(a_1, a_2, \dots, a_n) \mid m$.

A demonstração que demos do teorema de Bachet-Bézout não mostra como efetivamente encontrar uma solução de $ax + by = \text{mdc}(a, b)$. Porém, isto pode ser feito utilizando-se o algoritmo de Euclides, como mostra o exemplo a seguir. De fato, este exemplo pode servir como ponto de partida para uma segunda demonstração do teorema de Bachet-Bézout (veja os exercícios).

Exemplo 1.14. *Encontre todos os $x, y \in \mathbb{Z}$ tais que*

$$1001x + 109y = \text{mdc}(1001, 109).$$

SOLUÇÃO: Fazemos as divisões sucessivas para o cálculo de $\text{mdc}(1001, 109) = 1$ utilizando o algoritmo de Euclides (veja o exemplo 1.5). Em seguida, isolamos os restos:

$$\boxed{20} = \boxed{1001} - \boxed{109} \cdot 9$$

$$\boxed{9} = \boxed{109} - \boxed{20} \cdot 5$$

$$\boxed{2} = \boxed{20} - \boxed{9} \cdot 2$$

$$\boxed{1} = \boxed{9} - \boxed{2} \cdot 4$$

Note que a última divisão permite expressar o mdc 1 como combinação linear de 9 e 2:

$$\boxed{9} \cdot 1 - \boxed{2} \cdot 4 = 1.$$

Mas da penúltima divisão, temos que $\boxed{2} = \boxed{20} - \boxed{9} \cdot 2$, logo substituindo esta expressão na combinação linear acima, temos

$$\boxed{9} - (\boxed{20} - \boxed{9} \cdot 2) \cdot 4 = 1 \iff \boxed{9} \cdot 9 - \boxed{20} \cdot 4 = 1$$

e agora expressamos 1 como combinação linear de 20 e 9. Repetindo este procedimento, eventualmente expressaremos 1 como combinação linear

de 1001 e 109. Tomamos o cuidado de lembrar quais são os “coeficientes” a e b nas equações $ax + by = \text{mdc}(a, b)$ durante as simplificações. Continuando, obtemos

$$1 = (\boxed{109} - \boxed{20} \cdot 5) \cdot 9 - \boxed{20} \cdot 4 = \boxed{109} \cdot 9 - \boxed{20} \cdot 49$$

$$1 = \boxed{109} \cdot 9 - (\boxed{1001} - \boxed{109} \cdot 9) \cdot 49 = \boxed{1001} \cdot (-49) + \boxed{109} \cdot 450.$$

Logo uma solução da equação $1001x + 109y = 1$ é $(x_0, y_0) = (-49, 450)$. Para encontrar as demais, escrevemos o lado direito desta equação utilizando a solução particular que acabamos de encontrar:

$$1001x + 109y = 1001x_0 + 109y_0 \iff 1001(x - x_0) = -109(y - y_0).$$

Como $\text{mdc}(1001, 109) = 1$ temos pela proposição 1.9 que 1001 divide $y - y_0$, ou seja, $y - y_0 = 1001t$ para algum $t \in \mathbb{Z}$ e, portanto, $x - x_0 = -109t$. Assim, as soluções da equação dada são todos os pontos da reta $1001x + 109y = 1$ da forma

$$(x, y) = (x_0 - 109t, y_0 + 1001t) = (-49, 450) + (-109, 1001) \cdot t$$

com $t \in \mathbb{Z}$. □

Em geral, o raciocínio do exemplo acima mostra que se $\text{mdc}(a, b) = 1$ e (x_0, y_0) é uma solução da equação $ax + by = c$, então todas as soluções inteiras são dadas por $x = x_0 - bk$ e $y = y_0 + ak$ com $k \in \mathbb{Z}$.

Exemplo 1.15. *Sejam a, b inteiros positivos com $\text{mdc}(a, b) = 1$. Mostre que para todo $c \in \mathbb{Z}$ com $c > ab - a - b$, a equação $ax + by = c$ admite soluções inteiras com $x, y \geq 0$.*

SOLUÇÃO: Seja (x_0, y_0) uma solução inteira (que existe pelo teorema de Bachet-Bézout). Devemos mostrar a existência de um inteiro k tal que

$$x = x_0 - bk > -1 \quad \text{e} \quad y = y_0 + ak > -1,$$

ou seja,

$$-\frac{y_0 + 1}{a} < k < \frac{x_0 + 1}{b}.$$

Mas isto segue do fato de o intervalo $(-\frac{y_0+1}{a}, \frac{x_0+1}{b})$ ter tamanho maior do que 1:

$$\frac{x_0 + 1}{b} - \left(-\frac{y_0 + 1}{a}\right) = \frac{ax_0 + by_0 + a + b}{ab} = \frac{c + a + b}{ab} > 1.$$

□

1.3 O Teorema Fundamental da Aritmética

Estamos agora prontos para enunciar o teorema que caracteriza todo número natural em termos de seus “constituintes” primos.

Teorema 1.16 (Teorema Fundamental da Aritmética). *Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \dots \leq p_m$ são primos.

DEMONSTRAÇÃO: Mostramos a existência da fatoração de n em primos por indução. Se n é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n .

Vamos agora mostrar a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \dots \leq p_m$, $q_1 \leq \dots \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 \mid q_1 \cdots q_{m'}$ temos $p_1 \mid q_i$ para algum valor de i pelo corolário 1.10. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, pela minimalidade de n , donde $m = m'$ e $p_i = q_i$ para todo i , o que contradiz o fato de n ter duas fatorações. \square

Outra forma de escrever a fatoração acima é

$$n = p_1^{e_1} \cdots p_m^{e_m},$$

com $p_1 < \dots < p_m$ e $e_i > 0$. Ainda outra formulação é escrever

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \cdots p^{e_p} \cdots$$

onde o produto é tomado sobre *todos* os primos mas apenas um número finito de expoentes é maior do que zero. Vamos nos referir a qualquer destas expressões como a *fatoração canônica* de n em primos.

A fatoração única em primos se aplica em contextos mais gerais, como veremos mais tarde. Aqui, como aplicação imediata do Teorema Fundamental da Aritmética, vamos mostrar a prova atribuída a Euclides para a existência de infinitos primos (uma prova com mais de 2000 anos e que ainda funciona!).

Teorema 1.17 (Euclides). *Existem infinitos primos.*

DEMONSTRAÇÃO: Suponha por absurdo que p_1, p_2, \dots, p_m fossem *todos* os primos. O número $N = p_1 p_2 \dots p_m + 1 > 1$ não seria divisível por nenhum primo p_i , o que contradiz o Teorema Fundamental da Aritmética.

□

Observe que *não* provamos que $p_1 p_2 \dots p_m + 1$ é primo para algum conjunto finito de primos (por exemplo, os m primeiros primos). Aliás, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ não é primo. Não se conhece nenhuma fórmula simples que gere sempre números primos (veja a seção 7.2 para uma discussão sobre este assunto).

Embora a quantidade de primos seja infinita, uma questão natural é saber o quão “raros” ou “frequentemente” eles são. Na segunda parte do livro, discutiremos mais a fundo esta questão sobre a distribuição dos primos. Por outro lado, é interessante notar que existem cadeias arbitrariamente longas de números compostos consecutivos: na sequência

$$(k+1)! + 2, (k+1)! + 3, (k+1)! + 4, \dots, (k+1)! + (k+1),$$

nenhum termo é primo, pois eles admitem fatores próprios $2, 3, 4, \dots, k+1$, respectivamente.

Uma interessante prova alternativa, devida a Erdős, de que existem infinitos primos é a seguinte:

Suponha, por contradição, que existe um número finito de primos, digamos p_1, p_2, \dots, p_k . Seja n um número natural. Então podemos escrever qualquer número $m \leq n$ na forma $m = m_1^2 m_2$, onde $m_1^2 \leq n$ e

$$m_2 = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \quad \text{onde } a_k = 0 \text{ ou } 1 \text{ para cada } k.$$

Assim, considerando todas as possíveis maneiras de escrever os naturais $m \leq n$, temos: 2^k escolhas para m_2 e no máximo $\lfloor \sqrt{n} \rfloor$ escolhas para m_1 . Ou seja, para todo n natural, vale que

$$n \leq 2^k \sqrt{n}$$

absurdo, pois esta desigualdade não vale para n suficientemente grande. \square

Exemplo 1.18 (OIbM1987). *A sequência p_n é definida da seguinte forma:*

$$(i) \ p_1 = 2.$$

(ii) *Para todo $n \geq 2$, p_n é o maior divisor primo da expressão*

$$p_1 p_2 p_3 \cdots p_{n-1} + 1.$$

Demonstrar que p_n é diferente de 5.

SOLUÇÃO: Dado que $p_1 = 2$, $p_2 = 3$, $p_3 = 7$, segue-se que para qualquer $n \geq 3$, $p_1 p_2 \cdots p_{n-1}$ é múltiplo de 2 e de 3, portanto $p_1 p_2 \cdots p_{n-1} + 1$ não é múltiplo nem de 2 nem de 3. Além disso, como $p_1 = 2$, então p_n é ímpar para todo $n \geq 2$, assim $p_1 p_2 \cdots p_{n-1}$ não é múltiplo de 4.

Suponhamos que exista n tal que $p_n = 5$, isto é, o maior divisor primo de $p_1 p_2 \cdots p_{n-1} + 1$ é 5. Como 2 e 3 não dividem $p_1 p_2 \cdots p_{n-1} + 1$, temos que

$$p_1 p_2 \cdots p_{n-1} + 1 = 5^k.$$

Portanto

$$p_1 p_2 \cdots p_{n-1} = 5^k - 1 = (5 - 1)(5^{k-1} + 5^{k-2} + \cdots + 5 + 1),$$

donde $4 \mid p_1 p_2 \cdots p_{n-1}$, uma contradição. \square

Exemplo 1.19. *Determine todas as ternas (a, b, c) de inteiros positivos tais que $a^2 = 2^b + c^4$.*

SOLUÇÃO: Como $a^2 = 2^b + c^4 \iff (a - c^2)(a + c^2) = 2^b$, pelo Teorema Fundamental da Aritmética existem dois naturais $m > n$ tais que $m +$

$n = b$, $a - c^2 = 2^n$ e $a + c^2 = 2^m$. Subtraindo as duas últimas equações, obtemos que $2c^2 = 2^m - 2^n$, assim $c^2 = 2^{n-1}(2^{m-n} - 1)$. Como 2^{n-1} e $2^{m-n} - 1$ são primos entre si e o seu produto é um quadrado perfeito (i.e. os expoentes das potências de primos distintos são pares), novamente pelo Teorema Fundamental da Aritmética 2^{n-1} e $2^{m-n} - 1$ devem ser ambos quadrados perfeitos, logo $n - 1$ é par e $2^{m-n} - 1 = (2k - 1)^2$ para algum inteiro positivo k . Como $2^{m-n} = (2k - 1)^2 + 1 = 4k(k - 1) + 2$ é divisível por 2 mas não por 4, temos $m - n = 1$. Assim, fazendo $n - 1 = 2t$, temos que todas as soluções são da forma $(a, b, c) = (3 \cdot 2^{2t}, 4t + 3, 2^t)$ com $t \in \mathbb{N}$ e é fácil verificar que todos os números desta forma são soluções. \square

Segue do Teorema Fundamental da Aritmética que todo divisor de $n = p_1^{e_1} \dots p_m^{e_m}$ é da forma

$$p_1^{d_1} \dots p_m^{d_m}$$

com $0 \leq d_i \leq e_i$. Assim, obtemos o outro algoritmo usual para calcular o mdc de dois números: fatoramos os dois números em primos e tomamos os fatores comuns com os menores expoentes. Este algoritmo é bem menos eficiente do que o de Euclides para inteiros grandes (que em geral não sabemos fatorar de forma eficiente computacionalmente) mas é instrutivo saber que os dois algoritmos dão o mesmo resultado. Além disso, este algoritmo tem consequências teóricas importantes, como por exemplo o

Corolário 1.20. *Se $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$, então $\text{mdc}(ab, n) = 1$.*

DEMONSTRAÇÃO: Evidente a partir do algoritmo descrito acima. \square

Para encerrar esta seção, vejamos ainda algumas outras aplicações do Teorema Fundamental da Aritmética.

Proposição 1.21. *Seja $n = p_1^{e_1} \dots p_m^{e_m}$ a fatoração de n em potências de primos distintos p_i e seja $\sigma_k(n) \stackrel{\text{def}}{=} \sum_{d|n, d>0} d^k$ a soma das k -ésimas potências dos divisores positivos de n . Então*

$$\sigma_k(n) = \frac{p_1^{(e_1+1)k} - 1}{p_1^k - 1} \cdot \dots \cdot \frac{p_m^{(e_m+1)k} - 1}{p_m^k - 1}.$$

Para $k = 0$, a fórmula acima deve ser interpretada tomando-se o limite $k \rightarrow 0$, de modo que a quantidade de divisores positivos de n é $\sigma_0(n) = (e_1 + 1) \cdots (e_m + 1)$.

DEMONSTRAÇÃO: Como a soma na definição de $\sigma_k(n)$ percorre todos os números da forma $d^k = p_1^{d_1 k} \cdots p_m^{d_m k}$ com $0 \leq d_i \leq e_i$, temos a seguinte fatoração:

$$\sigma_k(n) = (1 + p_1^k + p_1^{2k} + \cdots + p_1^{e_1 k}) \cdots (1 + p_m^k + p_m^{2k} + \cdots + p_m^{e_m k}).$$

Somando as progressões geométricas $1 + p_i^k + p_i^{2k} + \cdots + p_i^{e_i k} = \frac{p_i^{(e_i+1)k} - 1}{p_i^k - 1}$, o resultado segue. \square

Proposição 1.22 (Fatores do Fatorial). *Seja p um primo. Então a maior potência de p que divide $n!$ é p^α onde*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Observe que a soma acima é finita pois os termos $\left\lfloor \frac{n}{p^i} \right\rfloor$ são eventualmente zero.

DEMONSTRAÇÃO: No produto $n! = 1 \cdot 2 \cdots n$, apenas os múltiplos de p contribuem com um fator p . Há $\left\lfloor \frac{n}{p} \right\rfloor$ tais múltiplos entre 1 e n . Destes, os que são múltiplos de p^2 contribuem com um fator p extra e há $\left\lfloor \frac{n}{p^2} \right\rfloor$ tais fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p e assim por diante, resultando na fórmula acima. \square

Exemplo 1.23. *Determine com quantos zeros termina $1000!$.*

SOLUÇÃO: O problema é equivalente a determinar qual a maior potência de 10 que divide $1000!$ e como há muito mais fatores 2 do que 5 em $1000!$, o expoente desta potência coincide com o da maior potência de 5 que divide $1000!$, ou seja,

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 249.$$

Assim, $1000!$ termina com 249 zeros. \square

Problemas Propostos

1.1 (IMO1959). *Mostre que a fração $\frac{21n+4}{14n+3}$ é irredutível para todo n natural.*

1.2. *Encontre todos os inteiros positivos tais que*

(a) $n + 1 \mid n^3 - 1$

(b) $2n - 1 \mid n^3 + 1$

(c) $\frac{1}{n} + \frac{1}{m} = \frac{1}{143}$

(d) $2n^3 + 5 \mid n^4 + n + 1$

1.3. *Demonstre:*

(a) *se $m \mid a - b$, então $m \mid a^k - b^k$ para todo natural k .*

(b) *se $f(x)$ é um polinômio com coeficientes inteiros e a e b são inteiros quaisquer, então $a - b \mid f(a) - f(b)$.*

(c) *se k é um natural ímpar, então $a + b \mid a^k + b^k$.*

1.4. *Mostre que*

(a) $2^{15} - 1$ e $2^{10} + 1$ *são primos entre si.*

(b) $2^{32} + 1$ e $2^4 + 1$ *são primos entre si.*

1.5. *Demonstrar que $(n - 1)^2 \mid n^k - 1$ se, e só se, $n - 1 \mid k$.*

1.6 (IMO1992). *Encontrar todos os inteiros a, b, c com $1 < a < b < c$ tais que $(a - 1)(b - 1)(c - 1)$ é divisor de $abc - 1$.*

Dica: Mostrar primeiro que $a \leq 4$ e considerar os possíveis casos.

1.7 (IMO1998). *Determine todos os pares de inteiros positivos (a, b) tais que $ab^2 + b + 7$ divide $a^2b + a + b$.*

Dica: Mostre que $ab^2 + b + 7 \mid 7a - b^2$ e considerar três casos: $7a - b^2$ maior, menor ou igual a zero.

1.8. *Mostre que, se $n > 1$, então*

$$\sum_{k=1}^n \frac{1}{k} = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

não é um número inteiro.

1.9 (OBM1997). *Sejam $c \in \mathbb{Q}$, $f(x) = x^2 + c$. Definimos*

$$f^0(x) = x, \quad f^{n+1}(x) = f(f^n(x)), \forall n \in \mathbb{N}.$$

Dizemos que $x \in \mathbb{R}$ é pré-periódico se $\{f^n(x), n \in \mathbb{N}\}$ é finito. Mostre que $\{x \in \mathbb{Q} \mid x \text{ é pré-periódico}\}$ é finito.

1.10. *Demonstrar que se $\text{mdc}(a, 2^{n+1}) = 2^n$ e $\text{mdc}(b, 2^{n+1}) = 2^n$, então $\text{mdc}(a + b, 2^{n+1}) = 2^{n+1}$.*

1.11. *Demonstrar que se a, b, c, d, m e n são inteiros tais que $ad - bc = 1$ e $mn \neq 0$, então*

$$\text{mdc}(am + bn, cm + dn) = \text{mdc}(m, n).$$

1.12. *Seja F_n o n -ésimo termo da sequência de Fibonacci.*

(a) *Encontrar dois números inteiros a e b tais que $233a + 144b = 1$ (observe que 233 e 144 são termos consecutivos da sequência de Fibonacci).*

(b) *Mostre que $\text{mdc}(F_n, F_{n+1}) = 1$ para todo $n \geq 0$.*

(c) *Determine x_n e y_n tais que $F_n \cdot x_n + F_{n+1} \cdot y_n = 1$.*

1.13. *Sejam a e b dois inteiros positivos e d seu máximo divisor comum. Demonstrar que existem dois inteiros positivos x e y tais que $ax - by = d$.*

1.14. *Definimos a sequência de frações de Farey de ordem n como o conjunto de frações reduzidas $\frac{a}{b}$ tais que $0 \leq \frac{a}{b} \leq 1$, $1 \leq b \leq n$. Por exemplo a sequência de Farey de ordem 3 é $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$.*

(a) *Demonstrar que se $\frac{a}{b}$ e $\frac{c}{d}$ são dois termos consecutivos de uma sequência de Farey, então $cb - ad = 1$.*

(b) *Demonstrar que se $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}$ são três termos consecutivos de uma sequência de Farey, então $\frac{a_2}{b_2} = \frac{a_1 + a_3}{b_1 + b_3}$.*

1.15. *Utilize indução em $\min\{a, b\}$ e o algoritmo de Euclides para mostrar que $ax + by = \text{mdc}(a, b)$ admite solução com $x, y \in \mathbb{Z}$, obtendo uma nova demonstração do teorema de Bachet-Bézout.*

1.16. *Sejam a e b números inteiros positivos. Considere o conjunto*

$$C = \{ax + by \mid x, y \in \mathbb{N}\}.$$

Lembre-se de que já mostramos no exemplo 1.15 que todo número maior que $ab - a - b$ pertence a C .

(a) *Demonstre que o número $ab - a - b$ não pertence a C .*

(b) *Achar a quantidade de números inteiros positivos que não pertencem a C .*

1.17 (IMO1984). *Dados os inteiros positivos a, b e c , dois a dois primos entre si, demonstrar que $2abc - ab - bc - ca$ é o maior número inteiro que não pode expressar-se na forma $xbc + yca + zab$ com x, y e z inteiros não negativos.*

1.18 (IMO1977). *Sejam a, b inteiros positivos. Quando dividimos $a^2 + b^2$ por $a + b$, o quociente é q e o resto é r . Encontrar todos os a, b tais que $q^2 + r = 1977$.*

1.19. *Demonstrar que $\text{mdc}(2^a - 1, 2^b - 1) = 2^{\text{mdc}(a, b)} - 1$ para todo $a, b \in \mathbb{N}$.*

1.20. *Encontrar todas as funções $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ satisfazendo simultaneamente as seguintes propriedades*

(i) $f(a, a) = a$.

(ii) $f(a, b) = f(b, a)$.

(iii) *Se $a > b$, então $f(a, b) = \frac{a}{a-b}f(a-b, b)$.*

1.21. *Mostre que se n é um número natural composto, então n é divisível por um primo p com $p \leq \lfloor \sqrt{n} \rfloor$.*

1.22 (IMO1989). *Prove que, para todo inteiro positivo n , existem n inteiros positivos consecutivos, nenhum dos quais é potência de primo.*

1.23 (Chi1998). *Encontrar todos os n para os quais $1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}$ divide 2^{2000} .*

1.24 (IMO2002). *Sejam $d_1 < d_2 < \dots < d_k$ os divisores positivos de um inteiro $n > 1$. Seja $d = d_1d_2 + d_2d_3 + \dots + d_{k-1}d_k$. Mostre que $d < n^2$ e encontre todos os n para os quais $d \mid n^2$.*

1.25 (IMO1997). *Encontrar todos os pares (x, y) de inteiros positivos tais que $x^{y^2} = y^x$.*

Dica: Sejam $x = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ e $y = p_1^{\beta_1} \dots p_n^{\beta_n}$ as fatorações canônicas de x e y . Mostre que $\alpha_j = t\beta_j$ e $x = y^t$ para algum $t \in \mathbb{Q}$ e limite os valores de t .

1.26. *Generalizar o resultado anterior para $x^{y^n} = y^x$, onde x e y são inteiros positivos.*

1.27 (IMO1984). *Sejam a, b, c, d inteiros ímpares tais que $0 < a < b < c < d$ e $ad = bc$. Demonstre que se $a + d = 2^k$ e $b + c = 2^m$ para inteiros k e m , então $a = 1$.*

1.4 Congruências

Sejam $a, b, n \in \mathbb{Z}$. Dizemos que a é congruente a b módulo n , e escrevemos

$$a \equiv b \pmod{n}$$

se $n \mid a - b$, ou seja, se a e b deixam o mesmo resto na divisão por n . Por exemplo, temos que $17 \equiv 3 \pmod{7}$ e $10 \equiv -5 \pmod{3}$.

Proposição 1.24. *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$ temos:*

1. (Reflexividade) $a \equiv a \pmod{n}$;
2. (Simetria) se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$;
3. (Transitividade) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$;
4. (Compatibilidade com a soma e diferença) Podemos somar e subtrair “membro a membro”:

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{n} \\ a - c \equiv b - d \pmod{n} \end{cases}$$

Em particular, se $a \equiv b \pmod{n}$, então $ka \equiv kb \pmod{n}$ para todo $k \in \mathbb{Z}$.

5. (*Compatibilidade com o produto*) Podemos multiplicar “membro a membro”:

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \implies ac \equiv bd \pmod{n}$$

Em particular, se $a \equiv b \pmod{n}$, então $a^k \equiv b^k \pmod{n}$ para todo $k \in \mathbb{N}$.

6. (*Cancelamento*) Se $\text{mdc}(c, n) = 1$, então

$$ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n}.$$

DEMONSTRAÇÃO: Para o item (1) basta observar que $n \mid a - a = 0$. Em (2), se $n \mid a - b$, então $n \mid -(a - b) \iff n \mid b - a$. Em (3), se $n \mid a - b$ e $n \mid b - c$, então $n \mid (a - b) + (b - c) \iff n \mid a - c$. Em (4) e (5), se $n \mid a - b$ e $n \mid c - d$, então $n \mid (a - b) + (c - d) \iff n \mid (a + c) - (b + d)$, $n \mid (a - b) - (c - d) \iff n \mid (a - c) - (b - d)$ e $n \mid (a - b)c + (c - d)b \iff n \mid ac - bd$. Finalmente, como $\text{mdc}(c, n) = 1$ temos que $n \mid ac - bc \iff n \mid (a - b)c \iff n \mid a - b$ pela proposição 1.9. \square

As propriedades acima mostram que a relação $\equiv \pmod{n}$ (“ser congruente módulo n ”) tem um comportamento muito similar à relação de igualdade usual. São estas propriedades que tornam as congruências tão úteis em problemas de divisibilidade. Vejamos alguns exemplos.

Exemplo 1.25. *Demonstrar que $31 \mid 20^{15} - 1$.*

SOLUÇÃO: Isto é equivalente a demonstrar que $20^{15} \equiv 1 \pmod{31}$. Para isso observemos que

$$20 \equiv -11 \pmod{31} \tag{*}$$

e assim $20^2 \equiv (-11)^2 \pmod{31} \iff 20^2 \equiv 121 \pmod{31}$. Como $121 \equiv -3 \pmod{31}$ temos

$$20^2 \equiv -3 \pmod{31}. \tag{**}$$

Multiplicando (*) e (**) membro a membro, obtemos $20^3 \equiv 33 \pmod{31}$ e, como $33 \equiv 2 \pmod{31}$,

$$20^3 \equiv 2 \pmod{31}.$$

Elevando a 5, temos que $20^{15} \equiv 32 \pmod{31}$ e como $32 \equiv 1 \pmod{31}$, obtemos $20^{15} \equiv 1 \pmod{31}$, como desejado. \square

Exemplo 1.26. *Encontre os restos das divisões de*

1. 3^{1000} por 101

2. 5^{320} por 13

SOLUÇÃO: Como $3^4 \equiv -20 \pmod{101}$, elevando ao quadrado obtemos $3^8 \equiv 400 \pmod{101} \iff 3^8 \equiv -4 \pmod{101}$. Multiplicando por 3^2 , obtemos $3^{10} \equiv -36 \pmod{101}$. Portanto

$$\begin{aligned} 3^{20} &\equiv 1296 \pmod{101} \iff 3^{20} \equiv -17 \pmod{101} \\ 3^{40} &\equiv 289 \pmod{101} \iff 3^{40} \equiv -14 \pmod{101} \\ 3^{80} &\equiv 196 \pmod{101} \iff 3^{80} \equiv -6 \pmod{101} \\ 3^{80} \cdot 3^{20} &\equiv (-6) \cdot (-17) \pmod{101} \iff 3^{100} \equiv 1 \pmod{101}. \end{aligned}$$

Assim, elevando a última congruência a 10, obtemos $3^{1000} \equiv 1 \pmod{101}$, ou seja, 3^{1000} deixa resto 1 na divisão por 101.

Para encontrar o resto da divisão de 5^{320} por 13, note que como $5^4 \equiv 1 \pmod{13}$, os restos de 5^n por 13 se repetem com período 4:

$$\begin{array}{ll} 5^0 \equiv 1 \pmod{13} & 5^4 \equiv 1 \pmod{13} \\ 5^1 \equiv 5 \pmod{13} & 5^5 \equiv 5 \pmod{13} \\ 5^2 \equiv -1 \pmod{13} & 5^6 \equiv -1 \pmod{13} \\ 5^3 \equiv -5 \pmod{13} & 5^7 \equiv -5 \pmod{13} \quad \dots \end{array}$$

Por outro lado, temos $3 \equiv -1 \pmod{4} \implies 3^{20} \equiv 1 \pmod{4}$, isto é, 3^{20} deixa resto 1 na divisão por 4. Assim, $5^{320} \equiv 5^1 \pmod{13}$, ou seja, 5^{320} deixa resto 5 na divisão por 13. \square

O problema a seguir tem uma história interessante. Em um artigo publicado em 1969, D. J. Lewis afirmava que a equação $x^3 - 117y^3 = 5$ tem no máximo 18 soluções inteiras. Na verdade, ela não possui nenhuma, como foi provado dois anos mais tarde por R. Finkelstein e H. London, utilizando métodos de Teoria Algébrica dos Números. Em 1973, F. Halter-Koch e V. Št. Udresco observaram independentemente que existe uma prova muito mais simples deste fato, como mostra o exemplo a seguir.

Exemplo 1.27. *Mostre que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras.*

SOLUÇÃO: Observe que como 117 é múltiplo de 9, qualquer solução inteira deve satisfazer

$$x^3 - 117y^3 \equiv 5 \pmod{9} \iff x^3 \equiv 5 \pmod{9}.$$

Porém, x só pode deixar resto 0, 1, ..., 8 na divisão por 9. Analisando estes 9 casos, temos

$x \bmod 9$	0	1	2	3	4	5	6	7	8
$x^3 \bmod 9$	0	1	8	0	1	8	0	1	8

Ou seja, x^3 só pode deixar resto 0, 1 ou 8 na divisão por 9. Logo $x^3 \equiv 5 \pmod{9}$ é impossível e a equação não possui soluções inteiras. \square

Exemplo 1.28 (AusPol2002). *Encontrar todas as ternas (a, b, c) de inteiros não negativos tais que $2^a + 2^b + 1$ é múltiplo de $2^c - 1$.*

SOLUÇÃO: O problema pede para determinar quando $2^a + 2^b + 1 \equiv 0 \pmod{2^c - 1}$. Note que como $2^c \equiv 1 \pmod{2^c - 1}$, escrevendo $a = cq_1 + a'$ e $b = cq_2 + b'$ com $0 \leq a', b' < c$ temos que

$$\begin{aligned} 2^a + 2^b + 1 &\equiv 0 \pmod{2^c - 1} \\ \iff (2^c)^{q_1} \cdot 2^{a'} + (2^c)^{q_2} \cdot 2^{b'} + 1 &\equiv 0 \pmod{2^c - 1} \\ \iff 2^{a'} + 2^{b'} + 1 &\equiv 0 \pmod{2^c - 1} \end{aligned}$$

que é o mesmo problema com a' e b' no lugar de a e b . Assim, basta resolver o problema supondo $0 \leq a, b < c$. Temos alguns casos a analisar.

Não há soluções com $c = 0$ e para $c = 1$ temos que $(a, b, 1)$ é solução para todos os $a, b \geq 0$. Se $c = 2$, temos que apenas $(0, 0, 2)$ é solução com $0 \leq a, b < c = 2$, o que dá origem às soluções $(2m, 2n, 2)$ para todos os m e n naturais. Se $c = 3$, temos que apenas $(1, 2, 3)$ e $(2, 1, 3)$ são soluções com $0 \leq a, b < c = 3$, o que nos fornece soluções $(1 + 3m, 2 + 3n, 3)$ e $(2 + 3m, 1 + 3n, 3)$ para todos os m e n naturais. Finalmente, para $c \geq 4$, temos que se $a < c - 1$ ou $b < c - 1$, então

$$3 \leq 2^a + 2^b + 1 \leq 2^{c-1} + 2^{c-2} + 1 = 3 \cdot 2^{c-2} + 1 < 2^c - 1$$

e assim $2^a + 2^b + 1$ não pode ser múltiplo de $2^c - 1$. Neste caso devemos ter $a = b = c - 1$ e $2^{c-1} + 2^{c-1} + 1 \equiv 0 \pmod{2^c - 1} \iff 2^c + 1 \equiv 0 \pmod{2^c - 1} \iff 2 \equiv 0 \pmod{2^c - 1}$, o que não ocorre pois $2^c - 1 \geq 15$ não pode dividir 2. Logo não há soluções neste último caso.

Resumindo, as ternas pedidas são $(m, n, 1)$, $(2m, 2n, 2)$, $(1 + 3m, 2 + 3n, 3)$ e $(2 + 3m, 1 + 3n, 3)$ onde m e n são naturais arbitrários. \square

1.5 Bases

A notação usual para naturais é a chamada base 10, com dígitos $0, \dots, 9$. Isto significa, por exemplo, que

$$196883 = 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0.$$

O teorema abaixo mostra como escrever qualquer natural em qualquer base d .

Teorema 1.29. *Seja $n \geq 0$ e $d > 1$. Então existe uma única sequência (os “dígitos” de n na base d) a_0, \dots, a_k, \dots com as seguintes propriedades:*

1. para todo k , $0 \leq a_k < d$,
2. existe m tal que se $k \geq m$, então $a_k = 0$,
3. $n = \sum_{k \geq 0} a_k d^k$.

DEMONSTRAÇÃO: Escrevemos $n = n_0 = n_1 d + a_0$, $0 \leq a_0 < d$, $n_1 = n_2 d + a_1$, $0 \leq a_1 < d$ e em geral $n_k = n_{k+1} d + a_k$, $0 \leq a_k < d$. Nossa primeira afirmação é que $n_k = 0$ para algum valor de k . De fato, se

$n_0 < d^m$, então $n_1 = \lfloor \frac{n_0}{d} \rfloor < d^{m-1}$ e mais geralmente, por indução, $n_k < d^{m-k}$; fazendo $k \geq m$ temos $n_k < 1$ donde $n_k = 0$. Segue daí que $a_k = 0$ para $k \geq m$. A identidade do item 3 é facilmente demonstrada por indução.

Para a unicidade, suponha $\sum_{k \geq 0} a_k d^k = \sum_{k \geq 0} b_k d^k$. Se as sequências a_k e b_k são distintas existe um menor índice, digamos j , para o qual $a_j \neq b_j$. Podemos escrever $a_j + \sum_{k > j} a_k d^{k-j} = b_j + \sum_{k > j} b_k d^{k-j}$ donde $a_j \equiv b_j \pmod{d}$, o que é uma contradição, pois $0 < |a_j - b_j| < d$ e portanto $a_j - b_j$ não pode ser um múltiplo de d . \square

Ignorando os dígitos 0's iniciais, denotamos por $(a_n a_{n-1} \cdots a_1 a_0)_d$ o natural cuja representação na base d tem algarismos a_k como no teorema acima:

$$(a_n a_{n-1} \cdots a_1 a_0)_d \stackrel{\text{def}}{=} \sum_{0 \leq k \leq n} a_k d^k.$$

Muitos dos famosos critérios de divisibilidade que aprendemos na escola decorrem diretamente da representação acima. Por exemplo, se $N = (a_n a_{n-1} \cdots a_1 a_0)_{10}$, como $10 \equiv 1 \pmod{9}$, temos que $10^k \equiv 1 \pmod{9}$, donde

$$N = \sum_{0 \leq k \leq n} a_k 10^k \equiv \sum_{0 \leq k \leq n} a_k \pmod{9}.$$

Segue que N e a soma de seus dígitos na base 10 possuem o mesmo resto na divisão por 9; em particular N é divisível por 9 se, e só se, a soma de seus dígitos $a_0 + \cdots + a_n$ é divisível por 9.

De forma similar, para o critério de divisibilidade por 11, observemos que $10 \equiv -1 \pmod{11}$, logo

$$N = \sum_{0 \leq k \leq n} a_k 10^k \equiv \sum_{0 \leq k \leq n} (-1)^k a_k \pmod{11}$$

e assim um número é divisível por 11 se, e só se, a soma dos dígitos em posição par menos a soma dos dígitos em posição ímpar é divisível por 11. De igual forma, podemos encontrar critérios de divisibilidade por 7, 13 e 37, que deixamos como exercício para o leitor enunciá-los e demonstrá-los (utilize o fato que $10^3 \equiv -1 \pmod{7}$, $10^3 \equiv -1 \pmod{13}$ e $10^3 \equiv 1 \pmod{37}$).

Exemplo 1.30. *Encontrar os últimos dois dígitos na representação decimal de 3^{200} .*

SOLUÇÃO: Como

$$\begin{aligned}(a_n a_{n-1} \cdots a_1 a_0)_{10} &= 10^2 \cdot (a_n \cdot 10^{n-2} + \cdots + a_2) + (10 \cdot a_1 + a_0) \\ &= 100 \cdot (a_n \cdots a_2)_{10} + (a_1 a_0)_{10}\end{aligned}$$

temos que o número formado pelos dois últimos dígitos de $(a_n \cdots a_1 a_0)_{10}$ é o resto da divisão deste número por 100, logo o problema se resume a calcular 3^{200} módulo 100. Podemos utilizar o binômio de Newton para simplificar as contas:

$$3^{200} = 9^{100} = (10 - 1)^{100} = \sum_{0 \leq k \leq 100} \binom{100}{k} 10^{100-k} (-1)^k,$$

logo $3^{200} \equiv -\binom{100}{99}10 + \binom{100}{100} \pmod{100} \iff 3^{200} \equiv 1 \pmod{100}$ e assim os dois últimos dígitos de 3^{200} são 01. \square

Exemplo 1.31. *Demonstrar que, para todo n natural ímpar,*

$$s_n = 2^{2n} \cdot (2^{2n+1} - 1)$$

termina em 28 quando escrito em notação decimal.

SOLUÇÃO: Vamos mostrar por indução em n que s_n termina em 28. Para $n = 1$ temos que $s_1 = 28$. Suponhamos que para algum $n \geq 1$ ímpar s_n termina em 28 e vamos mostrar que s_{n+2} termina em 28 ou, equivalentemente, que $100 \mid s_{n+2} - s_n$. Temos

$$\begin{aligned}s_{n+2} - s_n &= 2^{2(n+2)} \cdot (2^{2(n+2)+1} - 1) - 2^{2n} \cdot (2^{2n+1} - 1) \\ &= 2^{2n} \cdot (16 \cdot 2^{2n+5} - 16 - 2^{2n+1} + 1) \\ &= 5 \cdot 2^{2n} \cdot (51 \cdot 2^{2n+1} - 3).\end{aligned}$$

Como, para n ímpar,

$$\begin{aligned}2^2 &\equiv -1 \pmod{5} \implies 2^{2n} \equiv -1 \pmod{5} \\ &\implies 2^{2n+1} \equiv -2 \pmod{5},\end{aligned}$$

temos que $51 \cdot 2^{2n+1} - 3 \equiv 1 \cdot (-2) - 3 \pmod{5} \iff 51 \cdot 2^{2n+1} - 3 \equiv 0 \pmod{5}$. Assim, $s_{n+2} - s_n$ é divisível por $5 \cdot 4 \cdot 5 = 100$. \square

1.6 O Anel de Inteiros Módulo n

As semelhanças entre as relações de congruência módulo n e igualdade não são mero fruto do acaso, ambas são instâncias de *relações de equivalência* em \mathbb{Z} . Em geral, uma relação \sim sobre um conjunto X é dita de *equivalência* se ela é reflexiva ($x \sim x$ para todo $x \in X$), simétrica ($x \sim y \iff y \sim x$) e transitiva ($x \sim y$ e $y \sim z \implies x \sim z$).

Dar uma relação de equivalência em X é o mesmo que dar uma *partição* $X = \bigsqcup_{\lambda \in \Lambda} X_\lambda$ de X , i.e., uma coleção de subconjuntos $X_\lambda \neq \emptyset$, dois a dois disjuntos, cuja união é X . De fato, dada a partição acima, podemos definir uma relação de equivalência \sim declarando que $x \sim y$ se, e somente se, x e y pertencem a um mesmo X_λ . Reciprocamente, se \sim é uma relação de equivalência, dado um elemento $x \in X$ podemos definir a *classe de equivalência* \bar{x} de x como o conjunto de todos os elementos equivalentes a x :

$$\bar{x} = \{y \in X \mid y \sim x\}.$$

Observe que ou $\bar{x} \cap \bar{y} = \emptyset$ (se $x \not\sim y$) ou $\bar{x} = \bar{y}$ (se $x \sim y$). Assim, as distintas classes de equivalência \bar{x} formam uma partição de X . O conjunto $\{\bar{x} \mid x \in X\}$ das classes de equivalência de \sim é chamado de *quociente* de X por \sim e é denotado por X/\sim . Intuitivamente, X/\sim é o conjunto obtido “igualando-se” elementos equivalentes entre si.

Agora aplicamos esta construção geral ao nosso caso. O quociente de \mathbb{Z} pela relação $\equiv \pmod{n}$ é chamado de *anel de inteiros módulo n* e é denotado por uma das notações $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$, \mathbb{Z}/n ou às vezes \mathbb{Z}_n . Por exemplo, para $n = 2$, temos que $\mathbb{Z}/2\mathbb{Z}$ possui apenas dois elementos, $\bar{0}$ e $\bar{1}$ (popularmente conhecidos como conjunto dos pares e ímpares, respectivamente).

A definição de \bar{a} como um subconjunto de \mathbb{Z} raramente será importante, sendo apenas uma maneira de formalizar o fato de que estamos “identificando” todos os inteiros que deixam o mesmo resto na divisão por n (como no exemplo dos pares e ímpares acima). Assim, o importante é sabermos que

$$\begin{aligned} \bar{a} = \bar{a'} &\iff a \equiv a' \pmod{n} \\ &\iff a \text{ e } a' \text{ deixam o mesmo resto na divisão por } n. \end{aligned}$$

Se $n > 0$, a divisão euclidiana diz que todo inteiro a é côngruo a um único inteiro a' com $0 \leq a' < n$; podemos reescrever este fato na nossa

nova linguagem como

$$\mathbb{Z}/(n) = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Os itens (4) e (5) da proposição 1.24 dizem que as operações de soma, diferença e produto são compatíveis com a relação de congruência. Uma formulação mais abstrata da mesma ideia é dizer que as operações $+$, $-$ e \cdot *passam ao quociente*, i.e., que podemos definir a soma, subtração e o produto de classes de congruência por

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a + b} \\ \bar{a} - \bar{b} &= \overline{a - b} \\ \bar{a} \cdot \bar{b} &= \overline{a \cdot b}\end{aligned}$$

respectivamente. A dúvida à primeira vista seria se a escolha de a e b não afeta a resposta: afinal existem infinitos inteiros a' e b' com $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$. Os itens (4) e (5) da proposição são exatamente o que precisamos: eles nos dizem que nestas condições $\overline{a \pm b} = \overline{a' \pm b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$, de modo que as operações acima estão bem definidas.

Por exemplo, em $\mathbb{Z}/6\mathbb{Z}$ temos as seguintes tabelas de soma e produto:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$		\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	e	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$		$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$		$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$		$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$		$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$		$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

A próxima proposição diz quando podemos “dividir” por a módulo n , isto é, quando o “inverso multiplicativo” de a módulo n está definido:

Proposição 1.32. *Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod{n}$ se, e somente se, $\text{mdc}(a, n) = 1$.*

DEMONSTRAÇÃO: Temos que $ab \equiv 1 \pmod{n}$ admite solução na variável b se, e somente se, existem $b, k \in \mathbb{Z}$ tais que $ab - 1 = nk \iff ab - nk = 1$. Pelo corolário 1.8 do teorema de Bachet-Bézout, isto ocorre se, e só se, $\text{mdc}(a, n) = 1$. \square

Dizemos portanto que a é *invertível* módulo n quando $\text{mdc}(a, n) = 1$ e chamamos b com $ab \equiv 1 \pmod{n}$ de *inverso multiplicativo* de a módulo n . O inverso é sempre único módulo n : se $ab \equiv ab' \equiv 1 \pmod{n}$ temos

$$b \equiv b \cdot 1 \equiv b \cdot (ab') \equiv (ba) \cdot b \equiv 1 \cdot b' \equiv b' \pmod{n}.$$

Assim, \bar{b} está bem definido e, em termos de classes de congruência, temos que $\bar{a} \cdot \bar{b} = \bar{1}$; denotamos \bar{b} por $(\bar{a})^{-1}$. Note que pela demonstração da proposição acima calcular $(\bar{a})^{-1}$ é equivalente a resolver a equação diofantina linear $ax + ny = 1$ e para isto podemos utilizar o método do exemplo 1.14.

Definimos o *grupo de unidades* $(\mathbb{Z}/n\mathbb{Z})^\times \subset \mathbb{Z}/n\mathbb{Z}$ do anel de inteiros módulo n como o subconjunto formado pelos elementos invertíveis de $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{mdc}(a, n) = 1\}.$$

Observe que o produto de elementos de $(\mathbb{Z}/n\mathbb{Z})^\times$ é sempre um elemento de $(\mathbb{Z}/n\mathbb{Z})^\times$. Por exemplo, temos a seguinte tabela de multiplicação em $(\mathbb{Z}/15\mathbb{Z})^\times$:

\cdot	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{14}$	$\bar{1}$	$\bar{7}$	$\bar{11}$	$\bar{13}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{13}$	$\bar{2}$	$\bar{14}$	$\bar{7}$	$\bar{11}$
$\bar{7}$	$\bar{7}$	$\bar{14}$	$\bar{13}$	$\bar{4}$	$\bar{11}$	$\bar{2}$	$\bar{1}$	$\bar{8}$
$\bar{8}$	$\bar{8}$	$\bar{1}$	$\bar{2}$	$\bar{11}$	$\bar{4}$	$\bar{13}$	$\bar{14}$	$\bar{7}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{14}$	$\bar{2}$	$\bar{13}$	$\bar{1}$	$\bar{8}$	$\bar{4}$
$\bar{13}$	$\bar{13}$	$\bar{11}$	$\bar{7}$	$\bar{1}$	$\bar{14}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{14}$	$\bar{14}$	$\bar{13}$	$\bar{11}$	$\bar{8}$	$\bar{7}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

Uma aplicação do inverso multiplicativo é o famoso *teorema de Wilson*. Primeiramente precisamos de um lema.

Lema 1.33. *Se p é primo, então as únicas soluções de $x^2 = \bar{1}$ em $\mathbb{Z}/(p)$ são $\bar{1}$ e $-\bar{1}$. Em particular, se $x \in (\mathbb{Z}/(p))^\times - \{1, -1\}$, então $x^{-1} \neq x$ em $\mathbb{Z}/(p)$.*

DEMONSTRAÇÃO: Temos

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\iff p \mid (x^2 - 1) \iff p \mid (x - 1)(x + 1) \\ &\iff p \mid x - 1 \text{ ou } p \mid x + 1 \\ &\iff x \equiv 1 \pmod{p} \text{ ou } x \equiv -1 \pmod{p} \end{aligned}$$

donde o resultado segue. \square

Teorema 1.34 (Wilson). *Seja $n > 1$. Então $n \mid (n-1)! + 1$ se, e só se, n é primo. Mais precisamente,*

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \text{se } n \text{ é primo} \\ 0 \pmod{n} & \text{se } n \text{ é composto e } n \neq 4. \end{cases}$$

DEMONSTRAÇÃO: Se n é composto mas não é o quadrado de um primo podemos escrever $n = ab$ com $1 < a < b < n$. Neste caso tanto a quanto b são fatores de $(n-1)!$ e portanto $(n-1)! \equiv 0 \pmod{n}$. Se $n = p^2$, $p > 2$, então p e $2p$ são fatores de $(n-1)!$ e novamente $(n-1)! \equiv 0 \pmod{n}$; isto demonstra que para todo $n \neq 4$ composto temos $(n-1)! \equiv 0 \pmod{n}$.

Se n é primo podemos escrever $(n-1)! \equiv -2 \cdot 3 \cdot \dots \cdot (n-2) \pmod{n}$; mas pelo lema anterior podemos juntar os inversos aos pares no produto do lado direito, donde $(n-1)! \equiv -1 \pmod{n}$. \square

Vejamos uma aplicação do teorema de Wilson.

Teorema 1.35 (Teorema de Wolstenholme). *Seja $p > 3$ um número primo. Então o numerador do número*

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$$

é divisível por p^2 .

DEMONSTRAÇÃO: Note que somando os “extremos” temos

$$\sum_{1 \leq i \leq p-1} \frac{1}{i} = \sum_{1 \leq i \leq \frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i} \right) = p \sum_{1 \leq i \leq \frac{p-1}{2}} \frac{1}{i(p-i)}.$$

Como o mmc dos números de 1 a $p-1$ não é divisível por p , basta mostrar que o numerador da última soma é múltiplo de p . Equivalentemente, como $p \nmid (p-1)!$, devemos mostrar que o inteiro

$$S \stackrel{\text{def}}{=} \sum_{1 \leq i \leq \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)}$$

é um múltiplo de p . Para $1 \leq i \leq p-1$, denote por r_i o inverso de $i \bmod p$, ou seja, $ir_i \equiv 1 \pmod{p}$. Note que $r_{p-i} \equiv -r_i \pmod{p}$, assim

$$\begin{aligned} S &\equiv \sum_{1 \leq i \leq \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)} \cdot ir_i(p-i)r_{p-i} \\ &\equiv \sum_{1 \leq i \leq \frac{p-1}{2}} (p-1)!r_ir_{p-i} \equiv \sum_{1 \leq i \leq \frac{p-1}{2}} r_i^2 \pmod{p} \end{aligned}$$

pelo teorema de Wilson. Note que como cada r_i é congruente a um dos números $\pm 1, \pm 2, \dots, \pm \frac{p-1}{2}$, temos que os r_i^2 são congruentes a um dos números $1^2, 2^2, \dots, (\frac{p-1}{2})^2$ módulo p . Vamos mostrar que todos eles aparecem. De fato, se $r_i^2 \equiv r_j^2 \pmod{p}$, então $p \mid (r_i - r_j)(r_i + r_j)$, isto é, $r_i \equiv \pm r_j \pmod{p}$. Multiplicando por ij , temos que $j \equiv \pm i \pmod{p}$, o implica $i = j$ pois $1 \leq i, j \leq \frac{p-1}{2}$.

Assim, $S \equiv \sum_{1 \leq i \leq \frac{p-1}{2}} i^2 \pmod{p}$ e como $\sum_{1 \leq i \leq \frac{p-1}{2}} i^2 = \frac{p(p^2-1)}{24}$ é um múltiplo de p (pois $\text{mdc}(p, 24) = 1$), o resultado segue. \square

O teorema de Wilson produz ainda resultados interessantes sobre os coeficientes binomiais. Suponhamos que k e h são inteiros positivos tais que $k + h = p - 1$ onde p é primo. Então

$$\begin{aligned} h!k! &\equiv (-1)^h(p-1)(p-2) \cdots (p-h)k! = (-1)^k(p-1)! \\ &\equiv (-1)^{k+1} \pmod{p}. \end{aligned}$$

Portanto

$$\begin{aligned} h!k! \binom{p-1}{k} &\equiv (p-1)! \pmod{p} \\ \iff (-1)^{k+1} \binom{p-1}{k} &\equiv -1 \pmod{p} \\ \iff \binom{p-1}{k} &\equiv (-1)^k \pmod{p}. \end{aligned}$$

Exemplo 1.36. *Demonstrar que se $p > 3$ é primo, então $p^3 \mid \binom{2p}{p} - 2$.*

SOLUÇÃO: Primeiramente, vamos relembrar algumas identidades com coeficientes binomiais bem conhecidas. Para todo $1 \leq i \leq p-1$, temos

que $\binom{p}{i} = \frac{p}{i} \binom{p-1}{i-1}$ (basta utilizar a definição) enquanto que

$$\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \cdots + \binom{p}{p}^2$$

pois podemos escolher p objetos dentre $2p$ escolhendo i objetos dentre os p primeiros e $p-i$ dos p últimos para todo i entre 0 e p , logo

$$\binom{2p}{p} = \sum_{0 \leq i \leq p} \binom{p}{i} \binom{p}{p-i} = \sum_{0 \leq i \leq p} \binom{p}{i}^2.$$

Utilizando estas identidades, temos que

$$\binom{2p}{p} - 2 = \sum_{1 \leq i \leq p-1} \frac{p^2}{i^2} \binom{p-1}{i-1}^2 = p^2 \sum_{1 \leq i \leq p-1} \frac{1}{i^2} \binom{p-1}{i-1}^2.$$

Note que $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ é um múltiplo de p para $1 \leq i \leq p-1$ pois o denominador desta fração não é divisível por p . Assim, $\frac{1}{i^2} \binom{p-1}{i-1}^2 = \frac{1}{p^2} \binom{p}{i}^2$ é inteiro e portanto a soma $\sum_{1 \leq i \leq p-1} \frac{1}{i^2} \binom{p-1}{i-1}^2$ é inteira e devemos mostrar que ela é um múltiplo de p . Para isto observemos que cada $1 \leq i \leq p-1$ é invertível módulo p ; seja r_i tal que $1 \leq r_i \leq p-1$ e $ir_i \equiv 1 \pmod{p}$. Pela unicidade de r_i módulo p , temos que os r_i 's formam uma permutação de $1, 2, \dots, p-1$. Assim, como $\binom{p-1}{i-1} \equiv (-1)^{i-1} \pmod{p}$, temos

$$\begin{aligned} \sum_{1 \leq i \leq p-1} \frac{1}{i^2} \binom{p-1}{i-1}^2 &\equiv \sum_{1 \leq i \leq p-1} \frac{(ir_i)^2}{i^2} \binom{p-1}{i-1}^2 \pmod{p} \\ \iff \sum_{1 \leq i \leq p-1} \frac{1}{i^2} \binom{p-1}{i-1}^2 &\equiv \sum_{1 \leq i \leq p-1} r_i^2 = \sum_{1 \leq i \leq p-1} i^2 \pmod{p}. \end{aligned}$$

Como $\sum_{1 \leq i \leq p-1} i^2 = \frac{p(p-1)(2p-1)}{6}$ é um múltiplo de p (pois $\text{mdc}(p, 6) = 1$), a prova acaba. \square

Os termos grupo e anel empregados nesta seção estão em conformidade com o jargão usualmente utilizado em Álgebra. *Grupo* é o nome emprestado a um conjunto G juntamente com uma operação binária \cdot (produto) que satisfaz os seguintes três axiomas:

1. (Associatividade) Para quaisquer $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. (Existência de elemento neutro) Existe um elemento $e \in G$ tal que, para todo $a \in G$, $a \cdot e = e \cdot a = a$.
3. (Existência de inverso) Para qualquer elemento $a \in G$ existe um elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Se, além dos três axiomas acima, o grupo G satisfaz

4. (Comutatividade) Para quaisquer $a, b \in G$, $a \cdot b = b \cdot a$.

então G é chamado de *grupo abeliano*.

Um *anel* é um conjunto A com duas operações binárias $+$ (soma) e \cdot (produto) satisfazendo axiomas que abstraem as propriedades usuais dos inteiros (por exemplo). Estes axiomas são

1. $(A, +)$ é um grupo abeliano com elemento neutro 0 .
2. (Associatividade do produto) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a, b, c \in A$.
3. (Elemento neutro do produto) Existe um elemento $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in A$.
4. (Distributividade) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ para todo $a, b, c \in A$.

Se $a \cdot b = b \cdot a$ para todo $a, b \in A$, dizemos que o anel A é *comutativo*. Um anel comutativo $A \neq 0$ (isto é, $0 \neq 1$ em A) é chamado de *domínio* se, para $a, b \in A$, $a \cdot b = 0 \implies a = 0$ ou $b = 0$. Por outro lado, se um anel comutativo $A \neq 0$ é tal que todo elemento não nulo possui inverso multiplicativo (ou seja, $(A \setminus \{0\}, \cdot)$ é um grupo) então dizemos que o anel A é um *corpo*. Um importante resultado é a seguinte

Proposição 1.37. *O anel $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e só se, n é primo.*

DEMONSTRAÇÃO: Temos que $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e somente se, todo elemento $\bar{a} \neq \bar{0}$ é invertível, ou seja, se e somente se, $\text{mdc}(a, n) = 1$ para todo a com $0 < a < n$. Mas isto é equivalente a n ser primo, pois se n é composto e $a \mid n$ com $1 < a < n$, então $\text{mdc}(a, n) = a \neq 1$. \square

Um fato curioso e muito útil quando trabalhamos no corpo $\mathbb{Z}/p\mathbb{Z}$ (p primo) é a seguinte

Proposição 1.38 (“Sonho de todo estudante”). *Seja p um primo. Então em $\mathbb{Z}/p\mathbb{Z}$ temos*

$$(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p$$

para quaisquer $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$.

DEMONSTRAÇÃO: Devemos mostrar que $(a + b)^p \equiv a^p + b^p \pmod{p}$ para todo $a, b \in \mathbb{Z}$. Temos que se $0 < k < p$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \equiv 0 \pmod{p}$$

pois há um fator p no numerador que não pode ser cancelado com nada que apareça no denominador. Assim, utilizando o binômio de Newton, temos

$$(a + b)^p = \sum_{0 \leq k \leq p} \binom{p}{k} a^{p-k} b^k \equiv a^p + b^p \pmod{p}$$

como queríamos mostrar. □

1.7 A Função de Euler e o Teorema de Euler-Fermat

Dizemos que um conjunto de n números inteiros a_1, \dots, a_n forma um *sistema completo de restos módulo n* (scr) se

$$\{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n\} = \mathbb{Z}/(n),$$

isto é, se os a_i representam todas as classes de congruência módulo n . Por exemplo, $0, 1, 2, \dots, n-1$ formam um scr módulo n . Equivalentemente, podemos dizer que a_1, a_2, \dots, a_n formam um scr módulo n se, e somente se, $a_i \equiv a_j \pmod{n}$ implicar $i = j$.

De igual forma, dizemos que os números inteiros $b_1, b_2, \dots, b_{\varphi(n)}$ formam um *sistema completo de invertíveis módulo n* (sci) se

$$\{\bar{b}_1, \bar{b}_2, \dots, \bar{b}_{\varphi(n)}\} = (\mathbb{Z}/(n))^\times,$$

onde $\varphi(n)$ representa o número de elementos de $(\mathbb{Z}/(n))^\times$. Em outras palavras, $b_1, b_2, \dots, b_{\varphi(n)}$ formam um sci módulo n se, e somente se, representam todas as classes de congruência invertíveis módulo n ou, equivalentemente, $\text{mdc}(b_i, n) = 1$ para todo i e $b_i \equiv b_j \pmod{n}$ implica $i = j$. O conjunto $\{k \in \mathbb{Z} \mid 1 \leq k \leq n \text{ e } \text{mdc}(n, k) = 1\}$ é um exemplo de sci módulo n .

Definição 1.39. A função

$$\varphi(n) \stackrel{\text{def}}{=} |(\mathbb{Z}/n\mathbb{Z})^\times|$$

é chamada de função phi de Euler.

Temos $\varphi(1) = \varphi(2) = 1$ e, para $n > 2$, $1 < \varphi(n) < n$. Se p é primo, $\varphi(p) = p - 1$; mais geralmente $\varphi(p^k) = p^k - p^{k-1}$ pois $\text{mdc}(a, p^k) = 1$ se, e somente se, a não é múltiplo de p e há p^{k-1} múltiplos de p no intervalo $1 \leq a \leq p^k$. Para calcular a função φ no caso geral, vamos mostrar que se $\text{mdc}(n, m) = 1$, então $\varphi(nm) = \varphi(n)\varphi(m)$. Consideremos os números $1, 2, \dots, nm$, onde $\text{mdc}(n, m) = 1$ e os arrumamos em forma matricial assim:

$$\begin{array}{ccccc} 1 & 2 & 3 & \dots & n \\ n+1 & n+2 & n+3 & \dots & 2n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n(m-1)+1 & n(m-1)+2 & n(m-1)+3 & \dots & n(m-1)+n \end{array}$$

Note que, como $\text{mdc}(ni + j, n) = \text{mdc}(j, n)$, se um número nesta tabela é primo relativo com n , então todos os números nessa coluna são primos relativos com n . Logo existem $\varphi(n)$ colunas nas quais todos os números são primos relativos com n . Por outro lado, toda coluna possui um conjunto completo de restos módulo m : se duas entradas são tais que $ni_1 + j \equiv ni_2 + j \pmod{m}$, então $i_1 \equiv i_2 \pmod{m}$ pois n é invertível módulo m já que $\text{mdc}(m, n) = 1$, logo como $0 \leq i_1, i_2 < m$ devemos ter $i_1 = i_2$. Desta forma, em cada coluna existem exatamente $\varphi(m)$ números que são primos relativos com m e portanto o total de números nesta tabela que são simultaneamente primos relativos com m e n (i.e. primos com nm) é $\varphi(nm) = \varphi(n)\varphi(m)$.

Assim, se $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ é a fatoração de n em potências de primos

distintos p_i , temos que

$$\varphi(n) = \prod_{1 \leq i \leq k} \varphi(p_i^{\alpha_i}) = \prod_{1 \leq i \leq k} (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{1 \leq i \leq k} \left(1 - \frac{1}{p_i}\right).$$

Agora estamos prontos para enunciar e provar o importante

Teorema 1.40 (Euler-Fermat). *Sejam a e m dois inteiros com $m > 0$ e $\text{mdc}(a, m) = 1$. Então*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

DEMONSTRAÇÃO: Observemos que se $r_1, r_2, \dots, r_{\varphi(m)}$ é um sistema completo de invertíveis módulo m e a é um número natural tal que $\text{mdc}(a, m) = 1$, então $ar_1, ar_2, \dots, ar_{\varphi(m)}$ também é um sistema completo de invertíveis módulo m . De fato, temos que $\text{mdc}(ar_i, m) = 1$ para todo i e se $ar_i \equiv ar_j \pmod{m}$, então $r_i \equiv r_j \pmod{m}$ pois a é invertível módulo m , logo $r_i = r_j$ e portanto $i = j$. Consequentemente cada ar_i deve ser congruente com algum r_j e, portanto,

$$\begin{aligned} \prod_{1 \leq i \leq \varphi(m)} (ar_i) &\equiv \prod_{1 \leq i \leq \varphi(m)} r_i \pmod{m} \\ \iff a^{\varphi(m)} \cdot \prod_{1 \leq i \leq \varphi(m)} r_i &\equiv \prod_{1 \leq i \leq \varphi(m)} r_i \pmod{m}. \end{aligned}$$

Mas como cada r_i é invertível módulo m , simplificando o fator $\prod_{1 \leq i \leq \varphi(m)} r_i$, obtemos o resultado desejado. \square

Como caso particular do teorema anterior obtemos o

Teorema 1.41 (Pequeno Teorema de Fermat). *Seja a um inteiro positivo e p um primo, então*

$$a^p \equiv a \pmod{p}$$

DEMONSTRAÇÃO: De fato, observemos que se $p \mid a$ o resultado é evidente. Então, podemos supor que $\text{mdc}(a, p) = 1$. Como $\varphi(p) = p - 1$, pelo teorema de Euler temos $a^{p-1} \equiv 1 \pmod{p}$, logo multiplicando por a obtemos o resultado desejado. \square

Observação 1.42. *O teorema de Euler-Fermat também pode ser provado utilizando-se o seguinte corolário do teorema de Lagrange em Teoria dos Grupos: se G é um grupo finito e $g \in G$, então $g^{|G|} = e$ (identidade). Aplicando este resultado para $G = (\mathbb{Z}/m\mathbb{Z})^\times$, temos que $\bar{a}^{\varphi(m)} = \bar{1}$ para todo $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$, que é uma formulação equivalente para o teorema de Euler-Fermat.*

Observemos que o teorema de Euler-Fermat pode ser otimizado da seguinte forma:

Proposição 1.43. *Sejam a e n números inteiros tais que $\text{mdc}(a, n) = 1$ e n se fatora como $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ em potências de primos distintos. Então*

$$a^M \equiv 1 \pmod{n} \quad \text{onde} \quad M = \text{mmc}(\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_k^{\alpha_k})).$$

DEMONSTRAÇÃO: Pelo teorema de Euler-Fermat sabemos que $a^{\varphi(p_j^{\alpha_j})} \equiv 1 \pmod{p_j^{\alpha_j}}$ para todo $j = 1, \dots, k$. Elevando a $M/\varphi(p_j^{\alpha_j})$, obtemos $a^M \equiv 1 \pmod{p_j^{\alpha_j}}$. Assim, $a^M - 1$ é múltiplo de $p_j^{\alpha_j}$ para todo j e como estes números são dois a dois primos entre si concluímos que $n \mid a^M - 1 \iff a^M \equiv 1 \pmod{n}$, como desejado. \square

Vejamos agora algumas aplicações do teorema de Euler-Fermat.

Exemplo 1.44. *Mostre que existem infinitos números da forma $20000 \dots 009$ que são múltiplos de 2009.*

DEMONSTRAÇÃO: O problema é equivalente a encontrar infinitos naturais k tais que

$$\begin{aligned} 2 \cdot 10^k + 9 \equiv 0 \pmod{2009} &\iff 2 \cdot 10^k + 9 \equiv 2009 \pmod{2009} \\ &\iff 10^{k-3} \equiv 1 \pmod{2009} \end{aligned}$$

pois 2000 é invertível módulo 2009. Como $\text{mdc}(10, 2009) = 1$, pelo teorema de Euler-Fermat temos que $10^{\varphi(2009)} \equiv 1 \pmod{2009} \implies 10^{\varphi(2009)t} \equiv 1 \pmod{2009}$ para todo $t \in \mathbb{N}$, logo basta tomar $k = \varphi(2009)t + 3$. \square

Exemplo 1.45. *Encontre um número $n \in \mathbb{N}$ tal que $2^n > 10^{2000}$ e 2^n tenha entre suas 2000 últimas casas decimais pelo menos 1000 zeros consecutivos.*

SOLUÇÃO: Sabemos que $2^{\varphi(5^{2000})} \equiv 1 \pmod{5^{2000}}$ pelo teorema de Euler-Fermat. Portanto existe $b \in \mathbb{N}$ com

$$2^{\varphi(5^{2000})} = 5^{2000}b + 1 \implies 2^{2000+\varphi(5^{2000})} = 10^{2000}b + 2^{2000}.$$

Portanto os 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coincidem com a representação decimal de 2^{2000} , que tem no máximo 667 dígitos pois $2^{2000} < (2^3)^{667} < 10^{667}$. Desta forma, há pelo menos $2000 - 667 = 1333$ zeros consecutivos dentre as 2000 últimas casas decimais de $2^{2000+\varphi(5^{2000})}$ e assim $n = \varphi(5^{2000}) + 2000 = 4 \cdot 5^{1999} + 2000$ satisfaz as condições do enunciado. \square

Exemplo 1.46. *Mostre que não existe inteiro x tal que $103 \mid x^3 - 2$.*

SOLUÇÃO: Note primeiramente que 103 é primo. Agora suponha que $x^3 \equiv 2 \pmod{103}$, de modo que $103 \nmid x$. Elevando ambos os lados desta congruência a $(103 - 1)/3 = 34$, obtemos $x^{102} \equiv 2^{34} \pmod{103}$ e sabemos pelo teorema de Euler-Fermat que $x^{102} \equiv 1 \pmod{103}$. Porém, fazendo as contas, obtemos que $2^{34} \equiv 46 \pmod{103}$, uma contradição. Logo não há inteiro x tal que $103 \mid x^3 - 2$. \square

Utilizando o mesmo raciocínio do exemplo anterior, temos que se p é um primo tal que $p \equiv 1 \pmod{3}$ e $p \nmid a$, então uma condição necessária para que $x^3 \equiv a \pmod{p}$ tenha solução em x é que $a^{(p-1)/3} \equiv 1 \pmod{p}$. Esta condição também é suficiente, pela existência de raízes primitivas módulo p , como mostraremos no final deste capítulo.

Exemplo 1.47. *Demonstrar que se $p > 2$ é primo, então*

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv p + (p-1)! \pmod{p^2}.$$

SOLUÇÃO: Pelo pequeno teorema de Fermat, sabemos que $i^{p-1} \equiv 1 \pmod{p}$ para todo $1 \leq i \leq p-1$, isto é, que $i^{p-1} = k_i p + 1$ onde k_i é um inteiro. Assim, $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} = (k_1 + k_2 + \cdots + k_{p-1})p + p - 1$

e portanto devemos mostrar que $(k_1 + k_2 + \cdots + k_{p-1})p \equiv (p-1)! + 1 \pmod{p^2}$.

Multiplicando as equações $i^{p-1} = k_i p + 1$, temos

$$(k_1 p + 1)(k_2 p + 1) \cdots (k_{p-1} p + 1) = 1^{p-1} 2^{p-1} \cdots (p-1)^{p-1} = ((p-1)!)^{p-1}.$$

Por um lado, $(k_1 p + 1)(k_2 p + 1) \cdots (k_{p-1} p + 1) \equiv (k_1 + k_2 + \cdots + k_{p-1})p + 1 \pmod{p^2}$. Por outro, pelo teorema de Wilson sabemos que $(p-1)! \equiv -1 \pmod{p}$, ou seja, $(p-1)! = Kp - 1$ para algum K inteiro. Segue que

$$\begin{aligned} (k_1 + k_2 + \cdots + k_{p-1})p + 1 &\equiv (Kp - 1)^{p-1} \pmod{p^2} \\ \implies (k_1 + k_2 + \cdots + k_{p-1})p + 1 &\equiv 1 - \binom{p-1}{1} Kp \pmod{p^2} \\ \implies (k_1 + k_2 + \cdots + k_{p-1})p &\equiv Kp \pmod{p^2} \\ \implies (k_1 + k_2 + \cdots + k_{p-1})p &\equiv (p-1)! + 1 \pmod{p^2} \end{aligned}$$

o que encerra a prova. \square

Concluimos esta seção apresentando brevemente uma aplicação do Teorema de Euler que tem particular interesse prático: a *Criptografia RSA*. Trata-se de um método de criptografia com chave pública, isto é, um método que permite a qualquer pessoa transmitir mensagens por uma via insegura (ou seja, que pode ser monitorada por espíões) de modo que, na prática, apenas o legítimo destinatário, que conhece uma *chave*, pode recuperar a mensagem original. A sigla vem dos nomes de Ron Rivest, Adi Shamir, e Leonard Adleman, que desenvolveram esse método.

Para isso, o receptor publica um inteiro N que é o produto de dois primos razoavelmente grandes p e q (aproximadamente da mesma ordem de grandeza); N é público mas a sua fatoração pq só é conhecida pelo receptor. O receptor também publica um expoente s (em geral não muito grande) com $\text{mdc}(s, (p-1)(q-1)) = 1$. O receptor calcula (usando o algoritmo de Euclides) o inverso de $s \bmod (p-1)(q-1) = \varphi(N)$, isto é, um natural $r < (p-1)(q-1)$ com $rs \equiv 1 \pmod{(p-1)(q-1)}$ (donde $rs = 1 + k\varphi(N)$, para algum natural k). Note que apesar de N e s serem públicos, não parece ser fácil calcular $\varphi(N)$ ou r (neste contexto, calcular $\varphi(N) = (p-1)(q-1)$ dado $N = pq$ é equivalente a fatorar N , i.e., a encontrar os fatores primos p e q).

Uma mensagem é um número natural $m < N$. O emissor envia (ou publica) $\tilde{m} := m^s \pmod{N}$, com $0 < \tilde{m} < N$. O receptor recupera m via

$$m \equiv \tilde{m}^r \pmod{N}.$$

Para verificar essa equivalência, podemos observar que

$$\tilde{m}^r \equiv (m^s)^r = m^{rs} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \pmod{p};$$

note que, se $p \mid m$, os dois lados são $0 \pmod{p}$, e, caso contrário, $m^{p-1} \equiv 1 \pmod{p}$; analogamente $\tilde{m}^r \equiv m \pmod{q}$, donde $\tilde{m}^r \equiv m \pmod{N}$. Essas tarefas são relativamente rápidas computacionalmente. Mais precisamente, veremos a seguir que existem algoritmos polinomiais para testar primalidade, assim como para as demais operações necessárias (veja o capítulo 7, especialmente a seção sobre o teste de Agrawal, Kayal e Saxena que garante que testar primalidade de um número da ordem de N leva tempo no máximo polinomial em $\log N$).

Se existem algoritmos polinomiais para testar primalidade, não é verdade que sejam conhecidos algoritmos polinomiais (e *determinísticos*) para obter primos “novos” de uma determinada ordem de grandeza. Pelo teorema dos números primos (capítulo 5 e apêndice A), para todo N grande, a probabilidade de um número escolhido ao acaso entre N e $2N$ ser primo é $(1 + o(1))/\log N$, o que implica que, se testarmos $C \log N$ números ao acaso entre N e $2N$, a probabilidade de algum deles ser primo é da ordem de $1 - \exp(-C(1 + o(1)))$, que está muito perto de 1 para C grande. Se ao invés de sortear números procurarmos o menor primo maior ou igual a N (testando um por um) então, novamente pelo teorema dos números primos, *em média* o número de tentativas será da ordem de $\log(n)$. Entretanto, há gaps bem maiores do que $\log N$ e sabe-se muito pouco sobre o tamanho dos gaps (para um primo p , o gap $g(p)$ é igual a $q - p$ onde q é o menor primo maior do que p). Por exemplo, Harald Cramér conjectura que $g(p) < C(\log(p))^2$ (para algum $C > 0$; [41]): se isto for verdade então o algoritmo proposto acima é realmente polinomial. Pode ser que outra estratégia permita encontrar primos sem demonstrar esta conjectura, mas nada de tempo polinomial é conhecido. Há um projeto Polymath sobre este assunto: veja o preprint [117] e as páginas indicadas juntamente nas referências. Ainda assim, podemos considerar que o problema de obter primos é razoavelmente fácil e rápido para aplicações práticas pois aí devemos permitir algoritmos que dependem de sorteios e que obtêm o que é pedido em tempo

polinomial com probabilidade quase igual a 1. No interessante artigo de divulgação [125] é discutido o problema de gerar primos grandes, e em particular é apresentado um algoritmo que funciona em muitos casos e gera primos grandes cuja primalidade pode ser verificada por critérios bem mais simples que o teste de Agrawal, Kayal e Saxena, como o teste de Pocklington (veja o capítulo 7).

Não se conhecem algoritmos polinomiais para fatorar inteiros (grandes). A maioria dos especialistas duvida que exista tal algoritmo mas é preciso enfatizar que a não-existência de um tal algoritmo não é um teorema. Mais do que isso, a não-existência de tal algoritmo implica diretamente em $P \neq NP$ (um dos mais importantes problemas em aberto da matemática) mas $P \neq NP$ não parece implicar a não existência do algoritmo.

Existe ainda a possibilidade de que não exista um algoritmo rápido, mas que ainda assim exista uma máquina (no sentido literal) capaz de fatorar inteiros rapidamente. De fato, a mecânica quântica parece permitir a construção de um *computador quântico* e Peter Shor encontrou um “algoritmo” que permite a um computador quântico fatorar inteiros em tempo polinomial [135]. Em 2001 foi implementado tal algoritmo em um computador quântico nuclear de ressonância magnética com 7 qbit por um grupo da IBM, mas somente suficiente para fatorar o número 15 [116]. Em 2012 foi implementada uma modificação do algoritmo de Shor que tornou possível fatorar o número 21 em um (pequeno) computador quântico [99]. Não é claro se será possível construir computadores quânticos substancialmente maiores.

Resumindo, a criptografia RSA é eficiente e segura pois é muito mais rápido achar primos grandes do que fatorar números grandes e ele é bastante utilizado para encriptar mensagens transmitidas pela internet. Para mais informações sobre a criptografia RSA, veja [40].

Problemas Propostos

1.28. *Demonstrar que*

(a) $61 \mid 20^{15} - 1$.

(b) $13 \mid 2^{70} + 3^{70}$.

1.29. *Encontre os últimos três dígitos de 3^{2009} (na representação decimal).*

- 1.30.** Verifique se 987654321 é divisível por 9, 11, 13, 17 ou 19.
- 1.31.** Calcule o resto da divisão de $2^{2^{2011}}$ por 97.
- 1.32.** Determine um valor inteiro positivo de k tal que $5^k \equiv 97 \pmod{101}$.

1.33. Um inteiro positivo é capicua (ou palíndromo) se a sua representação decimal é igual lida da direita para a esquerda ou da esquerda para a direita.

Demonstre que todo número capicua com um número par de dígitos é divisível por 11. O que acontece com os números capicuas com um número ímpar de dígitos?

1.34. Encontre todos os números N de três dígitos (na representação decimal), tais que N é divisível por 11 e além disso $N/11$ é igual à soma dos quadrados dos dígitos de N .

1.35. Mostre que o dígito das dezenas de qualquer potência de 3 é um número par (por exemplo, o dígito das dezenas de $3^6 = 729$ é 2).

1.36. Mostre que, para todo $n \geq 0$, vale que $13 \mid 7^{2n+1} + 6^{2n+1}$.

1.37. Mostre que

$$a^{12} \equiv b^{12} \pmod{91} \iff \text{mdc}(a, 91) = \text{mdc}(b, 91).$$

1.38. (P. Sabini) Mostre que entre os números da forma

$$14, \quad 144, \quad 1444, \quad 14444, \quad 144 \cdots 44, \dots$$

os únicos quadrados perfeitos são $144 = 12^2$ e $1444 = 38^2$.

1.39. Seja $f : \mathbb{N}_{>0} \rightarrow \mathbb{N}$ uma função definida do conjunto dos inteiros positivos no conjunto dos números naturais tal que

$$(a) \quad f(1) = 0;$$

$$(b) \quad f(2n) = 2f(n) + 1;$$

$$(c) \quad f(2n + 1) = 2f(n).$$

Utilize a representação em base 2 de n para encontrar uma fórmula não recursiva para $f(n)$.

1.40. *Mostre que todo número racional positivo pode ser escrito de maneira única na forma*

$$\frac{a_1}{1!} + \frac{a_2}{2!} + \cdots + \frac{a_k}{k!}$$

onde:

$$0 \leq a_1, \quad 0 \leq a_2 < 2, \quad 0 \leq a_3 < 3, \quad \dots, \quad 0 < a_k < k.$$

1.41 (OBM1991). *Demonstre que existem infinitos múltiplos de 1991 que são da forma 19999...99991.*

1.42 (IMO1983). *É possível escolher 1983 inteiros positivos distintos, todos menores que 10^5 , tal que não existam três que sejam termos consecutivos de uma progressão aritmética?*

Dica: Usar base 3.

1.43. *Seja $S(n)$ a soma dos dígitos de n . Encontrar $S(S(S(2^{2^5} + 1)))$.*

1.44 (Chi2003). *Encontre todas as ternas (d, m, n) de inteiros positivos tais que $d^m + 1$ divide $d^n + 203$.*

1.45. *Seja $p > 2$ um número primo. Demonstre que*

$$\left(\left(\frac{p-1}{2} \right)! \right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

1.46 (AusPol1996). *Mostre que não existem inteiros não negativos m, n tais que $m! + 48 = 48(m+1)^n$.*

1.47. *Seja p um número primo. Demonstre que $(p-1)! + 1$ é uma potência de p se, e só se, $p = 2, 3$ ou 5 .*

1.48. *Demonstre que para todo número primo $p > 3$, o número $\binom{np}{p} - n$ é divisível por p^{3+r} onde p^r é a maior potência de p que divide n .*

1.49. *Demonstre que*

$$\sum_{\substack{1 \leq k \leq n \\ \text{mdc}(n, k) = 1}} k = \frac{n\varphi(n)}{2}.$$

1.50. *Demonstre que se $\text{mdc}(a, b) = 1$ então todos os divisores primos ímpares de $a^2 + b^2$ são da forma $4k + 1$.*

1.51. *Demonstre que existem infinitos primos da forma $4k + 1$.*

1.52. *Sejam m, n inteiros positivos. Demonstrar que $4mn - m - n$ nunca pode ser o quadrado de um número inteiro.*

1.53 (IMO1986). *Seja d um número positivo distinto de 2, 5 e 13. Demonstrar que é possível encontrar dois números diferentes a e b que pertençam ao conjunto $\{2, 5, 13, d\}$ tais que $ab - 1$ não é um quadrado perfeito.*

1.54. *Demonstre que se $p \mid (a^p - b^p)$, então $p^2 \mid (a^p - b^p)$.*

1.55 (IMO1984). *Encontre um par de inteiros positivos a, b tais que $ab(a + b)$ não é divisível por 7, mas $(a + b)^7 - a^7 - b^7$ é divisível por 7^7 .*

1.56. *Demonstre que para cada inteiro positivo n existe um inteiro m tal que 2^m tem no mínimo $\frac{2}{3}n - 1$ zeros entre seus últimos n dígitos em notação base 10.*

1.57 (IMO2003). *Seja p um número primo. Demonstre que existe um primo q tal que para todo n , o número $n^p - p$ não é divisível por q .*

1.58 (IMO1979). *Sejam m e n inteiros positivos tais que*

$$\frac{m}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Mostre que m é divisível por 1979.

1.59. *Seja p um número primo ímpar e sejam a e b inteiros não divisíveis por p tais que $p \mid a - b$. Mostre que $p^k \mid a^n - b^n \iff p^k \mid n(a - b)$.*

1.8 Polinômios

Dado um anel comutativo K , definimos o anel comutativo $K[x]$ como sendo o conjunto das expressões da forma $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ com $a_i \in K$, chamados de *polinômios* com coeficientes em K . A soma e o produto em $K[x]$ são definidos da maneira usual: dados $f(x) = \sum_i a_i x^i$ e $g(x) = \sum_i b_i x^i$ elementos de $K[x]$ temos

$$f(x) + g(x) \stackrel{\text{def}}{=} \sum_i (a_i + b_i) x^i;$$

$$f(x) \cdot g(x) \stackrel{\text{def}}{=} \sum_k c_k x^k \text{ onde } c_k = \sum_{i+j=k} a_i b_j.$$

Definimos o *grau* $\deg f(x)$ de um polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ como sendo o maior i tal que $a_i \neq 0$; o grau do polinômio nulo 0 é definido como sendo $-\infty$. Tal convenção visa a tornar válidas as seguintes identidades para todos os polinômios $f(x), g(x) \in K[x]$:

$$\begin{aligned}\deg(f(x) \cdot g(x)) &= \deg f(x) + \deg g(x) & \text{e} \\ \deg(f(x) + g(x)) &\leq \max\{\deg f(x), \deg g(x)\}.\end{aligned}$$

O coeficiente do termo de maior grau de um polinômio é chamado de *coeficiente líder*. Um polinômio cujo coeficiente líder é igual a 1 é chamado de *mônico*.

Observe que nas definições acima x é um símbolo formal e não um elemento de K . Apesar disso, cada polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ define uma *função polinomial*

$$\begin{aligned}f: K &\rightarrow K \\ c &\mapsto f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n\end{aligned}$$

também chamada de f . A distinção entre um polinômio e uma função polinomial é bem ilustrada pelo polinômio $f(x) = x^p - x \in (\mathbb{Z}/(p))[x]$: este polinômio é não nulo pois seus coeficientes são não nulos, mas para todo $c \in \mathbb{Z}/(p)$ temos $f(c) = 0$ pelo pequeno teorema de Fermat. Dado um polinômio $f(x) \in K[x]$, qualquer $c \in K$ tal que $f(c) = 0$ é chamado de *raiz* ou *zero* de $f(x)$.

Como veremos nesta seção, polinômios guardam muitas semelhanças com números inteiros. Por exemplo, podemos definir divisibilidade de polinômios de maneira completamente análoga: $d(x) \mid f(x)$ em $K[x]$ se, e só se, existe $g(x) \in K[x]$ tal que $f(x) = d(x) \cdot g(x)$. Temos também uma generalização da divisão euclidiana:

Proposição 1.48 (Algoritmo da divisão). *Seja K um corpo. Dados polinômios $f(x), g(x) \in K[x]$, com $g(x) \neq 0$, existem $q(x), r(x) \in K[x]$ (chamados respectivamente de quociente e resto da divisão de $f(x)$ por $g(x)$), unicamente determinados, tais que*

$$f(x) = q(x) \cdot g(x) + r(x) \quad \text{com} \quad \deg r(x) < \deg g(x).$$

DEMONSTRAÇÃO: Sejam $n = \deg f(x)$ e $m = \deg g(x)$. Para demonstrar a existência de $q(x)$ e $r(x)$, procederemos por indução sobre n . Note

que se $m > n$, então basta tomar $q(x) = 0$ e $r(x) = f(x)$, logo podemos supor que $m \leq n$. Se $n = m = 0$, então $f(x) = a$ e $g(x) = b$ são ambos constantes não nulas, logo basta tomar $q(x) = a/b$ e $r(x) = 0$ neste caso.

Agora suponha que $n \geq 1$. Escreva $f(x) = a_n x^n + f_1(x)$ e $g(x) = b_m x^m + g_1(x)$ com $a_n \neq 0$, $b_m \neq 0$ e $\deg f_1(x) < n$, $\deg g_1(x) < m$. Observemos que o polinômio $f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = f_1(x) - \frac{a_n}{b_m} x^{n-m} g_1(x)$ é de grau menor que n . Por hipótese de indução existem dois polinômios $q(x)$ e $r(x)$ tais que

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = q(x)g(x) + r(x) \quad \text{com} \quad \deg r(x) < \deg g(x).$$

Logo podemos escrever $f(x) = (\frac{a_n}{b_m} x^{n-m} + q(x)) \cdot g(x) + r(x)$, que era o que se queria demonstrar.

Para demonstrar que os polinômios $q(x)$ e $r(x)$ são únicos, suponha que

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

com $q_1(x) \neq q_2(x)$ e $\deg r_1(x), \deg r_2(x) < \deg g(x)$. Então $r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x) \neq 0$ é um múltiplo de $g(x)$ de grau estritamente menor do que $\deg g(x)$, o que é um absurdo. □

Corolário 1.49. *Seja K um corpo, $f(x) \in K[x]$ e $a \in K$. Então*

$$x - a \mid f(x) \iff f(a) = 0.$$

DEMONSTRAÇÃO: Como $\deg(x-a) = 1$, dividindo $f(x)$ por $x-a$ temos que $f(x) = (x-a)q(x) + r$ com $r \in K$. Assim, substituindo x por a , temos que $f(a) = r$ donde o resultado segue. □

Proposição 1.50. *Seja K um corpo. Um polinômio $f(x) \in K[x]$ não nulo de grau n tem no máximo n raízes em K .*

DEMONSTRAÇÃO: A demonstração é feita por indução em $n = \deg f(x)$; os casos $n = 0$ e $n = 1$ são triviais. Se $f(x)$ tivesse $n+1$ raízes distintas a_1, \dots, a_{n+1} , então $f(x) = (x - a_{n+1})g(x)$ para algum $g(x) \in K[x]$ pelo corolário anterior. Assim, para $i \neq n+1$, teríamos $0 = f(a_i) =$

$(a_i - a_{n+1})g(a_i) \implies g(a_i) = 0$ pois $(a_i - a_{n+1}) \neq 0$ é invertível em K . Logo $g(x)$, de grau $n - 1$, teria n raízes distintas a_1, \dots, a_n , contradizendo a hipótese de indução. \square

Note que o teorema anterior é falso se K não é um corpo. Por exemplo, o polinômio $f(x) = x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[x]$ tem 4 raízes em $\mathbb{Z}/8\mathbb{Z}$, a saber $\bar{1}, \bar{3}, \bar{5}, \bar{7}$.

Vejam os uma aplicação dos resultados anteriores quando $K = \mathbb{Z}/(p)$, p primo. A primeira é uma nova demonstração do teorema de Wilson:

Teorema 1.51. *Seja p um primo. Considere a função simétrica elementar σ_i em $1, 2, \dots, p - 1$ dada pela soma de todos os $\binom{p-1}{i}$ produtos de i termos distintos dentre $1, 2, \dots, p - 1$:*

$$\begin{aligned}\sigma_1 &= 1 + 2 + \dots + (p - 1) \\ \sigma_2 &= 1 \cdot 2 + 1 \cdot 3 + \dots + (p - 2)(p - 1) \\ &\vdots \\ \sigma_{p-1} &= 1 \cdot 2 \cdot \dots \cdot (p - 1).\end{aligned}$$

Então $\sigma_1, \dots, \sigma_{p-2}$ são todos múltiplos de p e $\sigma_{p-1} = (p - 1)! \equiv -1 \pmod{p}$ (teorema de Wilson).

DEMONSTRAÇÃO: Pelo teorema de Fermat e pela proposição anterior, temos que $\bar{1}, \bar{2}, \dots, \overline{p-1}$ são todas as raízes de $x^{p-1} - \bar{1}$ em $\mathbb{Z}/(p)$. Logo aplicando o corolário e comparando coeficientes líderes obtemos a fatoração

$$x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) \cdot \dots \cdot (x - \overline{p-1}).$$

Mas o polinômio do lado direito é igual a $x^{p-1} - \bar{\sigma}_1 x^{p-2} + \bar{\sigma}_2 x^{p-3} - \dots + (-1)^{p-1} \bar{\sigma}_{p-1}$. Comparando coeficientes, obtemos o resultado. \square

Seja K um corpo. Podemos considerar também congruências de polinômios em $K[x]$: se $a(x), b(x), m(x) \in K[x]$, escrevemos

$$a(x) \equiv b(x) \pmod{m(x)} \iff m(x) \mid a(x) - b(x).$$

As mesmas demonstrações do caso inteiro mostram que as congruências módulo $m(x)$ definem uma relação de equivalência em $K[x]$ compatível

com as operações de soma, subtração e produto. Assim, podemos formar o *anel quociente*

$$\frac{K[x]}{(m(x))}$$

cujos elementos são os conjuntos da forma

$$\overline{a(x)} \stackrel{\text{def}}{=} \{b(x) \in K[x] \mid b(x) \equiv a(x) \pmod{m(x)}\}$$

e as operações no anel quociente são dadas por

$$\overline{f(x)} + \overline{g(x)} \stackrel{\text{def}}{=} \overline{f(x) + g(x)} \quad \text{e} \quad \overline{f(x)} \cdot \overline{g(x)} \stackrel{\text{def}}{=} \overline{f(x) \cdot g(x)}$$

sendo independentes das escolhas dos representantes de classe $f(x)$ e $g(x)$. Se $\deg m(x) = n$, um sistema completo de resíduos módulo $m(x)$ é dado pelos polinômios de grau menor do que n (os possíveis restos na divisão euclidiana por $m(x)$):

$$\{a_0 + a_1x + \cdots + a_nx^{n-1} \mid a_i \in K\}$$

Em particular, $\frac{K[x]}{(m(x))}$ é infinito se K também o é.

Exemplo 1.52. *Determine o resto da divisão de $(x+1)^{2010}$ por x^2+x+1 em $\mathbb{Q}[x]$.*

SOLUÇÃO: Multiplicando por $x-1$ a congruência $x^2+x+1 \equiv 0 \pmod{x^2+x+1}$, obtemos $x^3 \equiv 1 \pmod{x^2+x+1}$. Assim, temos

$$\begin{aligned} (x+1)^2 &\equiv x \pmod{x^2+x+1} \\ \implies (x+1)^{2010} &\equiv x^{1005} = (x^3)^{335} \pmod{x^2+x+1} \\ \implies (x+1)^{2010} &\equiv 1 \pmod{x^2+x+1} \end{aligned}$$

Assim, o resto da divisão é 1. □

Podemos tentar definir o mdc $d(x)$ de dois polinômios $f(x)$ e $g(x)$ (com $f(x) \neq 0$ ou $g(x) \neq 0$) de maneira análoga ao mdc de inteiros, tomando o polinômio $d(x)$ de maior grau que divide $f(x)$ e $g(x)$ simultaneamente. Entretanto, $d(x)$ não está bem determinado, pois qualquer múltiplo $c \cdot d(x)$ com $c \neq 0$ constante ainda satisfaz as condições acima. Para evitar esta ambiguidade, definimos o mdc de $f(x)$ e $g(x)$ como

sendo o polinômio *mônico* de maior grau que divide $f(x)$ e $g(x)$ simultaneamente. Analogamente, define-se o mmc de $f(x)$ e $g(x)$ (com $f(x) \neq 0$ e $g(x) \neq 0$) como o polinômio mônico de menor grau que é divisível tanto por $f(x)$ como por $g(x)$.

A divisão euclidiana permite estender resultados de \mathbb{Z} para $K[x]$ de maneira quase trivial. Por exemplo, temos

Teorema 1.53 (Bachet-Bézout). *Seja $d(x)$ o máximo divisor comum de dois polinômios $f(x)$ e $g(x)$. Então existem dois polinômios $m(x)$ e $n(x)$ tais que $f(x)m(x) + g(x)n(x) = d(x)$.*

DEMONSTRAÇÃO: Análoga ao teorema 1.7; como naquele teorema $d(x)$ será o polinômio mônico de menor grau no conjunto

$$I(f, g) \stackrel{\text{def}}{=} \{f(x)m(x) + g(x)n(x) \mid m(x), n(x) \in K[x]\}.$$

□

Definição 1.54. *Seja K um corpo. Dizemos que um polinômio não constante $f(x) \in K[x]$ é irredutível em $K[x]$ se $f(x)$ não é o produto de dois polinômios em $K[x]$ de graus estritamente menores do que $\deg f(x)$.*

Polinômios irredutíveis fazem o papel de números primos para polinômios. Por exemplo, $x^2 + 1 \in \mathbb{R}[x]$ é irredutível em $\mathbb{R}[x]$, pois caso contrário ele poderia ser escrito como produto de polinômios de grau 1 em $\mathbb{R}[x]$, contradizendo o fato de $x^2 + 1 = 0$ não possuir raízes reais. Por outro lado, $x^2 + 1$ é *redutível* em $\mathbb{C}[x]$ já que $x^2 + 1 = (x - i)(x + i)$. Isto mostra que irredutibilidade é um conceito que depende do anel de polinômios sobre o qual estamos trabalhando.

Os exemplos mais evidentes de polinômios irredutíveis em $K[x]$ são os lineares mônicos, i.e., os da forma $x - a$, $a \in K$. Quando estes são os únicos polinômios irredutíveis em $K[x]$ dizemos que o corpo K é *algebricamente fechado*. Observe que em geral polinômios de graus 2 ou 3 são irredutíveis em $K[x]$ se, e somente se, não têm raízes em K .

A partir do teorema de Bachet-Bézout, como no caso dos inteiros, obtemos (c.f. proposição 1.10 e teorema 1.16):

Proposição 1.55. *Seja K um corpo e sejam $p(x), a_1(x), \dots, a_m(x) \in K[x]$ com $p(x)$ irredutível em $K[x]$. Se $p(x) \mid a_1(x) \cdot \dots \cdot a_m(x)$, então $p(x) \mid a_i(x)$ para algum i .*

Teorema 1.56 (Fatoração Única). *Seja K um corpo. Todo polinômio não nulo em $K[x]$ pode ser fatorado como um produto de polinômios irredutíveis em $K[x]$; esta fatoração é única a menos da ordem dos fatores e multiplicação por constantes não nulas.*

Outra importante consequência do teorema de Bachet-Bézout é o seguinte (c.f. teorema 1.37)

Teorema 1.57. *Seja K um corpo e $f(x)$ um polinômio irredutível em $K[x]$. Então $K[x]/(f(x))$ é um corpo.*

DEMONSTRAÇÃO: Assim como na demonstração de que $\mathbb{Z}/p\mathbb{Z}$ é um corpo para p primo, a dificuldade aqui é mostrar que todo elemento $\overline{a(x)} \neq 0$ é invertível em $K[x]/(f(x))$. Temos que $\text{mdc}(a(x), f(x)) = 1$ pois $f(x)$ é irredutível e $f(x)$ não divide $a(x)$, caso contrário teríamos $\overline{a(x)} = 0$. Logo, pelo teorema de Bachet-Bézout, existem $r(x), s(x) \in K[x]$ tais que

$$a(x)r(x) + f(x)s(x) = 1 \implies a(x)r(x) \equiv 1 \pmod{f(x)}$$

Portanto $\overline{r(x)}$ é o inverso multiplicativo de $\overline{a(x)}$. □

Por exemplo, seja $K = \mathbb{Z}/(2)$ e $f(x) = x^2 + x + \overline{1} \in K[x]$. Temos que $f(x)$ é irredutível pois ele tem grau 2 e não possui raízes em K . Assim, $K[x]/(f(x))$ é um corpo, que possui 4 elementos. As tabelas de adição e multiplicação deste corpo são as seguintes:

+	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	\overline{x}
\overline{x}	\overline{x}	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	\overline{x}	$\overline{1}$	$\overline{0}$

\cdot	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{x+1}$
\overline{x}	$\overline{0}$	\overline{x}	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	\overline{x}

Encerramos esta seção com um importante critério de irredutibilidade para polinômios com coeficientes inteiros. Primeiro, precisamos de uma

Definição 1.58. *Um polinômio não nulo $f(x) \in \mathbb{Z}[x]$ é dito primitivo se o mdc de seus coeficientes é 1.*

Lema 1.59. *O produto de dois polinômios primitivos é primitivo.*

DEMONSTRAÇÃO: Sejam $g(x)$ e $h(x)$ dois polinômios primitivos. Seja p um primo e suponha por absurdo que p divida todos os coeficientes de $g(x)h(x)$. Assim, em $\mathbb{Z}/p\mathbb{Z}[x]$ teríamos que $\overline{g(x)h(x)} = \overline{g(x)}\overline{h(x)} = \overline{0}$, onde a barra denota o polinômio obtido reduzindo-se seus coeficientes módulo p . Por outro lado, $\overline{g(x)} \neq \overline{0}$ e $\overline{h(x)} \neq \overline{0}$, já que por hipótese p não divide todos os coeficientes de $g(x)$ e o mesmo para $h(x)$. Assim, temos uma contradição pois $\mathbb{Z}/p\mathbb{Z}[x]$ é um domínio, isto é, o produto de dois polinômios não nulos em $\mathbb{Z}/p\mathbb{Z}[x]$ é diferente de zero (de fato, olhe por exemplo para os coeficientes líderes e use o fato de que $\mathbb{Z}/p\mathbb{Z}$ é um corpo). \square

O lema anterior é o passo essencial na prova do famoso *lema de Gauß*, que permite reduzir a questão da irredutibilidade de um polinômio em $\mathbb{Q}[x]$ para a mesma questão em $\mathbb{Z}[x]$.

Teorema 1.60 (Lema de Gauß). *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Então $f(x)$ é irredutível em $\mathbb{Q}[x]$ se, e somente se, $f(x)$ é irredutível em $\mathbb{Z}[x]$ (isto é, não podemos escrever $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Z}[x]$ não constantes).*

DEMONSTRAÇÃO: É claro que se $f(x)$ é irredutível sobre $\mathbb{Q}[x]$, então ele é irredutível sobre $\mathbb{Z}[x]$. Reciprocamente, suponha por contradição que $f(x)$ seja irredutível sobre $\mathbb{Z}[x]$ mas que $f(x) = g(x)h(x)$ com

$g(x), h(x) \in \mathbb{Q}[x]$, ambos não constantes. Multiplicando esta última igualdade por um inteiro conveniente $d > 0$, podemos escrever

$$d \cdot f(x) = e \cdot g_0(x)h_0(x)$$

com $g_0(x), h_0(x) \in \mathbb{Z}[x]$ primitivos e $e \in \mathbb{N}$. Como $f(x)$ e $g_0(x)h_0(x)$ (pelo lema anterior) são primitivos, temos que d é o mdc dos coeficientes de $d \cdot f(x)$, enquanto que e é o mdc dos coeficientes de $e \cdot g_0(x)h_0(x)$. Logo $d = e$ e assim $f(x) = g_0(x)h_0(x)$ é redutível sobre $\mathbb{Z}[x]$, uma contradição. \square

Finalmente, para polinômios em $\mathbb{Z}[x]$, podemos aplicar o

Proposição 1.61 (Critério de Eisenstein). *Seja $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Suponha que exista um número primo p tal que $p \nmid a_n$, $p \mid a_j$ para todo $0 \leq j < n$ e $p^2 \nmid a_0$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.*

DEMONSTRAÇÃO: Suponha por absurdo que $f(x)$ é redutível, i.e., existam $g(x), h(x) \in \mathbb{Z}[x]$ tais que $f(x) = g(x)h(x)$ e $0 < \deg g(x), \deg h(x) < n$. Em $\mathbb{Z}/p\mathbb{Z}[x]$, temos então $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, onde a barra denota o polinômio obtido reduzindo-se os seus coeficientes módulo p . Porém, como $p \mid a_j$ para todo $0 \leq j < n$, temos que $\bar{f}(x) = \bar{a}_n x^n$ e portanto, pela fatoração única em $\mathbb{Z}/p\mathbb{Z}[x]$ (teorema 1.56), devemos ter $g(x) = \bar{b}x^i$ e $h(x) = \bar{c}x^j$ com $0 < i, j < n$, $i + j = n$ e $\bar{b} \cdot \bar{c} = \bar{a}_n$. Mas isto significa que os coeficientes de x^0 em $g(x)$ e $h(x)$ são múltiplos de p , e como $f(x) = g(x)h(x)$, que a_0 é múltiplo de p^2 , absurdo. \square

Exemplo 1.62. *Seja p um primo. Demonstrar que o polinômio $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ é irredutível em $\mathbb{Q}[x]$.*

SOLUÇÃO: Pelo lema de Gauß, basta provar a irredutibilidade sobre $\mathbb{Z}[x]$ e para isto utilizaremos o critério de Eisenstein. Observemos que $f(x) = \frac{x^p - 1}{x - 1}$, logo

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}$$

e, com exceção do coeficiente líder, todos os coeficientes deste polinômio são múltiplos de p , sendo que o termo independente $\binom{p}{p-1} = p$ não é múltiplo de p^2 . Pelo critério de Eisenstein, $f(x+1)$ é irredutível em $\mathbb{Z}[x]$ e, portanto, $f(x)$ também o é. \square

Observação 1.63. *Existem polinômios primitivos irredutíveis $f(x) \in \mathbb{Z}[x]$ mas que são redutíveis módulo p para todo primo p , por exemplo $f(x) = x^4 - 10x^2 + 1$ (veja o exemplo 2.10). Por outro lado, se $f(x) \in \mathbb{Z}[x]$ admite raiz módulo p para todo primo p suficientemente grande, então $f(x)$ possui raiz em \mathbb{Z} ! Veja o excelente artigo de Serre [132] para uma demonstração deste fato.*

Problemas Propostos

1.60. *Seja $f(x) \in \mathbb{C}[x]$ um polinômio que deixa restos 10 e 1 quando dividido por $x - 1$ e $x - 10$ respectivamente. Encontrar o resto de $f(x)$ na divisão por $(x - 1)(x - 10)$.*

1.61. *Seja $\theta \in \mathbb{R}$ e n um inteiro positivo. Calcule o resto da divisão do polinômio $(\cos \theta + x \sin \theta)^n \in \mathbb{R}[x]$ por $x^2 + 1$.*

1.62. *Seja $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ um polinômio de grau n . Mostre que se p/q é uma raiz racional de $f(x)$, com $p, q \in \mathbb{Z}$ e $\text{mdc}(p, q) = 1$, então $p \mid a_0$ e $q \mid a_n$.*

1.63 (IMO1993). *Seja $f(x) = x^n + 5x^{n-1} + 3$ onde $n > 1$. Demonstrar que $f(x)$ não pode se expressar como produto de dois polinômios não constantes com coeficientes inteiros.*

1.64. *Seja α uma raiz de $x^3 - 3x + 1 = 0$. Mostre que $\alpha^2 - 2$ também é uma raiz deste polinômio.*

1.65. *Encontrar todos os pares $(c, P(x))$ onde c é um real e $P(x)$ é um polinômio não nulo tal que*

$$P(x^4 + x^2 + x) = (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)P(cx).$$

1.66 (AusPol1998). *Encontrar todos os inteiros positivos n e m tais que todas as soluções de $x^3 - 17x^2 + mx - n^2 = 0$ são inteiras.*

1.67. *Dados $x, y \in \mathbb{N}$, defina $a := x(y+1) - (y!+1)$. Mostre que imagem da função $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ dada por*

$$f(x, y) = \frac{y-1}{2} (|a^2 - 1| - (a^2 - 1)) + 2$$

é exatamente o conjunto dos números primos.

1.68. Prove a seguinte modificação do Critério de Eisenstein: seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ um polinômio primitivo não constante e sem raízes racionais. Suponha que exista um número primo p tal que $p \nmid a_n$, $p \mid a_j$ para todo $0 \leq j < n$ e $p^2 \nmid a_1$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.

1.69. (Zagier) Dado um número primo, associe a ele um polinômio cujos coeficientes são os dígitos decimais desse primo (por exemplo, $9x^3 + 4x^2 + 3$ para o primo 9403). Mostre que este polinômio é sempre irredutível em $\mathbb{Z}[x]$.

1.70. Encontrar todos os valores de k para os quais o polinômio $x^{2k+1} + x + 1$ é divisível por $x^k + x + 1$.

1.71 (IMO2002). Encontrar todos os pares de inteiros $m, n > 2$ tais que existam infinitos valores de k para os quais

$$\frac{k^m + k - 1}{k^n + k^2 - 1}$$

é inteiro.

1.9 Ordem e Raízes Primitivas

Dado $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, definimos a *ordem de \bar{a}* , denotado por $\text{ord } \bar{a}$, como o menor inteiro $t > 0$ tal que $\bar{a}^t = \bar{1}$ em $\mathbb{Z}/n\mathbb{Z}$. Se $a, n \in \mathbb{Z}$ com $\text{mdc}(a, n) = 1$, definimos a *ordem de a módulo n* , denotado por $\text{ord}_n a$, como a ordem de $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note que pelo teorema de Euler-Fermat, temos que $\text{ord}_n a \leq \varphi(n)$. Se $\text{ord}_n a = \varphi(n)$, dizemos que a é *raiz primitiva módulo n* . Por exemplo, 2 é raiz primitiva módulo 5, pois $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, que é a primeira potência de 2 congruente a 1 módulo 5 e $4 = \varphi(5)$.

O resultado básico mais importante sobre ordem é a seguinte

Proposição 1.64. Temos que $a^t \equiv 1 \pmod{n}$ se, e só se, $\text{ord}_n a \mid t$.

DEMONSTRAÇÃO: Como $a^{\text{ord}_n a} \equiv 1 \pmod{n}$, para todo $k \in \mathbb{N}$ tem-se $a^{k \text{ord}_n a} \equiv 1 \pmod{n}$. Por outro lado, se $a^t \equiv 1 \pmod{n}$, pelo algoritmo da divisão existem inteiros q e r tais que $0 \leq r < \text{ord}_n a$ e $t = q \text{ord}_n a + r$. Portanto

$$1 \equiv a^t = a^{q \text{ord}_n a + r} = (a^{\text{ord}_n a})^q \cdot a^r \equiv a^r \pmod{n}$$

Ou seja, $a^r \equiv 1 \pmod{n}$. Pela minimalidade de $\text{ord}_n a$, temos que $r = 0$, i.e., $\text{ord}_n a \mid t$. \square

Corolário 1.65. $\text{ord}_n a \mid \varphi(n)$.

Exemplo 1.66. *Demonstrar que $n \mid \varphi(a^n - 1)$ para todo inteiro positivo $a > 1$.*

SOLUÇÃO: Já que $\text{mdc}(a, a^n - 1) = 1$, pelo teorema de Euler-Fermat temos que $a^{\varphi(a^n - 1)} \equiv 1 \pmod{a^n - 1}$; por outro lado, n é a ordem de a módulo $a^n - 1$ já que $a^n \equiv 1 \pmod{a^n - 1}$ e se $0 < t < n$ temos $0 < a^t - 1 < a^n - 1$ e assim $a^n - 1 \nmid a^t - 1$. Pela proposição, temos portanto $n \mid \varphi(a^n - 1)$. \square

Exemplo 1.67. *Demonstrar que não existe um inteiro $n > 1$ tal que $n \mid 2^n - 1$.*

SOLUÇÃO: Suponhamos o contrário; seja p o menor divisor primo de n e $r = \text{ord}_p 2$. Sabemos que $2^n \equiv 1 \pmod{p}$ e além disso, pelo teorema de Fermat, $2^{p-1} \equiv 1 \pmod{p}$.

Portanto $r \mid n$ e $r \mid p - 1$, o que implica que $r \mid \text{mdc}(n, p - 1)$. Mas $\text{mdc}(n, p - 1) = 1$ pois p é o menor divisor primo de n e assim os divisores primos de $p - 1$ são menores que os divisores primos de n . Isto mostra que $r = 1$, isto é $2^1 \equiv 1 \pmod{p}$, donde $p \mid 1$, uma contradição. \square

Exemplo 1.68. *Sejam a, m e n inteiros positivos; defina m' e n' por $m = \text{mdc}(m, n) \cdot m'$ e $n = \text{mdc}(m, n) \cdot n'$, de modo que $\text{mdc}(m', n') = 1$. Mostre que*

$$\text{mdc}(a^m + 1, a^n + 1) = \begin{cases} a^{\text{mdc}(m, n)} + 1 & \text{se } m' \text{ e } n' \text{ são ímpares.} \\ 2 & \text{se } m' + n' \text{ e } a \text{ são ímpares.} \\ 1 & \text{se } m' + n' \text{ é ímpar e } a \text{ é par.} \end{cases}$$

SOLUÇÃO: Como

$$\text{mdc}(a^m + 1, a^n + 1) = \text{mdc}((a^{\text{mdc}(m, n)})^{m'} + 1, (a^{\text{mdc}(m, n)})^{n'} + 1),$$

o resultado no caso geral seguirá do caso em que $\text{mdc}(m, n) = 1$. Assim, vamos supor m e n são primos entre si e seja $d = \text{mdc}(a^n + 1, a^m + 1)$. Temos

$$\begin{aligned} \begin{cases} a^n \equiv -1 \pmod{d} \\ a^m \equiv -1 \pmod{d} \end{cases} &\implies \begin{cases} a^{2n} \equiv 1 \pmod{d} \\ a^{2m} \equiv 1 \pmod{d} \end{cases} \\ &\implies \text{ord}_d a \mid \text{mdc}(2n, 2m) = 2. \end{aligned}$$

Assim, $a^2 \equiv 1 \pmod{d}$. Digamos que m seja ímpar (como estamos supondo $\text{mdc}(m, n) = 1$, não podemos ter m e n ambos pares), de modo que

$$\begin{aligned} a \cdot (a^2)^{(m-1)/2} = a^m \equiv -1 \pmod{d} &\implies a \equiv -1 \pmod{d} \\ &\iff d \mid a + 1. \end{aligned}$$

Se n é ímpar também, então $d = a + 1$ já que $a + 1 \mid a^m + 1$ e $a + 1 \mid a^n + 1$ neste caso (utilize a fatoração $a^m + 1 = (a + 1)(a^{m-1} - a^{m-2} + a^{m-3} - \dots + 1)$ ou a implicação $a \equiv -1 \pmod{a+1} \implies a^m \equiv -1 \pmod{a+1}$). Por outro lado, se n é par, temos

$$\begin{aligned} (a^2)^{n/2} = a^n \equiv -1 \pmod{d} &\implies 1 \equiv -1 \pmod{d} \\ &\implies d = 1 \text{ ou } d = 2. \end{aligned}$$

O caso $d = 2$ ocorre se, e só se, $a^m + 1$ e $a^n + 1$ são ambos pares, ou seja, quando a é ímpar. Isto encerra a análise de casos e com isso o problema. \square

Uma outra caracterização de raiz primitiva é dada pela

Proposição 1.69. *O número a é raiz primitiva módulo n se, e somente se, $\{\bar{a}^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^\times$.*

DEMONSTRAÇÃO: Para todo $a \in \mathbb{Z}$ com $\text{mdc}(a, n) = 1$ temos $\{\bar{a}^t, t \in \mathbb{N}\} \subset (\mathbb{Z}/n\mathbb{Z})^\times$. Note que $\{\bar{a}^t, t \in \mathbb{N}\} = \{\bar{1}, \bar{a}, \bar{a}^2, \dots, \bar{a}^{\text{ord}_n a - 1}\}$ é um conjunto com $\text{ord}_n a$ elementos. De fato, para qualquer $t \in \mathbb{N}$ temos $\bar{a}^t = \bar{a}^r$ onde r é o resto na divisão de t por $\text{ord}_n a$; por outro lado, os elementos $\bar{1}, \bar{a}, \bar{a}^2, \dots, \bar{a}^{\text{ord}_n a - 1}$ são distintos pois caso $\bar{a}^i = \bar{a}^j$ com $0 \leq i < j < \text{ord}_n a$, então $\bar{a}^{j-i} = \bar{1}$ com $0 < j - i < \text{ord}_n a$, o que é absurdo.

Assim, $\{\bar{a}^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^\times$ se, e só se, $\text{mdc}(a, n) = 1$ e $\text{ord}_n a = \varphi(n)$, isto é, se, e só se, a é uma raiz primitiva módulo n . \square

Corolário 1.70. *Se m divide n e a é raiz primitiva módulo n , então a é raiz primitiva módulo m .*

DEMONSTRAÇÃO: Como o mapa natural $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ que leva $x \bmod n$ em $x \bmod m$ é sobrejetor, temos que se as potências de $a \bmod n$ cobrem todo o $(\mathbb{Z}/n\mathbb{Z})^\times$, então as potências de $a \bmod m$ também cobrem todo o $(\mathbb{Z}/m\mathbb{Z})^\times$. Pela proposição, isto implica o corolário. \square

Raízes primitivas são muito úteis em diversas questões de Teoria dos Números. Entretanto elas nem sempre existem para qualquer módulo n . O resto desta seção é dedicado a provar o seguinte importante

Teorema 1.71. *Existe alguma raiz primitiva módulo n se, e só se, $n = 2$, $n = 4$, $n = p^k$ ou $n = 2p^k$ onde p é primo ímpar.*

A demonstração deste teorema é longa e é composta de vários passos. Começamos com a seguinte

Proposição 1.72. *Se $k \geq 3$, então não existe nenhuma raiz primitiva módulo 2^k .*

DEMONSTRAÇÃO: Pelo corolário anterior, basta provar que não existe raiz primitiva módulo 8, e isso segue do fato de que se $\text{mdc}(a, 8) = 1$, isto é, $a = 2r + 1$, $r \in \mathbb{N}$, então $a^2 = 4r(r + 1) + 1 \equiv 1 \pmod{8}$ (sendo $r(r + 1)$ par, visto que é o produto de dois números consecutivos). Assim, não há elemento de ordem $\varphi(8) = 4$ módulo 8. \square

Proposição 1.73. *Se $n = ab$, com $a \geq 3$ e $b \geq 3$ inteiros tais que $\text{mdc}(a, b) = 1$, então não existe raiz primitiva módulo n .*

DEMONSTRAÇÃO: Como $\varphi(n) = \varphi(a)\varphi(b)$ e $a \geq 3$ e $b \geq 3$, segue que $\varphi(a)$ e $\varphi(b)$ são pares (verifique!). Se $\text{mdc}(k, n) = 1$, então temos

$$\begin{aligned} k^{\varphi(n)/2} &= (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod{a} & \text{e} \\ k^{\varphi(n)/2} &= (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \pmod{b}. \end{aligned}$$

Assim, $k^{\varphi(n)/2} \equiv 1 \pmod{n}$ e portanto $\text{ord}_n k \leq \varphi(n)/2 < \varphi(n)$ para todo k primo com n . \square

Proposição 1.74. *Se p é um número primo e $a \in \mathbb{Z}$ é uma raiz primitiva módulo p , então a ou $a + p$ é raiz primitiva módulo p^2 .*

DEMONSTRAÇÃO: Por hipótese, $\text{ord}_p a = \text{ord}_p(a + p) = \varphi(p) = p - 1$. Portanto $p - 1 \mid \text{ord}_{p^2} a$, pois $a^t \equiv 1 \pmod{p^2}$ implica $a^t \equiv 1 \pmod{p}$. Além disso, como $\text{ord}_{p^2} a \mid \varphi(p^2) = p(p - 1)$, devemos ter $\text{ord}_{p^2} a = p - 1$ ou $\text{ord}_{p^2} a = p(p - 1) = \varphi(p^2)$. Do mesmo modo, $\text{ord}_{p^2}(a + p) = p - 1$ ou $\text{ord}_{p^2}(a + p) = p(p - 1) = \varphi(p^2)$. Basta provar, portanto, que $\text{ord}_{p^2} a \neq p - 1$ ou $\text{ord}_{p^2}(a + p) \neq p - 1$. Suponha que $\text{ord}_{p^2} a = p - 1$. Portanto $a^{p-1} \equiv 1 \pmod{p^2}$ e assim

$$\begin{aligned} (a + p)^{p-1} &= a^{p-1} + \binom{p-1}{1} a^{p-2} p + \binom{p-1}{2} a^{p-3} p^2 + \dots \\ &\equiv 1 - pa^{p-2} \pmod{p^2}. \end{aligned}$$

Portanto $(a + p)^{p-1}$ não é congruente a 1 módulo p^2 , pois p^2 não divide pa^{p-2} (lembre-se de que $\text{mdc}(a, p) = 1$), donde $\text{ord}_{p^2}(a + p) \neq p - 1$. \square

Proposição 1.75. *Se p é um número primo ímpar e a é raiz primitiva módulo p^2 , então a é raiz primitiva módulo p^k para todo $k \in \mathbb{N}$.*

DEMONSTRAÇÃO: Como $a^{p-1} \equiv 1 \pmod{p}$, mas a^{p-1} não é congruente a 1 módulo p^2 (já que a é raiz primitiva módulo p^2), temos $a^{p-1} = 1 + b_1 p$, onde p não divide b_1 . Vamos mostrar por indução que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, onde p não divide b_k , para todo $k \geq 1$. De fato, para $k \geq 1$ e $p > 2$ primo,

$$\begin{aligned} a^{p^k(p-1)} &= (1 + b_k p^k)^p = 1 + \binom{p}{1} b_k p^k + \binom{p}{2} b_k^2 p^{2k} + \dots \\ &= 1 + p^{k+1} (b_k + pt) \end{aligned}$$

para algum $t \in \mathbb{Z}$ e assim $b_{k+1} = b_k + pt$ também não é divisível por p pois $p \nmid b_k$.

Vamos agora mostrar por indução que a é raiz primitiva módulo p^k para todo $k \geq 2$. Suponha que a seja raiz primitiva módulo p^k . Como $a^{\text{ord}_{p^{k+1}} a} \equiv 1 \pmod{p^{k+1}} \implies a^{\text{ord}_{p^{k+1}} a} \equiv 1 \pmod{p^k}$ temos

$$p^{k-1}(p - 1) = \varphi(p^k) = \text{ord}_{p^k} a \mid \text{ord}_{p^{k+1}} a \mid \varphi(p^{k+1}) = p^k(p - 1).$$

Portanto $\text{ord}_{p^{k+1}} a = p^{k-1}(p-1)$ ou $\text{ord}_{p^{k+1}} a = p^k(p-1) = \varphi(p^{k+1})$, mas o primeiro caso é impossível pois $a^{p^{k-1}(p-1)} = 1 + b_k p^k$ com $p \nmid b_k$. Logo $\text{ord}_{p^{k+1}} a = \varphi(p^{k+1})$ e a é raiz primitiva módulo p^{k+1} . \square

Por exemplo 2 é raiz primitiva módulo 5^k para todo $k \geq 1$. De fato, 2 é raiz primitiva módulo 5 e, como $2^4 = 16 \not\equiv 1 \pmod{25}$, 2 é raiz primitiva módulo $25 = 5^2$ também. Portanto, pela proposição anterior, 2 é raiz primitiva módulo 5^k para todo $k \geq 1$.

Proposição 1.76. *Se p é primo ímpar e a é um inteiro ímpar tal que a é raiz primitiva módulo p^k , então a é raiz primitiva módulo $2p^k$. Em particular, se a é raiz primitiva qualquer módulo p^k , então a ou $a + p^k$ é raiz primitiva módulo $2p^k$ (pois um deles é ímpar).*

DEMONSTRAÇÃO: Temos, como nas provas acima, $\varphi(p^k) = \text{ord}_{p^k} a \mid \text{ord}_{2p^k} a$ e $\text{ord}_{2p^k} a \mid \varphi(2p^k) = \varphi(p^k)$, logo $\text{ord}_{2p^k} a = \varphi(2p^k)$. \square

Para completar a prova do teorema 1.71, falta provar que se p é primo ímpar, então existe raiz primitiva módulo p . Para isto, precisamos de dois lemas.

Lema 1.77. $\sum_{d \mid n} \varphi(d) = n$ para todo $n \in \mathbb{N}$.

DEMONSTRAÇÃO: Seja d um divisor de n . A quantidade de a 's tais que $1 \leq a \leq n$ e $d = \text{mdc}(n, a)$ é igual a $\varphi(\frac{n}{d})$ pois $d = \text{mdc}(n, a) \iff d \mid a$ e $1 = \text{mdc}(\frac{n}{d}, \frac{a}{d})$. Como $\varphi(\frac{n}{d})$ conta justamente a quantidade de inteiros entre 1 e $\frac{n}{d}$ (inclusive) que são primos com $\frac{n}{d}$, temos que $\sum_{d \mid n} \varphi(\frac{n}{d}) = \sum_{d \mid n} \varphi(d)$ conta a quantidade de números a entre 1 e n (inclusive), particionados segundo os valores de $\text{mdc}(a, n)$. \square

Lema 1.78. *Seja p um primo e d um divisor de $p-1$. Defina $N(d)$ como a quantidade de elementos $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ com $\text{ord } \bar{a} = d$. Então $N(d) \leq \varphi(d)$.*

DEMONSTRAÇÃO: Podemos supor que $N(d) > 0$, logo existe a tal que $\text{ord}_p a = d$. Logo $\bar{a}^d = \bar{1}$ e, para $0 \leq k < d$, as classes de a^k são todas distintas módulo p . Como $(\bar{a}^k)^d = 1$ e a equação $x^d - \bar{1} = 0$ tem no

máximo d raízes distintas em $\mathbb{Z}/p\mathbb{Z}$ (pois $\mathbb{Z}/p\mathbb{Z}$ é um corpo), suas raízes são exatamente \bar{a}^k , $0 \leq k < d$. Por outro lado, se $\text{ord}_p a^k = d$, então $\text{mdc}(k, d) = 1$, pois caso $r = \text{mdc}(k, d) > 1$, então $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1 \pmod{p}$, logo $\text{ord}_p(a^k) \leq d/r < d$. Desta forma,

$$\{b \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \text{ord}_p b = d\} \subset \{\bar{a}^k \mid 0 \leq k < d \text{ e } \text{mdc}(k, d) = 1\},$$

portanto $N(d) \leq \varphi(d)$ (na verdade, os dois conjuntos acima são iguais, como ficará claro a partir da demonstração da proposição abaixo). \square

Proposição 1.79. *Se p é um primo, então existe uma raiz primitiva módulo p .*

DEMONSTRAÇÃO: Para cada $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, tem-se $\text{ord}_p a \mid p - 1$ e portanto $p - 1 = \sum_{d \mid p-1} N(d)$. Por outro lado, temos pelos dois lemas acima que

$$p - 1 = \sum_{d \mid p-1} N(d) \leq \sum_{d \mid p-1} \varphi(d) = p - 1.$$

Logo devemos ter $N(d) = \varphi(d)$ para todo d . Em particular, $N(p - 1) = \varphi(p - 1) > 0$, logo existem raízes primitivas módulo p . \square

Corolário 1.80. *Seja p um primo. Para cada $d \mid p - 1$, existem exatamente $\varphi(d)$ elementos em $(\mathbb{Z}/p\mathbb{Z})^\times$ com ordem d . Em particular, p possui exatamente $\varphi(p - 1)$ raízes primitivas.*

Com isto, encerramos a demonstração do teorema 1.71. Vejamos algumas aplicações.

Exemplo 1.81. *Mostre que existe n natural tal que os mil últimos dígitos de 2^n pertencem a $\{1, 2\}$.*

SOLUÇÃO: Observamos inicialmente que para todo $k \in \mathbb{N}$ existe um número m_k de k dígitos, todos 1 ou 2, divisível por 2^k . De fato, $m_1 = 2$ e $m_2 = 12$ satisfazem o enunciado. Seja $m_k = 2^k r_k$, $r_k \in \mathbb{N}$. Se r_k é par, tome $m_{k+1} = 2 \times 10^k + m_k = 2^{k+1}(5^k + r_k/2)$, e se r_k é ímpar, tome $m_{k+1} = 10^k + m_k = 2^{k+1}(5^k + r_k)/2$.

Como $m_{1000} \equiv 2 \pmod{10}$, 5 não divide $r_{1000} = \frac{m_{1000}}{2^{1000}}$. Portanto, como 2 é raiz primitiva módulo 5^{1000} pela proposição 1.75, existe $k \in \mathbb{N}$ com $2^k \equiv r_{1000} \pmod{5^{1000}}$. Logo $2^k = b5^{1000} + r_{1000}$ para algum $b \in \mathbb{N}$ e assim

$$2^{k+1000} = b10^{1000} + 2^{1000}r_{1000} = b10^{1000} + m_{1000},$$

e as 1000 últimas casas de 2^{k+1000} são as 1000 casas de m_{1000} , que pertencem todas a $\{1, 2\}$. \square

Observação 1.82. *Um grupo G é chamado de cíclico se existe um elemento g tal que $G = \{g^n \mid n \in \mathbb{Z}\}$. O fato de p^n e $2p^n$, p primo ímpar, admitirem raízes primitivas equivale a dizer que os grupos $(\mathbb{Z}/p^n\mathbb{Z})^\times$ e $(\mathbb{Z}/2p^n\mathbb{Z})^\times$ são cíclicos, ou ainda que há isomorfismos de grupos $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p^n)$ e $(\mathbb{Z}/2p^n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(2p^n)$ onde a operação nos grupos da direita é a adição.*

O leitor não deve ter dificuldades para adaptar a prova acima a fim de mostrar que todo corpo K com um número finito de elementos (tal como o construído no exemplo após o teorema 1.57) admite raiz primitiva, isto é, o seu grupo de unidades $K^\times = K \setminus \{0\}$ é um grupo cíclico.

Um exercício interessante que pode ser proposto a alunos muito jovens é pedir que calculem os seguintes produtos:

$$142857 \cdot 2, 142857 \cdot 3, 142857 \cdot 4, 142857 \cdot 5 \quad \text{e} \quad 142857 \cdot 6.$$

Os resultados, que são, respectivamente, 285714, 428571, 571428, 714285 e 857142 têm os mesmos dígitos que 142857, na mesma ordem cíclica. A explicação para este fato está relacionada com o resultado de $142857 \cdot 7$, que é 999999. De fato, 142857 é o período de $\frac{1}{7} = 0,142857142857 \dots$.

Temos então, por exemplo, $\frac{100}{7} = 14,285714285714285714 \dots$, donde $\frac{2}{7} = \frac{100}{7} - 14 = 0,285714285714285714 \dots$, e portanto $142857 \cdot 2 = 285714$. Isso dá certo pois 10 é raiz primitiva módulo 7, e logo, para cada $a \in \{1, 2, 3, 4, 5, 6\}$, existe um inteiro k com $0 \leq k \leq 5$ tal que $10^k \equiv a \pmod{7}$.

Em geral, se n é um inteiro positivo relativamente primo com 10, existe k inteiro positivo tal que $n \mid 10^k - 1$, o que equivale a existir

M inteiro positivo tal que $\frac{1}{n} = \frac{M}{10^k - 1} = \sum_{j=1}^{\infty} \frac{M}{10^{kj}}$. Como $M < 10^k$,

existem $a_0, a_1, \dots, a_{k-1} \in \{0, 1, \dots, 9\}$ tais que $M = \sum_{j=0}^{k-1} a_j \cdot 10^j$, e logo

$$\frac{1}{n} = 0, a_{k-1}a_{k-2} \dots a_0 a_{k-1}a_{k-2} \dots a_0 a_{k-1}a_{k-2} \dots a_0 \dots,$$

ou seja, a representação decimal de $\frac{1}{n}$ é puramente periódica com período $a_{k-1}a_{k-2} \dots a_0$. O menor período da representação decimal de $\frac{1}{n}$ tem $\text{ord}_n(10)$ dígitos. O tamanho deste menor período é $n - 1$ se, e somente se, n é primo (pois devemos ter $\varphi(n) \geq n - 1$) e 10 é raiz primitiva módulo n . Nesse caso, para todo inteiro r com $1 \leq r \leq n - 1$, existe um inteiro j com $0 \leq j \leq n - 2$ tal que 10^j deixa resto r quando dividido por n , e o mesmo fenômeno do parágrafo anterior acontece com o período de $\frac{1}{n}$. Os menores primos n com essa propriedade (*i.e.*, tais que 10 é raiz primitiva módulo n) são 7, 17, 19, 23, 29, 47, 59, 61 e 97. Para $n = 17$, por exemplo, o período de $\frac{1}{n}$ é 0588235294117647 (sugerimos ao leitor que multiplique este número por 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 e 17 e relacione os resultados com a discussão acima).

Mais geralmente, dado inteiros $B, n > 1$, o período de $\frac{1}{n}$ na base B tem $n - 1$ algarismos se, e somente se, n é primo e B é raiz primitiva módulo n . Dado n primo, sempre existem inteiros positivos B com essa propriedade (a qual só depende da classe de congruência de B módulo n). Nesse caso, o período de $\frac{1}{n}$ na base B (que é o número $\frac{B^{n-1}-1}{n}$), quando multiplicado por $1, 2, 3, \dots, n - 1$, terá representações em base B que serão permutações uma da outra, e com a mesma ordem cíclica.

Por outro lado, não se sabe se existem infinitos primos n tais que 10 é raiz primitiva módulo n . Isso seria consequência da conjectura de Artin, segundo a qual, dado qualquer inteiro a que não pertença a $\{-1, 0, 1\}$ nem seja quadrado perfeito, existem infinitos primos p tais que a é raiz primitiva módulo p , e, mais ainda, existe uma constante $C(a) > 0$ tal que, se $N_a(x)$ denota o número de tais primos que são menores ou iguais a x , e $\pi(x)$ denota o número total de primos $p \leq x$, então $\lim_{x \rightarrow +\infty} \frac{N_a(x)}{\pi(x)} = C(a)$. Conjectura-se que essa constante $C(a)$ seja sempre um múltiplo racional da constante de Artin $C = \prod_{p \text{ primo}} (1 - \frac{1}{p(p-1)})$.

Mais precisamente, escrevemos $a = a_1 \cdot b^2$, com $b \geq 1$ máximo (a_1 é a parte livre de quadrados de a : se $n \geq 1$ e $n^2 \mid a$ então $n = 1$). Tomamos

$h \geq 1$ máximo tal que $a = c^h$ para algum c inteiro. Definimos

$$\tilde{C}(h) = \prod_{\substack{q \text{ primo} \\ q|h}} \left(1 - \frac{1}{q-1}\right) \prod_{\substack{q \text{ primo} \\ q \nmid h}} \left(1 - \frac{1}{q(q-1)}\right).$$

Temos então:

- Se $a_1 \not\equiv 1 \pmod{4}$ então $C(a) = \tilde{C}(h)$.
- Se $a_1 \equiv 1 \pmod{4}$ então

$$C(a) = \tilde{C}(h) \left(1 - (-1)^{|\{p \text{ primo}; p|a_1\}|}\right) \prod_{\substack{q \text{ primo} \\ q|h, q|a_1}} \frac{1}{q-2} \prod_{\substack{q \text{ primo} \\ q \nmid h, q|a_1}} \frac{1}{q^2 - q - 1}.$$

Esta conjectura foi provada condicionalmente por Hooley em [72], assumindo a chamada *Hipótese de Riemann Estendida*, uma generalização da famosa *Hipótese de Riemann*. Por outro lado, Heath-Brown provou incondicionalmente em [71] que há no máximo três inteiros positivos livres de quadrados que são raiz primitiva módulo apenas um número finito de primos.

Problemas Propostos

1.72. *Encontrar as ordens de 2 e 5 módulo 101. Encontrar também todos os elementos de ordem 20 em $(\mathbb{Z}/101\mathbb{Z})^\times$.*

1.73. *Determine um elemento de $(\mathbb{Z}/99\mathbb{Z})^\times$ de ordem 30.*

1.74. *Determine todos os valores de n para os quais $|(\mathbb{Z}/n\mathbb{Z})^\times| = 24$.*

1.75. *Determine um gerador de $(\mathbb{Z}/242\mathbb{Z})^\times$.*

1.76. *Demonstrar que $2n \mid \varphi(a^n + 1)$ para todo inteiro positivo a .*

1.77 (IMO1978). *Sejam m e n inteiros positivos com $m < n$. Se os três últimos dígitos de 1978^m são os mesmos que os três últimos dígitos de 1978^n , encontrar m e n tais que $m + n$ assume o menor valor possível.*

1.78. *Sejam d e n números naturais tais que $d \mid 2^{2^n} + 1$. Demonstre que existe um inteiro k tal que $d = k \cdot 2^{n+1} + 1$.*

1.79. Seja $k \geq 2$ e $n_1, n_2, \dots, n_k \geq 1$ números naturais que tem a propriedade

$$n_2 \mid (2^{n_1} - 1), \quad n_3 \mid (2^{n_2} - 1), \dots, n_k \mid (2^{n_{k-1}} - 1) \text{ e } n_1 \mid (2^{n_k} - 1)$$

Demonstrar que $n_1 = n_2 = \dots = n_k = 1$.

1.80. Mostrar que $x^3 - x + 1$ é irredutível em $\mathbb{Z}/3\mathbb{Z}[x]$. Encontrar todas as raízes primitivas do corpo finito $\frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^3 - x + 1)}$.

1.81 (Teorema de Lagrange). Seja G um grupo com número finito de elementos. Seja H um subgrupo de G , i.e., um subconjunto de G tal que $a, b \in H \implies a \cdot b \in H$ e $a \in H \implies a^{-1} \in H$, de modo que o produto de G se restringe a H e faz de H um grupo também.

(a) Mostre que os subconjuntos de G do tipo

$$g \cdot H \stackrel{\text{def}}{=} \{g \cdot h \mid h \in H\}$$

formam uma partição de G , ou seja, todo elemento de G pertence a algum $g \cdot H$ e que se $g_1 \cdot H \cap g_2 \cdot H \neq \emptyset$, então $g_1 \cdot H = g_2 \cdot H$.

(b) Mostre que $|g_1 \cdot H| = |g_2 \cdot H|$ para quaisquer $g_1, g_2 \in G$ e que portanto $|H|$ divide $|G|$ (teorema de Lagrange).

(c) Seja $g \in G$. Mostre que existe $t > 0$ tal que $g^t = e$. Se $\text{ord } g$ é o menor t positivo com esta propriedade, mostre que

$$H = \{g^n \mid n \in \mathbb{N}\}$$

é um subgrupo de G com $\text{ord } g$ elementos.

(d) Aplicando o teorema de Lagrange ao subgrupo do item anterior, prove que $g^{|G|} = e$ para todo $g \in G$. Observe que isto fornece uma nova prova do teorema de Euler-Fermat no caso em que $G = (\mathbb{Z}/(n))^\times$.

1.82 (APMO1997). Encontrar um n no conjunto $\{100, 101, \dots, 1997\}$ tal que n divide $2^n + 2$.

1.83. Definimos a função de Carmichael $\lambda: \mathbb{N} \rightarrow \mathbb{N}$ como o menor inteiro positivo tal que $a^{\lambda(n)} \equiv 1 \pmod{n}$ para todo a primo com n . Observe que, pelo teorema 1.71, $\lambda(p^l) = p^{l-1}(p-1)$ para todo p primo ímpar. Mostrar que

(a) $\lambda(2) = 1$, $\lambda(4) = 2$ e $\lambda(2^l) = 2^{l-2}$ para todo $l \geq 3$.

(b) Se $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ é a fatoração em primos de n , então

$$\lambda(n) = \text{mmc}\{\lambda(p_1^{\alpha_1}), \dots, \lambda(p_k^{\alpha_k})\}.$$

1.84. Prove que existem infinitos inteiros positivos n tais que $n \mid 4^n + 1$.

1.85 (IMO2000). Existe um inteiro N divisível por exatamente 2000 primos diferentes e tal que N divide $2^N + 1$?

1.86 (IMO1990). Encontrar todos os números naturais n tais que $n^2 \mid 2^n + 1$.

1.87 (IMO1999). Encontrar todos os pares (n, p) de inteiros positivos tais que p é primo, $n \leq 2p$ e $(p-1)^n + 1$ é divisível por n^{p-1} .

1.88 (Banco-IMO2000). Determine todas as triplas (a, m, n) de inteiros positivos tais que $a^m + 1 \mid (a+1)^n$.

1.89 (OBM2012). Qual é o menor natural n para o qual existe k natural de modo que os 2012 últimos dígitos na representação decimal de n^k são iguais a 1?

Capítulo 2

Equações Módulo m

Neste capítulo estudaremos equações do tipo

$$f(x) \equiv 0 \pmod{m}$$

na variável x , onde $f(x)$ é um polinômio com coeficientes inteiros.

2.1 Equações Lineares Módulo m

Se $\text{mdc}(a, m) = 1$, como a é invertível módulo m , a equação

$$ax \equiv b \pmod{m},$$

tem solução única módulo m , dada por $x \equiv a^{\varphi(m)-1}b \pmod{m}$ (utilizando o teorema de Euler-Fermat para encontrar o inverso de $\bar{a} \in \mathbb{Z}/(m)$). Assim, todas as soluções da equação acima são da forma $x = a^{\varphi(m)-1}b + km$ onde $k \in \mathbb{Z}$. No caso geral, se $\text{mdc}(a, m) = d > 1$ temos que

$$ax \equiv b \pmod{m} \implies ax \equiv b \pmod{d} \iff b \equiv 0 \pmod{d}.$$

Logo uma condição necessária para que a congruência linear $ax \equiv b \pmod{m}$ tenha solução é que $d \mid b$. Esta condição é também suficiente, já que escrevendo $a = da'$, $b = db'$ e $m = dm'$, temos que

$$ax \equiv b \pmod{m} \iff a'x \equiv b' \pmod{m'}.$$

Como $\text{mdc}(a', m') = 1$, há uma única solução $(a')^{\varphi(m')-1}b'$ módulo m' , isto é, há d soluções distintas módulo m , a saber $x \equiv (a')^{\varphi(m')-1}b' +$

$km' \pmod{m}$ com $0 \leq k < d$. Note ainda que como resolver $ax \equiv b \pmod{m}$ é equivalente a resolver a equação diofantina linear $ax + my = b$, poderíamos também ter utilizado o teorema de Bachet-Bézout e o algoritmo de Euclides para encontrar as soluções desta congruência linear como no exemplo 1.14. Resumimos esta discussão na seguinte

Proposição 2.1. *A congruência linear*

$$ax \equiv b \pmod{m}$$

admite solução se, e somente se, $\text{mdc}(a, m) \mid b$. Neste caso, há exatamente $\text{mdc}(a, m)$ soluções distintas módulo m .

Agora queremos encontrar condições para que um sistema de congruências lineares tenha solução. O seguinte teorema nos garante a existência de tais soluções.

Teorema 2.2 (Teorema Chinês dos Restos). *Se b_1, b_2, \dots, b_k são inteiros quaisquer e a_1, a_2, \dots, a_k são primos relativos dois a dois, o sistema de equações*

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

admite solução, que é única módulo $A = a_1 a_2 \dots a_k$.

DEMONSTRAÇÃO: Daremos duas provas do teorema chinês dos restos. Para a primeira, consideremos os números $M_i = \frac{A}{a_i}$. Como $\text{mdc}(a_i, M_i) = 1$, logo existe X_i tal que $M_i X_i \equiv 1 \pmod{a_i}$. Note que se $j \neq i$ então M_j é múltiplo de a_i e portanto $M_j X_j \equiv 0 \pmod{a_i}$. Assim, temos que

$$x_0 = M_1 X_1 b_1 + M_2 X_2 b_2 + \dots + M_k X_k b_k$$

é solução do sistema de equações, pois $x_0 \equiv M_i X_i b_i \equiv b_i \pmod{a_i}$. Além disso, se x_1 é outra solução, então $x_0 \equiv x_1 \pmod{a_i} \iff a_i \mid$

$x_0 - x_1$ para todo a_i , e como os a_i 's são dois a dois primos, temos que $A \mid x_0 - x_1 \iff x_0 \equiv x_1 \pmod{A}$, mostrando a unicidade módulo A .

Para a segunda prova, considere o mapa natural

$$\begin{aligned} f: \mathbb{Z}/(A) &\rightarrow \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_k) \\ b \bmod A &\mapsto (b \bmod a_1, b \bmod a_2, \dots, b \bmod a_k). \end{aligned}$$

Note que este mapa está bem definido, isto é, o valor de $f(b \bmod A)$ independe da escolha do representante da classe de $b \bmod A$, pois quaisquer dois representantes diferem de um múltiplo de A , que tem imagem $(0 \bmod a_1, \dots, 0 \bmod a_k)$ no produto $\mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_k)$. Observe agora que o teorema chinês dos restos é equivalente a mostrar que f é uma bijeção: o fato de f ser sobrejetor corresponde à existência da solução do sistema, enquanto que o fato de f ser injetor corresponde à unicidade módulo A . Como o domínio e o contradomínio de f têm mesmo tamanho (ambos têm A elementos), para mostrar que f é uma bijeção basta mostrarmos que f é injetora. Suponha que $f(b_1 \bmod A) = f(b_2 \bmod A)$, então $b_1 \equiv b_2 \pmod{a_i}$ para todo i , e como na primeira demonstração temos que isto implica $b_1 \equiv b_2 \pmod{A}$, o que encerra a prova. \square

Observação 2.3. Como

$$\text{mdc}(b, a_1 a_2 \dots a_k) = 1 \iff (\forall j \leq k, \text{mdc}(b, a_j) = 1),$$

a bijeção f definida na segunda prova do teorema anterior satisfaz

$$f((\mathbb{Z}/(A))^\times) = (\mathbb{Z}/(a_1))^\times \times (\mathbb{Z}/(a_2))^\times \times \cdots \times (\mathbb{Z}/(a_k))^\times.$$

Em particular, isso nos dá uma nova prova de que

$$\varphi(a_1 a_2 \dots a_k) = \varphi(a_1) \varphi(a_2) \cdots \varphi(a_k)$$

sempre que $\text{mdc}(a_i, a_j) = 1$ para quaisquer i e j .

Por exemplo, para $k = 2$, $a_1 = 3$ e $a_2 = 5$, temos a seguinte tabela, que mostra, para cada i e j com $0 \leq i < 3$ e $0 \leq j < 5$, a única solução x com $0 \leq x < 3 \cdot 5 = 15$ tal que $x \equiv i \pmod{3}$ e $x \equiv j \pmod{5}$:

	0 mod 5	1 mod 5	2 mod 5	3 mod 5	4 mod 5
0 mod 3	0	6	12	3	9
1 mod 3	10	1	7	13	4
2 mod 3	5	11	2	8	14

Vejamos algumas aplicações.

Exemplo 2.4. *Um inteiro é livre de quadrados se ele não é divisível pelo quadrado de nenhum número inteiro maior do que 1. Demonstrar que existem intervalos arbitrariamente grandes de inteiros consecutivos, nenhum dos quais é livre de quadrados.*

SOLUÇÃO: Seja n um número natural qualquer. Sejam p_1, \dots, p_n primos distintos. O teorema chinês dos restos nos garante que o sistema

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2} \\ x &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -n \pmod{p_n^2} \end{aligned}$$

tem solução. Se x_0 é uma solução positiva do sistema, então cada um dos números $x_0 + 1, x_0 + 2, \dots, x_0 + n$ é divisível pelo quadrado de um inteiro maior do que 1, logo nenhum deles é livre de quadrados. \square

Exemplo 2.5. *Seja $P(x)$ um polinômio não constante com coeficientes inteiros. Demonstrar que para todo inteiro n , existe um inteiro i tal que*

$$P(i), P(i+1), P(i+2), \dots, P(i+n)$$

são números compostos.

SOLUÇÃO: Demonstraremos primeiro o seguinte

Lema 2.6. *Seja $P(x)$ um polinômio não constante com coeficientes inteiros. Para todo par de inteiros k, i , tem-se que $P(i) \mid P(kP(i) + i)$.*

DEMONSTRAÇÃO: Dado que $(kP(i) + i)^n \equiv i^n \pmod{P(i)}$ para todo n inteiro não negativo, é fácil ver que $P(kP(i) + i) \equiv P(i) \equiv 0 \pmod{P(i)}$. \square

Suponhamos por contradição que, para cada i , o conjunto $\{P(i), P(i+1), \dots, P(i+n)\}$ contenha um número primo. Então a sequência $(P(i))_{i \geq 1}$ assume infinitos valores primos. Consideremos os $n+1$ primos distintos $P(i_0), P(i_1), \dots, P(i_n)$. Pelo teorema chinês dos restos segue que existem infinitas soluções x do sistema de equações

$$x \equiv i_0 \pmod{P(i_0)}$$

$$x \equiv i_1 - 1 \pmod{P(i_1)}$$

$$x \equiv i_2 - 2 \pmod{P(i_2)}$$

$$\vdots$$

$$x \equiv i_n - n \pmod{P(i_n)}$$

onde, se x_0 é uma solução, então $x = x_0 + k(P(i_0) \cdots P(i_n))$ também é solução para todo $k \geq 0$. Assim, pelo lema anterior, podemos dizer que $P(x), P(x+1), \dots, P(x+n)$ são números compostos quando k é suficientemente grande, múltiplos respectivamente de $P(i_0), P(i_1), \dots, P(i_n)$. \square

Exemplo 2.7. *Uma potência não trivial é um número da forma m^k , onde m, k são inteiros maiores do que ou iguais a 2. Dado $n \in \mathbb{N}$, prove que existe um conjunto $A \subset \mathbb{N}$ com n elementos tal que para todo subconjunto $B \subset A$ não vazio, $\sum_{x \in B} x$ é uma potência não trivial. Em outras palavras, se $A = \{x_1, x_2, \dots, x_n\}$ então todas as somas $x_1, x_2, \dots, x_n, x_1 + x_2, x_1 + x_3, \dots, x_{n-1} + x_n, \dots, x_1 + x_2 + \dots + x_n$ são potências não triviais.*

SOLUÇÃO: Vamos provar a existência de um tal conjunto por indução em n . Para $n = 1$, $A = \{4\}$ é solução e, para $n = 2$, $A = \{9, 16\}$ é solução. Suponha agora que $A = \{x_1, \dots, x_n\}$ é um conjunto com n elementos e para todo $B \subset A$, $B \neq \emptyset$, $\sum_{x \in B} x = m_B^{k_B}$. Vamos mostrar

que existe $c \in \mathbb{N}$ tal que o conjunto $\tilde{A} = \{cx_1, cx_2, \dots, cx_n, c\}$ satisfaz o enunciado. Seja $\lambda = \text{mmc}\{k_B \mid B \subset A, B \neq \emptyset\}$, o mínimo múltiplo comum de todos os expoentes k_B . Para cada $B \subset A$, $B \neq \emptyset$, associamos um número primo $p_B > \lambda$, de forma que $B_1 \neq B_2$ implica $p_{B_1} \neq p_{B_2}$.

Pelo teorema chinês dos restos existe um natural r_B com

$$\begin{aligned} r_B &\equiv 0 \pmod{p_X} \text{ para todo subconjunto } X \subset A, X \neq B \\ \lambda \cdot r_B &\equiv -1 \pmod{p_B}. \end{aligned}$$

(λ é invertível módulo p_B). Tomemos

$$c = \prod_{\substack{X \subset A \\ X \neq \emptyset}} (1 + m_X^{k_X})^{\lambda r_X}$$

e vamos mostrar que $\tilde{A} = \{cx_1, cx_2, \dots, cx_n, c\}$ continua a satisfazer as condições do enunciado.

Dado $B' \subset \{cx_1, cx_2, \dots, cx_n\}$, temos que $B' = \{cx \mid x \in B\}$ para algum $B \subset A$. Como c é uma potência λ -ésima, c também é uma potência k_B -ésima, portanto, $\sum_{x \in B'} x = cm_B^{k_B}$ será uma potência k_B -ésima para todo $B' \neq \emptyset$. Além disso, para subconjuntos de \tilde{A} da forma $B' \cup \{c\}$, temos

$$\sum_{x \in B' \cup \{c\}} x = c \cdot (1 + m_B^{k_B}) = \left(\prod_{\substack{X \subset A \\ X \neq \emptyset, B}} (1 + m_X^{k_X})^{\lambda r_X} \right) (1 + m_B^{k_B})^{\lambda r_B + 1},$$

que é uma potência p_B -ésima, pois $\lambda r_B + 1$ e r_X ($X \neq B$) são múltiplos de p_B . \square

Problemas Propostos

2.1. Resolver as equações lineares

(a) $7x \equiv 12 \pmod{127}$

(b) $12x \equiv 5 \pmod{122}$

(c) $40x \equiv 64 \pmod{256}$

2.2. Resolver o sistema de congruências lineares

$$x \equiv 0 \pmod{7}$$

$$x \equiv 1 \pmod{12}$$

$$x \equiv -5 \pmod{17}$$

2.3. Determine um valor de s tal que $1024s \equiv 1 \pmod{2011}$ e calcule o resto da divisão de 2^{2000} por 2011.

2.4. Um inteiro positivo n é chamado de auto-replicante se os últimos dígitos de n^2 formam o número n . Por exemplo, 25 é auto-replicante pois $25^2 = 625$. Determine todos os números auto-replicantes com exatamente 4 dígitos.

2.5. Sejam $a, n \in \mathbb{N}_{>0}$ e considere a sequência (x_k) definida por $x_1 = a$, $x_{k+1} = a^{x_k}$ para todo $k \in \mathbb{N}$. Demonstrar que existe $N \in \mathbb{N}$ tal que $x_{k+1} \equiv x_k \pmod{n}$ para todo $k \geq N$.

2.6. Demonstrar que o sistema de equações

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

tem solução se, e só se, para todo i e j , $\text{mdc}(a_i, a_j) \mid (b_i - b_j)$. (No caso particular em que $\text{mdc}(a_i, a_j) = 1$, o problema se reduz ao teorema chinês dos restos).

2.7. Demonstrar que, para k e n números naturais, é possível encontrar k números consecutivos, cada um dos quais tem ao menos n divisores primos diferentes.

2.8. Demonstrar que se a , b e c são três inteiros diferentes, então existem infinitos valores de n para os quais $a + n$, $b + n$ e $c + n$ são primos relativos.

2.9. Demonstrar que para todo inteiro positivo m e todo número par $2k$, este último pode ser escrito como a diferença de dois inteiros positivos, cada um dos quais é primo relativo com m .

2.10. Demonstrar que existem progressões aritméticas de comprimento arbitrário formadas por inteiros positivos tais que cada termo é a potência de um inteiro positivo com expoente maior do que 1.

2.11 (Olimpíada de Maio 2013). É possível escrever 100 números ímpares numa fila de tal forma que a soma de cada 5 adjacentes seja um quadrado perfeito e que a soma de cada 9 números adjacentes também seja um quadrado perfeito

2.2 Congruências de Grau 2

Seja $p > 2$ um número primo e $a, b, c \in \mathbb{Z}$ com a não divisível por p . Resolver a equação quadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

é o mesmo que resolver (completando quadrados)

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

(note que 2 e a são invertíveis módulo p). Assim, estamos interessados em encontrar critérios de existência de soluções da equação

$$X^2 \equiv d \pmod{p}.$$

Se a equação acima admite solução (i.e. se \bar{d} é um “quadrado perfeito” em $\mathbb{Z}/p\mathbb{Z}$) então dizemos que d é um *resíduo ou resto quadrático* módulo p . Há exatamente $(p+1)/2$ resíduos quadráticos módulo p , a saber

$$0^2, 1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod{p}$$

já que todo inteiro x é congruente a $\pm i \pmod{p}$ para algum i tal que $0 \leq i \leq (p-1)/2$, de modo que x^2 é congruente a um dos números da lista acima. Note que módulo p estes números são todos distintos: de fato, temos que

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} &\implies p \mid (i-j)(i+j) \\ &\iff p \mid i-j \text{ ou } p \mid i+j \\ &\iff i \equiv \pm j \pmod{p} \end{aligned}$$

Mas como $0 \leq i, j \leq (p-1)/2 \implies 0 < i+j \leq p-1$ ou $i = j = 0$, temos que a única possibilidade é $i \equiv j \pmod{p}$.

Embora saibamos a lista completa dos resíduos quadráticos, na prática pode ser difícil reconhecer se um número é ou não resíduo quadrático. Por exemplo, você sabe dizer se 2 é resíduo quadrático módulo 1019? Veremos a seguir o teorema da reciprocidade quadrática, que permite responder estas questões de maneira bastante eficiente.

2.2.1 Resíduos Quadráticos e Símbolo de Legendre

Seja $p > 2$ um número primo e a um inteiro qualquer. Para simplificar cálculos e notações definiremos o chamado *símbolo de Legendre*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ 0 & \text{se } p \mid a \\ -1 & \text{caso contrário} \end{cases}$$

Proposição 2.8 (Critério de Euler). *Seja $p > 2$ um primo e a um inteiro qualquer. Então*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

DEMONSTRAÇÃO: Para $a \equiv 0 \pmod{p}$ o resultado é claro, de modo que podemos supor $p \nmid a$. Pelo teorema de Fermat temos que $a^{p-1} \equiv 1 \pmod{p}$, donde

$$\begin{aligned} (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) &\equiv 0 \pmod{p} \iff p \mid a^{\frac{p-1}{2}} - 1 \text{ ou } p \mid a^{\frac{p-1}{2}} + 1 \\ &\iff a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}. \end{aligned}$$

Assim, devemos mostrar que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se, e só se, a é um resíduo quadrático módulo p .

Se a é um resíduo quadrático, digamos $a \equiv i^2 \pmod{p}$, novamente pelo teorema de Fermat temos que

$$a^{\frac{p-1}{2}} \equiv i^{p-1} \equiv 1 \pmod{p}.$$

Assim, os resíduos quadráticos $1^2, 2^2, \dots, (\frac{p-1}{2})^2$ módulo p são raízes do polinômio $f(x) = x^{\frac{p-1}{2}} - 1$ em $\mathbb{Z}/(p)[x]$. Mas $\mathbb{Z}/(p)$ é corpo, logo $f(x)$ pode ter no máximo $\deg f = (p-1)/2$ raízes em $\mathbb{Z}/(p)$. Isto mostra que as raízes de $f(x)$ são exatamente os resíduos quadráticos não congruentes a zero módulo p e que, portanto, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se, e só se, a é um resíduo quadrático módulo p . \square

Corolário 2.9. *O símbolo de Legendre possui as seguintes propriedades:*

1. se $a \equiv b \pmod{p}$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a^2}{p}\right) = 1$ se $p \nmid a$.
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, ou seja, -1 é resíduo quadrático módulo p se, e só se, $p \equiv 1 \pmod{4}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

DEMONSTRAÇÃO: Os itens 1 e 2 são imediatos a partir da definição e 3 segue do critério de Euler: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \implies \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ já que $p > 2$ e ambos os lados da congruência são iguais a ± 1 . Da mesma forma, aplicando o critério de Euler temos que

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p},$$

o que mostra que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, pois novamente ambos os lados da congruência são iguais a ± 1 . \square

Exemplo 2.10. *Mostre que o polinômio $f(x) = x^4 - 10x^2 + 1$ é irreduzível em $\mathbb{Z}[x]$, mas é redutível módulo p para todo primo p .*

SOLUÇÃO: Vejamos que $f(x)$ é irreduzível em $\mathbb{Z}[x]$. Observe inicialmente que as raízes de $f(x)$ são todas irracionais: se $p, q \in \mathbb{Z}$ são tais que $\text{mdc}(p, q) = 1$ e $f(p/q) = 0 \iff p^4 - 10p^2q^2 + q^4 = 0$, temos da última igualdade que $q \mid p^4 \implies q = \pm 1$ e $p \mid q^4 \implies p = \pm 1$ já que p e q são primos entre si, logo $p/q = \pm 1$, nenhuma das quais é raiz de $f(x)$ (cujos zeros são $\pm\sqrt{2} \pm \sqrt{3}$).

Logo se $f(x)$ for redutível ele é o produto de dois polinômios de grau 2, que podemos supor mônicos. Como o produto dos coeficientes independentes destes dois fatores deve ser igual ao coeficiente independente de $f(x)$, que é 1, temos apenas duas possibilidades:

$$\begin{aligned} f(x) &= (x^2 + ax + 1)(x^2 + bx + 1) && \text{ou} \\ f(x) &= (x^2 + ax - 1)(x^2 + bx - 1) \end{aligned}$$

com $a, b \in \mathbb{Z}$. Em ambos os casos, temos $a + b = 0$ (coeficiente de x^3). Logo, no primeiro caso, comparando o coeficiente de x^2 temos $ab + 2 = -10 \iff a^2 = 12$, o que é impossível. O segundo caso é análogo.

Agora, para $p = 2$ e $p = 3$ temos

$$f(x) \equiv (x + 1)^4 \pmod{2} \quad \text{e} \quad f(x) \equiv (x^2 + 1)^2 \pmod{3}.$$

Agora se $p > 3$ é um primo, temos que ou $\left(\frac{2}{p}\right) = 1$, ou $\left(\frac{3}{p}\right) = 1$ ou $\left(\frac{6}{p}\right) = 1$ já que $\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{6}{p}\right)$. No primeiro caso, se $a^2 \equiv 2 \pmod{p}$ temos

$$f(x) \equiv (x^2 + 2ax - 1)(x^2 - 2ax - 1) \pmod{p}.$$

Já no segundo caso, se $b^2 \equiv 3 \pmod{p}$ temos

$$f(x) \equiv (x^2 + 2bx + 1)(x^2 - 2bx + 1) \pmod{p}.$$

Finalmente, no último caso, se $c^2 \equiv 6 \pmod{p}$ temos

$$f(x) \equiv (x^2 + 2c - 5)(x^2 - 2c - 5) \pmod{p}.$$

Isto mostra que $f(x)$ é redutível módulo p para todo primo p . □

2.2.2 Lei de Reciprocidade Quadrática

O critério de Euler já nos fornece uma maneira de identificar resíduos quadráticos. Entretanto, vamos provar um resultado muito mais forte, que é a famosa

Teorema 2.11 (Reciprocidade Quadrática).

1. *Sejam p e q primos ímpares distintos. Então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

2. *Seja p um primo ímpar. Então*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{8} \\ -1 & \text{se } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Antes de apresentar a prova, vejamos algumas aplicações.

Exemplo 2.12. *Determinar se -90 é resíduo quadrático módulo 1019 ou não.*

SOLUÇÃO:

$$\begin{aligned} \left(\frac{-90}{1019}\right) &= \left(\frac{-1}{1019}\right) \left(\frac{2}{1019}\right) \left(\frac{3^2}{1019}\right) \left(\frac{5}{1019}\right) \\ &= (-1) \cdot (-1) \cdot 1 \cdot \left(\frac{1019}{5}\right) \\ &= \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1. \end{aligned}$$

Ou seja, -90 é resíduo quadrático módulo 1019. \square

Exemplo 2.13. *Seja p um número primo. Mostre que*

1. *se p é da forma $4n + 1$ então $p \mid n^n - 1$.*
2. *se p é da forma $4n - 1$ então $p \mid n^n + (-1)^{n+1} \cdot 2n$.*

SOLUÇÃO: No primeiro item, $4n \equiv -1 \pmod{p}$, donde elevando a n obtemos

$$(4n)^n = 2^{2n} n^n \equiv (-1)^n \pmod{p}.$$

Por outro lado, pelo critério de Euler e pela reciprocidade quadrática temos

$$2^{2n} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \equiv (-1)^{n(2n+1)} \equiv (-1)^n \pmod{p}.$$

Portanto $n^n \equiv 1 \pmod{p}$, como queríamos demonstrar.

No segundo item, temos $4n \equiv 1 \pmod{p}$ e assim

$$(4n)^n = 2^{2n} n^n \equiv 1 \pmod{p},$$

mas $2^{2n-1} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} = (-1)^{n(2n-1)} \pmod{p}$, donde $2^{2n} \equiv 2 \cdot (-1)^n \pmod{p}$. Concluimos que $2n^n \equiv (-1)^n \pmod{p}$ e multiplicando por $2n$ e utilizando $4n \equiv 1 \pmod{p}$ obtemos $n^n \equiv 2n \cdot (-1)^n \pmod{p}$, como desejado. \square

O primeiro passo da demonstração da lei de reciprocidade quadrática é o seguinte

Lema 2.14 (Gauß). *Sejam $p > 2$ um número primo e a um inteiro positivo primo relativo com p . Seja s o número de elementos do conjunto*

$$\left\{a, 2a, 3a, \dots, \frac{p-1}{2} \cdot a\right\}$$

tais que seu resto módulo p é maior do que $\frac{p-1}{2}$. Então

$$\left(\frac{a}{p}\right) = (-1)^s.$$

DEMONSTRAÇÃO: A ideia é imitar a prova do teorema de Euler-Fermat. Como o conjunto $\{\pm 1, \pm 2, \dots, \pm \frac{p-1}{2}\}$ é um sistema completo de invertíveis módulo p , para cada $j = 1, 2, \dots, \frac{p-1}{2}$ podemos escrever $a \cdot j \equiv \epsilon_j m_j \pmod{p}$ com $\epsilon_j \in \{-1, 1\}$ e $m_j \in \{1, 2, \dots, \frac{p-1}{2}\}$. Temos que se $i \neq j$ então $m_i \neq m_j$ donde $\{m_1, m_2, \dots, m_{\frac{p-1}{2}}\} = \{1, 2, \dots, \frac{p-1}{2}\}$. De fato, se $m_i = m_j$ temos $a \cdot i \equiv a \cdot j \pmod{p}$ ou $a \cdot i \equiv -a \cdot j \pmod{p}$; como a é invertível módulo p e $0 < i, j \leq (p-1)/2$, temos que a primeira possibilidade implica $i = j$ e a segunda é impossível. Assim, multiplicando as congruências $a \cdot j \equiv \epsilon_j m_j \pmod{p}$, obtemos

$$\begin{aligned} (a \cdot 1)(a \cdot 2) \cdots (a \cdot \frac{p-1}{2}) &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} m_1 m_2 \cdots m_{\frac{p-1}{2}} \pmod{p} \\ a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \\ \iff \left(\frac{a}{p}\right) &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} \pmod{p}, \end{aligned}$$

donde $\left(\frac{a}{p}\right) = \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}}$, pois ambos os lados pertencem a $\{-1, 1\}$. Assim, $\left(\frac{a}{p}\right) = (-1)^s$ já s é o número de elementos j de $\{1, 2, \dots, \frac{p-1}{2}\}$ tais que $\epsilon_j = -1$. \square

O lema de Gauß já nos permite provar a fórmula para $\left(\frac{2}{p}\right)$. Se $p \equiv 1 \pmod{4}$, digamos $p = 4k + 1$, temos $\frac{p-1}{2} = 2k$. Como $1 \leq 2j \leq \frac{p-1}{2}$ para $j \leq k$ e $\frac{p-1}{2} < 2j \leq p-1$ para $k+1 \leq j \leq 2k$, temos

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} 1, & \text{se } p \equiv 1 \pmod{8}, \\ -1, & \text{se } p \equiv 5 \pmod{8}. \end{cases}$$

Se $p \equiv 3 \pmod{4}$, digamos $p = 4k + 3$, temos $\frac{p-1}{2} = 2k + 1$. Para $1 \leq j \leq k$ temos $1 \leq 2j \leq \frac{p-1}{2}$ e para $k+1 \leq j \leq 2k+1$ temos $\frac{p-1}{2} < 2j \leq p-1$, donde

$$\left(\frac{2}{p}\right) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod{8}, \\ 1, & \text{se } p \equiv 7 \pmod{8}. \end{cases}$$

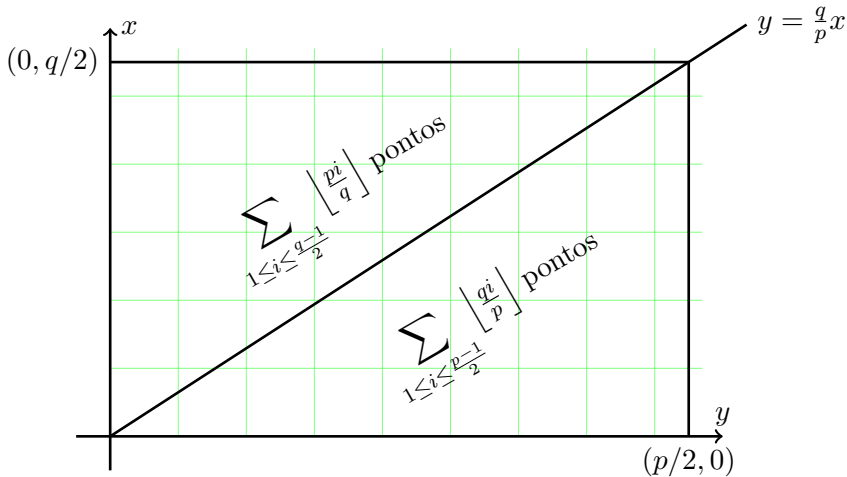
Agora, para provar o item 1 da lei de reciprocidade quadrática, vamos mostrar que

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{1 \leq i \leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \quad (*)$$

e que

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{1 \leq i \leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor} \quad \text{e} \quad \left(\frac{q}{p}\right) = (-1)^{\sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor}. \quad (**)$$

A fórmula (*) é apenas uma contagem: o lado esquerdo é o número de pontos com ambas as coordenadas inteiras no interior do retângulo de vértices $(0, 0)$, $(p/2, 0)$, $(0, q/2)$ e $(p/2, q/2)$.



Por outro lado, o primeiro somatório do lado direito conta o número de tais pontos que estão acima da diagonal $x = \frac{p}{q}y$ do retângulo, enquanto o segundo somatório conta o número de tais pontos abaixo desta diagonal (note que como p e q são primos, não há pontos com ambas as

coordenadas inteiras na diagonal). Por exemplo, no primeiro somatório cada termo $\left\lfloor \frac{ip}{q} \right\rfloor$ representa a quantidade de pontos na reta $y = i$ acima da diagonal $x = \frac{p}{q}y$.

Finalmente, para mostrar (**), basta checar que $\sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod{2}$, onde s é como no lema de Gauß aplicado para $a = q$. Seja r_i o resto da divisão de iq por p , de modo que $iq = \left\lfloor \frac{iq}{p} \right\rfloor p + r_i$. Somando e utilizando a notação da demonstração do lema de Gauß, obtemos

$$q \sum_{1 \leq i \leq \frac{p-1}{2}} i = p \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i < p/2} m_i + \sum_{r_i > p/2} (p - m_i).$$

Como p e q são ímpares, módulo 2 temos

$$\sum_{1 \leq i \leq \frac{p-1}{2}} i \equiv \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i < p/2} m_i + \sum_{r_i > p/2} (1 + m_i) \pmod{2},$$

e como $\{m_1, m_2, \dots, m_{\frac{p-1}{2}}\} = \{1, 2, \dots, \frac{p-1}{2}\}$, concluímos assim que

$$\begin{aligned} \sum_{1 \leq i \leq \frac{p-1}{2}} i &\equiv \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{1 \leq i \leq \frac{p-1}{2}} i + \sum_{r_i > p/2} 1 \pmod{2} \\ \iff \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor &\equiv s \pmod{2} \end{aligned}$$

o que encerra a prova. Na próxima subseção daremos uma demonstração alternativa da lei de reciprocidade quadrática. Para uma terceira prova, veja a seção 6.2.

Observação 2.15. O símbolo de Legendre $\left(\frac{a}{p}\right)$ pode ser estendido para o símbolo de Jacobi $\left(\frac{a}{n}\right)$, que está definido para a inteiro arbitrário e n inteiro positivo ímpar por $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_k}\right)^{\alpha_k}$ se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ é a fatoração prima de n (onde os $\left(\frac{a}{p_j}\right)$ são dados pelo símbolo de Legendre usual); temos $\left(\frac{a}{1}\right) = 1$ para todo inteiro a . Não é difícil provar as seguintes propriedades do símbolo de Jacobi, que podem ser usadas para calcular rapidamente símbolos de Legendre (e de Jacobi):

1. Se $a \equiv b \pmod{n}$ então $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

2. $\left(\frac{a}{n}\right) = 0$ se $\text{mdc}(a, n) \neq 1$ e $\left(\frac{a}{n}\right) \in \{-1, 1\}$ se $\text{mdc}(a, n) = 1$.
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$; em particular, $\left(\frac{a^2}{n}\right) \in \{0, 1\}$.
4. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$; em particular, $\left(\frac{a}{n^2}\right) \in \{0, 1\}$.
5. Se m e n são positivos e ímpares, então $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{m}\right)$.
6. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
7. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Os três últimos fatos, que generalizam a lei de reciprocidade quadrática, podem ser provados usando a multiplicatividade em a e em n do símbolo de Jacobi $\left(\frac{a}{n}\right)$ e a lei de reciprocidade quadrática para o símbolo de Legendre.

Como para o símbolo de Legendre, se $\left(\frac{a}{n}\right) = -1$, a não é resíduo quadrático módulo n , mas (diferentemente do que acontece para o símbolo de Legendre) é possível que $\left(\frac{a}{n}\right)$ seja igual a 0 ou a 1 sem que a seja resíduo quadrático módulo n . Por exemplo, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$ e $\left(\frac{3}{15}\right) = \left(\frac{3}{3}\right)\left(\frac{3}{5}\right) = 0 \cdot (-1) = 0$, mas 2 e 3 não são resíduos quadráticos módulo 15.

2.2.3 Uma demonstração trigonométrica

Nesta subseção usaremos as abreviações

$$s(x) = \sin(2\pi x), \quad c(x) = \cos(2\pi x).$$

Assim as funções s e c têm período 1. Por exemplo, $s(x) = 0$ se e somente se x é inteiro ou da forma inteiro mais meio. Vejamos uma reformulação do Lema de Gauß.

Lema 2.16. *Seja $p > 2$ primo e a inteiro, a primo com p . Então*

$$\prod_{1 \leq k \leq (p-1)/2} s\left(\frac{ak}{p}\right) = \left(\frac{a}{p}\right) \prod_{1 \leq k \leq (p-1)/2} s\left(\frac{k}{p}\right).$$

DEMONSTRAÇÃO: Observe que para cada k entre 1 e $(p-1)/2$ existe um único k' no mesmo intervalo com $ak \equiv \pm k' \pmod{p}$: assim os dois

grandes produtos acima têm o mesmo módulo. O segundo produto é claramente positivo. Por outro lado, temos

$$s\left(\frac{ak}{p}\right) < 0$$

se e somente se o resto de ak módulo p for maior do que $p/2$. Assim, para s como no Lema de Gauß, o número de termos negativos no primeiro produto é igual a s . Pelo Lema de Gauß, isto completa a demonstração. \square

Demonstraremos agora uma fórmula para um produto de senos.

Lema 2.17. *Seja $q > 0$ um inteiro ímpar. Então*

$$s(qx) = (-4)^{\frac{q-1}{2}} \prod_{0 \leq l < q} s\left(x + \frac{l}{q}\right).$$

Assim, por exemplo,

$$s(3x) = -4s(x)s\left(x + \frac{1}{3}\right)s\left(x + \frac{2}{3}\right).$$

Há muitas maneiras de demonstrar estas identidades: a demonstração abaixo usa números complexos e as fórmulas de Euler:

$$e(x) = c(x) + is(x) = \exp(2\pi ix),$$

$$s(x) = \frac{e(x) - e(-x)}{2i}, \quad c(x) = \frac{e(x) + e(-x)}{2}.$$

DEMONSTRAÇÃO: Seja $\zeta = e(1/q)$ é uma raiz do polinômio $w^q - 1$ e temos

$$w^q - 1 = \prod_{0 \leq j < q} w - \zeta^j.$$

Seja $z = e(x)$; temos

$$s(qx) = \frac{z^q - z^{-q}}{2i}, \quad s\left(x + \frac{l}{q}\right) = \frac{\zeta^l z - \zeta^{-l} z^{-1}}{2i}.$$

Substituindo na identidade do enunciado, devemos portanto demonstrar que

$$z^q - z^{-q} = \prod_{0 \leq l < q} \left(\zeta^l z - \zeta^{-l} z^{-1}\right).$$

Multiplicando o lado esquerdo por z^q e cada fator do lado direito por z , devemos mostrar que

$$z^{2q} - 1 = \prod_{0 \leq l < q} (\zeta^l z^2 - \zeta^{-l}).$$

Ora, colocando ζ^l em evidência, temos

$$\prod_{0 \leq l < q} (\zeta^l z^2 - \zeta^{-l}) = \zeta^{q(q-1)/2} \prod_{0 \leq l < q} (z^2 - \zeta^{-2l}).$$

Como q é ímpar, $(q-1)/2$ é inteiro e portanto $\zeta^{q(q-1)/2} = 1$; quando l varia de 0 a $q-1$ temos que $-2l$ corre um sistema completo de resíduos equivalente portanto a j correr de 0 a $q-1$. Devemos portanto provar que

$$z^{2q} - 1 = \prod_{0 \leq j < q} (z^2 - \zeta^j).$$

Fazendo $z^2 = w$, esta é a primeira identidade da demonstração. □

Lema 2.18. *Seja $q > 0$ um inteiro ímpar. Então*

$$\frac{s(qx)}{s(x)} = (-4)^{\frac{q-1}{2}} \prod_{1 \leq l \leq (q-1)/2} \left(s\left(x + \frac{l}{q}\right) s\left(x - \frac{l}{q}\right) \right).$$

DEMONSTRAÇÃO: Segue imediatamente do lema anterior, passando $s(x)$ para o denominador e juntando os termos correspondentes a l e $q-l$. □

Lema 2.19. *Seja $p > 2$ primo e q inteiro ímpar, q primo com p . Então*

$$\left(\frac{q}{p}\right) = (-4)^{\frac{(p-1)(q-1)}{4}} \prod_{1 \leq k \leq (p-1)/2, 1 \leq l \leq (q-1)/2} \left(s\left(\frac{k}{p} + \frac{l}{q}\right) s\left(\frac{k}{p} - \frac{l}{q}\right) \right).$$

DEMONSTRAÇÃO: Pelo Lema 2.16 temos

$$\left(\frac{q}{p}\right) = \prod_{1 \leq k \leq (p-1)/2} \frac{s(qk/p)}{s(k/p)}.$$

Aplicando o Lema 2.18 a cada termo temos

$$\left(\frac{q}{p}\right) = \prod_{1 \leq k \leq (p-1)/2} \left((-4)^{\frac{q-1}{2}} \prod_{1 \leq l \leq (q-1)/2} \left(s\left(\frac{k}{p} + \frac{l}{q}\right) s\left(\frac{k}{p} - \frac{l}{q}\right) \right) \right).$$

Passando as potências de -4 para fora do produtório e juntando os dois produtórios temos a fórmula do enunciado. \square

Estamos agora prontos para concluir a segunda demonstração da Lei de Reciprocidade Quadrática.

DEMONSTRAÇÃO: Se p e q são primos distintos e maiores do que 2 então usando duas vezes o Lema 2.19 temos

$$\frac{\left(\frac{q}{p}\right)}{\left(\frac{p}{q}\right)} = \prod_{1 \leq k \leq (p-1)/2, 1 \leq l \leq (q-1)/2} \frac{s\left(\frac{k}{p} + \frac{l}{q}\right) s\left(\frac{k}{p} - \frac{l}{q}\right)}{s\left(\frac{k}{p} + \frac{l}{q}\right) s\left(-\frac{k}{p} + \frac{l}{q}\right)} = (-1)^{\frac{(p-1)(q-1)}{4}},$$

como queríamos. \square

Problemas Propostos

2.12. Calcular $\left(\frac{44}{103}\right)$, $\left(\frac{-60}{1019}\right)$ e $\left(\frac{2010}{1019}\right)$.

2.13. Determine todas as soluções de $x^{10} \equiv 1 \pmod{49}$.

2.14. Sejam p um primo ímpar e c um inteiro que não é múltiplo de p . Prove que

$$\sum_{a=0}^{p-1} \left(\frac{a(a+c)}{p} \right) = -1.$$

2.15. Existem inteiros m e n tais que

$$5m^2 - 6mn + 7n^2 = 1985?$$

2.16. Demonstrar que a congruência $6x^2 + 5x + 1 \equiv 0 \pmod{m}$ tem solução para todo valor natural de m .

2.17 (OBM2010). Prove que se $10^{2n} + 8 \cdot 10^n + 1$ tem fator primo da forma $60k + 7$ então n e k são pares.

2.18 (Ibero2003). *Definem-se as sucessões $(a_n)_{n \geq 0}$, $(b_n)_{n \geq 0}$ por*

$$a_0 = 1, \quad b_0 = 4, \quad a_{n+1} = a_n^{2001} + b_n, \quad b_{n+1} = b_n^{2001} + a_n, \quad n \geq 0.$$

Demonstre que 2003 não divide nenhum dos termos destas sucessões.

2.19. *Demonstrar que existem infinitos primos da forma $3k+1$ e $3k-1$.*

2.20. *Demonstrar que se $\text{mdc}(a, b) = 1$ o número $a^2 + b^2$ não pode ter fatores primos da forma $4k-1$ e se além disso $\text{mdc}(a, 3) = 1$ então o número $a^2 + 3b^2$ não pode ter fatores da forma $6k-1$. Que podemos dizer sobre os fatores primos de $a^2 + pb^2$ onde p é um primo?*

2.21. *Demonstrar que, para $p = 1093$,*

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}.$$

2.22. *a) (Euler) Seja $F_n = 2^{2^n} + 1$ o n -ésimo número de Fermat. Prove que todo fator primo de F_n é da forma $k \cdot 2^{n+1} + 1$.*

b) (Lucas) Prove que, se $n \geq 2$, então todo fator primo de F_n é da forma $k \cdot 2^{n+2} + 1$.

c) Mostre que $2^{2^5} + 1$ é composto.

2.23 (IMO1996). *Os inteiros positivos a e b são tais que $15a + 16b$ e $16a - 15b$ são ambos quadrados perfeitos positivos. Encontre o menor valor que pode tomar o menor destes quadrados.*

2.24. *Seja p um número primo ímpar. Seja s o menor inteiro positivo que não é resíduo quadrático módulo p .*

(a) Mostre que $p > s^2 - s$.

(b) Suponha que $p > 5$ e que -1 seja resíduo quadrático módulo p : mostre que $p > 2s^2 - s$.

2.25. *Sejam M um número inteiro e p um número primo ímpar. Mostre que a sequência $M, M+1, \dots, M+2\lfloor\sqrt{p}\rfloor$ contém um elemento que não é resíduo quadrático módulo p (e portanto, em particular, não é múltiplo de p).*

2.26 (Putnam 1991). *Seja p um primo ímpar. Quantos elementos tem o conjunto*

$$\{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\} \cap \{y^2 + 1 \mid y \in \mathbb{Z}/p\mathbb{Z}\}?$$

2.27 (IMO2008). *Prove que existe um número infinito de inteiros positivos n tais que $n^2 + 1$ tem um divisor primo maior do que $2n + \sqrt{2n}$.*

2.3 Congruências de Grau Superior

Dado um polinômio $f(x) \in \mathbb{Z}[x]$ e um número natural n , vamos estudar condições para que a congruência

$$f(x) \equiv 0 \pmod{n}$$

tenha solução. O primeiro resultado diz que basta considerar o caso em que $n = p^k$ é a potência de um primo p .

Proposição 2.20. *Suponhamos que $n = p_1^{k_1} \cdots p_l^{k_l}$ onde os p_j são primos distintos. Temos uma equivalência*

$$f(x) \equiv 0 \pmod{n} \iff \begin{cases} f(x) \equiv 0 \pmod{p_1^{k_1}} \\ \vdots \\ f(x) \equiv 0 \pmod{p_l^{k_l}} \end{cases}$$

de modo que $f(x) \equiv 0 \pmod{n}$ admite solução se, e somente se, $f(x) \equiv 0 \pmod{p_j^{k_j}}$ tem solução para cada j .

DEMONSTRAÇÃO: Como as potências $p_j^{k_j}$ são coprimas duas a duas, temos que n divide um inteiro M se, e só se, $p_j^{k_j} \mid M$ para cada j , o que demonstra a equivalência. Assim, a existência de solução para $f(x) \equiv 0 \pmod{n}$ implica a existência de solução para o sistema acima. Reciprocamente, se cada $f(x) \equiv 0 \pmod{p_j^{k_j}}$ tem uma solução $x \equiv a_j \pmod{p_j^{k_j}}$, pelo teorema chinês dos restos existe a tal que $a \equiv a_j \pmod{p_j^{k_j}}$ para todo j , de modo que $f(a) \equiv f(a_j) \equiv 0 \pmod{p_j^{k_j}}$ para todo j e logo $f(a) \equiv 0 \pmod{n}$ pela equivalência acima. Note em particular que o número de soluções distintas módulo n de $f(x) \equiv 0 \pmod{n}$ é igual ao produto do número de soluções módulo $p_j^{k_j}$ de $f(x) \equiv 0 \pmod{p_j^{k_j}}$. \square

A próxima proposição indica como, a partir de uma solução de $f(x) \equiv 0 \pmod{p^{k_0}}$, obter soluções para $f(x) \equiv 0 \pmod{p^k}$ para todo $k \geq k_0$. Para isso, precisamos da noção de *derivada* de um polinômio: se $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{j=0}^n a_j x^j$, definimos sua

derivada $p'(x)$ como sendo o polinômio

$$p'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 = \sum_{j=1}^n ja_jx^{j-1}.$$

Note que, se $p(x) \in \mathbb{Z}[x]$, então $p'(x) \in \mathbb{Z}[x]$.

Proposição 2.21 (Lema de Hensel). *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio, p um número primo. Seja $a \in \mathbb{Z}$ tal que $f(a) \equiv 0 \pmod{p^{k_0}}$ e cuja maior potência p^{l_0} de p com $p^{l_0} \mid f'(a)$ satisfaz $0 \leq 2l_0 < k_0$. Então existe uma sequência de inteiros $(a_k)_{k \geq k_0}$ com*

$$\begin{aligned} a_{k_0} &= a, & a_{k+1} &\equiv a_k \pmod{p^{k-l_0}} & e \\ f(a_k) &\equiv 0 \pmod{p^k} & \text{para todo } k &\geq k_0. \end{aligned}$$

Em particular, se existe um inteiro a tal que $f(a) \equiv 0 \pmod{p}$ mas $f'(a) \not\equiv 0 \pmod{p}$ então $f(x) \equiv 0 \pmod{p^k}$ admite solução para todo $k \in \mathbb{N}$.

DEMONSTRAÇÃO: Construimos a sequência indutivamente. Seja $k \geq k_0$ e suponha por indução que $p^k \mid f(a_k)$, ou seja, $f(a_k) = r_k p^k$ para um certo $r_k \in \mathbb{Z}$ e $p^{l_0} \mid f'(a_k)$ mas $p^{l_0+1} \nmid f'(a_k)$, ou seja, $f'(a_k) = s_k p^{l_0}$ onde $p \nmid s_k$. Estamos procurando um número da forma $a_{k+1} = a_k + t_k p^{k-l_0}$, com $t_k \in \mathbb{Z}$, que satisfaz $p^{k+1} \mid f(a_{k+1})$, $p^{l_0} \mid f'(a_{k+1})$ mas $p^{l_0+1} \nmid f'(a_{k+1})$.

Para cada $r \in \mathbb{N}$, temos

$$\begin{aligned} (a_k + t_k p^{k-l_0})^r &= a_k^r + t_k r a_k^{r-1} p^{k-l_0} + \sum_{j=2}^r \binom{r}{j} a_k^{r-j} p^{j(k-l_0)} \equiv \\ &\equiv a_k^r + t_k r a_k^{r-1} p^{k-l_0} \pmod{p^{k+1}}, \end{aligned}$$

pois a hipótese $0 \leq 2l_0 < k_0$ implica $2(k-l_0) \geq k+1$. Se $f(x) = \sum_{r=0}^n c_r x^r$, multiplicando a congruência acima por c_r e somando, de $r=0$ até n , obtemos

$$f(a_{k+1}) = f(a_k + t_k p^{k-l_0}) = \sum_{r=0}^n c_r a_k^r + t_k \sum_{r=0}^n r a_k^{r-1} p^{k-l_0} =$$

$$= f(a_k) + t_k f'(a_k) p^{k-l_0} = r_k p^k + s_k t_k p^k \pmod{p^{k+1}}.$$

Logo para que $p^{k+1} \mid f(a_{k+1})$ devemos encontrar t_k tal que $r_k + s_k t_k \equiv 0 \pmod{p}$, o que é possível pois s_k é invertível módulo p . Finalmente, temos que

$$\begin{aligned} f'(a_{k+1}) &\equiv f'(a_k) = s_k p^{l_0} \pmod{p^{k-l_0}} \\ \implies \begin{cases} f'(a_{k+1}) &\equiv 0 \pmod{p^{l_0}} \\ f'(a_{k+1}) &\not\equiv 0 \pmod{p^{l_0+1}} \end{cases} \end{aligned}$$

o que completa a indução. \square

Observemos que a condição sobre a derivada de f no lema de Hensel é necessária. Para isto, consideremos $f(x) = x^m + 3$ com $m \geq 2$, $a = 0$ e $p = 3$. Assim, temos que $f(0) = 3 \equiv 0 \pmod{3}$, mas $f'(0) = 0$ é divisível por potências arbitrariamente grandes de 3, logo $f(x)$ não satisfaz a segunda hipótese da proposição. E de fato, se $b \in \mathbb{Z}$ e $f(b) = b^m + 3 \equiv 0 \pmod{3}$ então $b \equiv 0 \pmod{3}$, donde $b^m \equiv 0 \pmod{9}$ e $f(b) = b^m + 3 \equiv 3 \pmod{9}$, o que mostra que nenhuma raiz módulo 3 “levanta” para uma raiz módulo 9.

Agora vamos nos concentrar em equações módulo p . Para o próximo resultado, necessitamos de um

Lema 2.22. *Seja p um primo. Então*

$$1^k + 2^k + \cdots + (p-1)^k \pmod{p} = \begin{cases} 0 & \text{se } (p-1) \nmid k, \\ p-1 & \text{se } (p-1) \mid k. \end{cases}$$

DEMONSTRAÇÃO: Se $(p-1) \mid k$, temos que cada termo da soma acima é congruente a 1 módulo p e o resultado segue. Suponha agora que $(p-1) \nmid k$ e seja g uma raiz primitiva módulo p . Temos portanto

$$1^k + 2^k + \cdots + (p-1)^k \equiv 1 + g^k + g^{2k} + \cdots + g^{(p-2)k} \pmod{p}$$

Sendo $S = 1 + g^k + g^{2k} + \cdots + g^{(p-2)k}$, multiplicando por g^k e observando que $g^{(p-1)k} \equiv 1 \pmod{p}$ temos

$$\begin{aligned} g^k S &\equiv g^k + g^{2k} + \cdots + g^{(p-1)k} \pmod{p} \\ \iff g^k S &\equiv S \pmod{p} \iff (g^k - 1)S \equiv 0 \pmod{p} \end{aligned}$$

Como g é uma raiz primitiva e $(p-1) \nmid k$ temos que $g^k - 1 \not\equiv 0 \pmod{p}$, ou seja, $g^k - 1$ é invertível módulo p e portanto $S \equiv 0 \pmod{p}$, o que encerra a prova. \square

Teorema 2.23 (Chevalley-Warning). *Seja p um primo e sejam*

$$f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$$

polinômios em n variáveis com coeficientes inteiros tais que $f_i(0, \dots, 0) \equiv 0 \pmod{p}$ para todo $i \leq k$. Suponha que $\sum_{1 \leq i \leq k} \deg(f_i) < n$.

Então a quantidade de “pontos” em

$$A = \{(x_1, \dots, x_n) \in (\mathbb{Z}/p\mathbb{Z})^n \mid f_i(x_1, \dots, x_n) = \bar{0} \quad \forall i = 1, \dots, k\}$$

é um múltiplo de p . Em particular, existem pontos $(x_1, \dots, x_n) \neq (\bar{0}, \dots, \bar{0})$ em $(\mathbb{Z}/p\mathbb{Z})^n$ tais que $f_i(x_1, \dots, x_n) = \bar{0}$ para todo i .

DEMONSTRAÇÃO: Usaremos o lema anterior para determinar $|A| \pmod{p}$. Para isso, notemos que pelo teorema de Euler-Fermat $f_j(x_1, \dots, x_n) \not\equiv 0 \pmod{p} \iff f_j(x_1, \dots, x_n)^{p-1} \equiv 1 \pmod{p}$. Definamos

$$g(x_1, \dots, x_n) = \prod_{1 \leq j \leq k} (1 - f_j(x_1, \dots, x_n)^{p-1}).$$

Observemos que $g(x_1, \dots, x_n) \equiv 0 \pmod{p}$ se, e somente se, existe j tal que $f_j(x_1, \dots, x_n) \not\equiv 0 \pmod{p}$. Por outro lado, se $f_j(x_1, \dots, x_n) \equiv 0 \pmod{p}$ para todo j então $g(x_1, \dots, x_n) \equiv 1 \pmod{p}$, portanto

$$\sum_{(x_1, \dots, x_n) \in (\mathbb{Z}/p\mathbb{Z})^n} g(x_1, \dots, x_n) \equiv |A| \pmod{p}.$$

Notemos agora que $\deg(g) \leq \sum_{1 \leq j \leq k} (p-1) \deg(f_j) < (p-1)n$. Portanto cada monômio $cx_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ de g é tal que $\sum_{1 \leq j \leq n} i_j < (p-1)n$, donde pelo Princípio da Casa dos Pombos sempre existe algum r com $0 \leq i_r < p-1$. Assim, pelo lema anterior, $\sum_{x_r \in \mathbb{Z}/p\mathbb{Z}} x_r^{i_r} \equiv 0 \pmod{p}$ donde

$$\begin{aligned} \sum_{(x_1, \dots, x_n) \in (\mathbb{Z}/p\mathbb{Z})^n} cx_1^{i_1} x_2^{i_2} \dots x_n^{i_n} &\equiv c \sum_{x_1 \in \mathbb{Z}/p\mathbb{Z}} x_1^{i_1} \sum_{x_2 \in \mathbb{Z}/p\mathbb{Z}} x_2^{i_2} \dots \sum_{x_n \in \mathbb{Z}/p\mathbb{Z}} x_n^{i_n} \\ &\equiv 0 \pmod{p} \end{aligned}$$

Isso mostra que $\sum_{(x_1, \dots, x_n) \in (\mathbb{Z}/p\mathbb{Z})^n} g(x_1, \dots, x_n) \equiv 0 \pmod{p}$ e, portanto, $|A|$ é múltiplo de p . Como $(\bar{0}, \bar{0}, \dots, \bar{0}) \in A$, há pelo menos $p-1$ outros pontos nesse conjunto, o que prova o teorema. \square

Como aplicação, provemos o seguinte resultado, devido a Erdős, Ginzburg e Ziv.

Proposição 2.24. *Seja n um inteiro positivo. Dados inteiros x_1, \dots, x_{2n-1} existem $1 \leq i_1 < i_2 < \dots < i_n \leq 2n-1$ tais que $x_{i_1} + x_{i_2} + \dots + x_{i_n}$ é divisível por n .*

DEMONSTRAÇÃO: Mostremos primeiro que se o resultado vale para m e para n então vale para mn . Sejam $x_1, x_2, \dots, x_{2mn-1} \in \mathbb{Z}$. Por hipótese temos que, para cada subconjunto A de $\{1, 2, \dots, 2mn-1\}$ com $2n-1$ elementos, existe um subconjunto $B \subset A$ com n elementos tal que $\sum_{i \in B} x_i$ é divisível por n . Assim, construímos B_j indutivamente para todo $1 \leq j \leq 2m-1$, seguindo os seguintes passos

- Escolhemos um subconjunto A_j de $\{1, 2, \dots, 2mn-1\} \setminus \bigcup_{k < j} B_k$ com $2n-1$ elementos.
- De A_j escolhemos um subconjunto B_j com n elementos tal que $\sum_{i \in B_j} x_i$ é divisível por n .

Observemos que se $j \leq 2m-1$ então

$$\begin{aligned} \left| \{1, 2, \dots, 2mn-1\} \setminus \bigcup_{k < j} B_k \right| &= 2mn-1 - (j-1)n \\ &\geq 2mn-1 - (2m-2)n = 2n-1, \end{aligned}$$

o que garante a construção até $j = 2m-1$. Definamos agora os inteiros $y_j = \frac{1}{n} \sum_{i \in B_j} x_i$ para $1 \leq j \leq 2m-1$. De novo por hipótese, existe um subconjunto de índices $C \subset \{1, \dots, 2m-1\}$ com m elementos tal que $\sum_{j \in C} y_j$ é divisível por m e portanto

$$\sum_{j \in C} \sum_{i \in B_j} x_i = n \sum_{j \in C} y_j$$

é uma soma com $|C||B_j| = mn$ somandos que é divisível por mn .

Assim, basta provar a proposição para n primo. Para isso, consideremos os polinômios

$$\begin{aligned} f_1(x_1, \dots, x_{2n-1}) &= x_1^{n-1} + x_2^{n-1} + \dots + x_{2n-1}^{n-1} \quad \text{e} \\ f_2(x_1, \dots, x_{2n-1}) &= a_1 x_1^{n-1} + a_2 x_2^{n-1} + \dots + a_{2n-1} x_{2n-1}^{n-1} \end{aligned}$$

onde a_1, \dots, a_{2n-1} são os inteiros dados. A soma dos graus de f_1 e f_2 é $2(n-1) < 2n-1$. Pelo teorema de Chevalley-Waring, existem $x_1, \dots, x_{2n-1} \in \mathbb{Z}/(n)$ não todos nulos com

$$f_1(x_1, \dots, x_{2n-1}) \equiv f_2(x_1, \dots, x_{2n-1}) \equiv 0 \pmod{n}.$$

Como $x^{n-1} \equiv 1 \pmod{n}$ para todo $x \in (\mathbb{Z}/(n))^\times$, $f_1(x_1, \dots, x_{2n-1}) \equiv 0 \pmod{n}$ implica que existem exatamente n valores $i \leq 2n-1$ com $x_i \not\equiv 0 \pmod{n}$. Sejam $1 \leq i_1 < i_2 < \dots < i_n \leq 2n-1$ tais valores de i , como $x_{i_s}^{n-1} \equiv 1 \pmod{n}$ para todo $s \leq n$ temos que

$$a_1 x_1^{n-1} + a_2 x_2^{n-1} + \dots + a_{2n-1} x_{2n-1}^{n-1} \equiv a_{i_1} + a_{i_2} + \dots + a_{i_n} \pmod{n},$$

pois $x_j \equiv 0 \pmod{n}$ se $j \neq i_s$ para todo $s \leq n$. Assim, $a_{i_1} + a_{i_2} + \dots + a_{i_n}$ é divisível por n , o que prova o resultado. \square

Problemas Propostos

2.28 (OBM2007). Para quantos inteiros c , $-2007 \leq c \leq 2007$, existe um inteiro x tal que $x^2 + c$ é múltiplo de 2^{2007} ?

2.29. Seja p um primo e seja n tal que $p^k \nmid n$. Demonstrar: se a equação $y^n \equiv a \pmod{p^k}$ tem solução com $\text{mdc}(y, p) = 1$, então para todo $m > k$ a equação $y^n \equiv a \pmod{p^m}$ possui solução.

2.30. Seja $f(x) \in \mathbb{Z}[x]$ um polinômio, p um número primo, a um inteiro tal que $f(a) \equiv 0 \pmod{p}$ mas $f'(a) \not\equiv 0 \pmod{p}$ e k um inteiro positivo. Prove que, se a_k é um inteiro tal que $a_k \equiv a \pmod{p}$ e $f(a_k) \equiv 0 \pmod{p^k}$, então, tomando b tal que $b \equiv a_k - f(a_k) \cdot f'(a_k)^{-1} \pmod{p^{2k}}$, então $f(b) \equiv 0 \pmod{p^{2k}}$.

2.31. Seja p um primo ímpar, a um inteiro e n um inteiro positivo. Sejam α e β inteiros não negativos, com $\alpha > 0$. Prove:

(a) Se p^β e p^α são as maiores potências de p que dividem n e $a-1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência de p que divide $a^n - 1$ (atenção, p deve dividir $a-1$ pois $\alpha > 0$! Mas note que p não precisa dividir n)

(b) Se n é ímpar e p^β e p^α são as maiores potências de p que dividem n e $a + 1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência de p que divide $a^n + 1$ (mesma ressalva do item (i)).

2.32. Sejam a um inteiro e n um inteiro positivo. Sejam α e β inteiros não negativos, com $\alpha, \beta > 0$. Prove:

- (a) Se n é ímpar e 2^α é a maior potência de 2 que divide $a - 1$ então 2^α é também a maior potência de 2 que divide $a^n - 1$.
- (b) Se $a \equiv 1 \pmod{4}$ e 2^β e 2^α são as maiores potências de 2 que dividem n e $a - 1$ respectivamente então $2^{\alpha+\beta}$ é a maior potência de 2 que divide $a^n - 1$.
- (c) Se $a \equiv 3 \pmod{4}$ e 2^β e 2^α são as maiores potências de 2 que dividem n e $a + 1$ respectivamente então $2^{\alpha+\beta}$ é a maior potência de 2 que divide $a^n - 1$.
- (d) Se n é ímpar e 2^α é a maior potência de 2 que divide $a + 1$ então 2^α é também a maior potência de 2 que divide $a^n + 1$.

2.33. Encontre todos os inteiros não negativos x e y tais que

$$7^y - 2 \cdot 3^x = 1$$

2.34. Encontre todas as ternas (a, m, n) de inteiros positivos tais que $a^m + 1$ divide $(a + 1)^n$.

2.35. Seja p um número primo e n, k e $a = p^t a_1$ números naturais tais que $\text{mdc}(p, a_1) = 1$. Prove: a congruência $x^n \equiv a \pmod{p^k}$ tem solução se, e só se, $k \leq t$ ou

$$k > t, \quad n \mid t \quad \text{e} \quad a_1^{\frac{p^{k-1}(p-1)}{\text{mdc}(n, p^{k-1}(p-1))}} \equiv 1 \pmod{p^{k-t}}.$$

2.36 (Irlanda 1997). Seja A um subconjunto de $\{1, 2, \dots, 2n - 1\}$ com n elementos. Prove que A contém uma potência de 2 ou dois elementos distintos cuja soma é uma potência de 2.

2.37 (Romênia 1996). Determinar o maior inteiro positivo n com a seguinte propriedade: existem inteiros não negativos x_1, \dots, x_n tais que,

para toda sequência $\epsilon_1, \epsilon_2, \dots, \epsilon_n$ de elementos de $\{-1, 0, 1\}$, não todos zero, o número

$$\epsilon_1 x_1 + \epsilon_2 x_2 + \dots + \epsilon_n x_n$$

não é divisível por n^3 .

2.38 (Erdős). *Mostrar que todo número inteiro positivo pode ser expresso como soma de números da forma $2^a 3^b$ de modo que nenhum termo é divisível por outro.*

2.39 (Romênia 1998). *Mostrar que para todo $n \geq 2$ existe um subconjunto S de $\{1, 2, \dots, n\}$ com no máximo $2\lfloor\sqrt{n}\rfloor + 1$ elementos tal que todo número natural menor do que n pode ser representado como diferença de dois elementos de S .*

2.40 (IMO2007). *Seja n um inteiro positivo. Considere*

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \dots, n\}, \quad x + y + z > 0\}$$

como um conjunto de $(n+1)^3 - 1$ pontos no espaço tridimensional. Determine o menor número de planos, a união dos quais contém S mas não inclui $(0, 0, 0)$.

Capítulo 3

Frações Contínuas

A teoria de frações contínuas é um dos mais belos assuntos da Matemática elementar, sendo ainda hoje tema de pesquisa.

Nas inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, a passagem de \mathbb{Q} para \mathbb{R} é sem dúvida a mais complicada conceitualmente e a representação de um número real está diretamente ligada à própria noção de número real.

De fato, o conceito de número natural é quase um conceito primitivo. Já um número inteiro é um número natural com um sinal que pode ser $+$ ou $-$, e um número racional é a razão entre um número inteiro e um natural não nulo. Por outro lado, dizer o que é um número real é tarefa bem mais complicada, mas há coisas que podemos dizer sobre eles. Uma propriedade essencial de \mathbb{R} é que todo número real pode ser bem aproximado por números racionais. Efetivamente, dado $x \in \mathbb{R}$, existe $k = \lfloor x \rfloor \in \mathbb{Z}$ tal que $0 \leq x - k < 1$. Podemos escrever a representação decimal de

$$x - k = 0, a_1 a_2 \dots a_n \dots, \quad a_i \in \{0, 1, \dots, 9\},$$

o que significa que se $r_n = a_n + 10 \cdot a_{n-1} + 100 \cdot a_{n-2} + \dots + 10^{n-1} \cdot a_1$, então $\frac{r_n}{10^n} \leq x - k < \frac{r_n+1}{10^n}$, e portanto $k + \frac{r_n}{10^n}$ é uma boa aproximação racional de x , no sentido de que o erro $|x - (k + \frac{r_n}{10^n})|$ é menor do que $\frac{1}{10^n}$, que é um número bem pequeno se n for grande. A representação decimal de um número real fornece pois uma sequência de aproximações por racionais cujos denominadores são potências de 10.

Dado qualquer $x \in \mathbb{R}$ e q natural não nulo existe $p \in \mathbb{Z}$ tal que $\frac{p}{q} \leq x < \frac{p+1}{q}$ (basta tomar $p = \lfloor qx \rfloor$), e portanto $|x - \frac{p}{q}| < \frac{1}{q}$ e $|x - \frac{p+1}{q}| \leq \frac{1}{q}$.

Em particular há aproximações de x por racionais com denominador q com erro menor do que $\frac{1}{q}$. A representação decimal de x equivale a dar essas aproximações para os denominadores q que são potências de 10, e tem méritos como sua praticidade para efetuar cálculos que a fazem a mais popular das representações dos números reais. Por outro lado, envolve a escolha arbitrária da base 10, e oculta frequentemente aproximações racionais de x muito mais eficientes do que as que exhibe. Por exemplo,

$$\left| \pi - \frac{22}{7} \right| < \frac{1}{700} < \left| \pi - \frac{314}{100} \right| \text{ e } \left| \pi - \frac{355}{113} \right| < \frac{1}{3000000} < \left| \pi - \frac{3141592}{1000000} \right|$$

mostram que $\frac{22}{7}$ e $\frac{355}{113}$ são melhores aproximações de π que aproximações decimais com denominadores muito maiores, e de fato são aproximações muito mais espetaculares do que se podia esperar.

O objetivo desta seção é apresentar uma outra maneira de representar números reais, a representação por *frações contínuas*, que sempre fornece aproximações racionais surpreendentemente boas, e de fato fornece todas as aproximações excepcionalmente boas, além de ser natural e conceitualmente simples. Boa parte desta exposição é baseada em [17].

Definimos recursivamente

$$\alpha_0 = x, \quad a_n = \lfloor \alpha_n \rfloor$$

$$\text{e, se } \alpha_n \notin \mathbb{Z}, \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n} \text{ para todo } n \in \mathbb{N}.$$

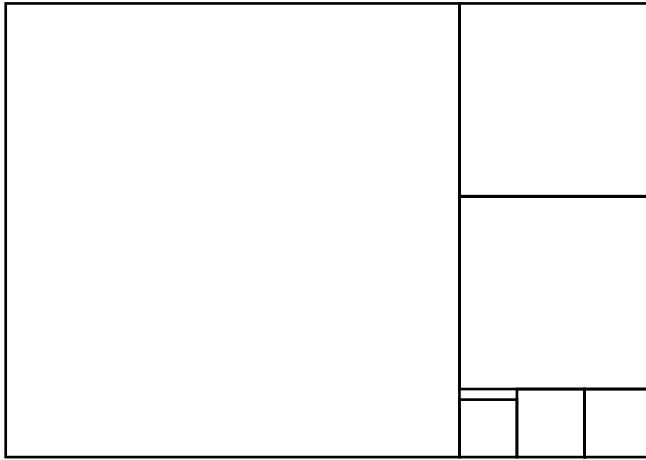
Se, para algum n , $\alpha_n = a_n$ temos

$$x = \alpha_0 = [a_0; a_1, a_2, \dots, a_n] \stackrel{\text{def}}{=} a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n}}}.$$

Se não denotamos

$$x = [a_0; a_1, a_2, \dots] \stackrel{\text{def}}{=} a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}.$$

O sentido dessa última notação ficará claro mais tarde. A representação acima se chama *representação por frações contínuas de x* .



A figura dá uma interpretação geométrica para a representação de um número por frações contínuas. Enchemos um retângulo $1 \times x$ com quadrados de forma “gulosa”, isto é, sempre colocando o maior quadrado possível dentro do espaço ainda livre. Os coeficientes a_0, a_1, a_2, \dots indicam o número de quadrados de cada tamanho. Na figura, se os lados do retângulo são $c < d$ então

$$\frac{d}{c} = [1; 2, 2, 1, \dots]$$

pois temos $a_0 = 1$ quadrado grande, $a_1 = 2$ quadrados menores, $a_2 = 2$ quadrados ainda menores, $a_3 = 1$ quadrados ainda ainda menores, e um número grande não desenhado de quadrados ainda ainda ainda menores (a_4 é grande). Deixamos a verificação de que esta descrição geométrica corresponde à descrição algébrica acima a cargo do leitor.

Note que, se a representação por frações contínuas de x for finita então x é claramente racional.

Reciprocamente, se $x \in \mathbb{Q}$, sua representação será finita, e seus coeficientes a_n vêm do algoritmo de Euclides: se $x = p/q$ (com $q > 0$) temos

$$\begin{array}{ll} p = a_0q + r_1 & 0 \leq r_1 < q \\ q = a_1r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = a_2r_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \vdots \\ r_{n-1} = a_nr_n & \end{array}$$

Temos então

$$\begin{aligned}
 x = p/q &= a_0 + r_1/q = a_0 + \frac{1}{a_1 + r_2/r_1} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + r_3/r_2}} \\
 &= \dots = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n}}} = [a_0; a_1, a_2, \dots, a_n].
 \end{aligned}$$

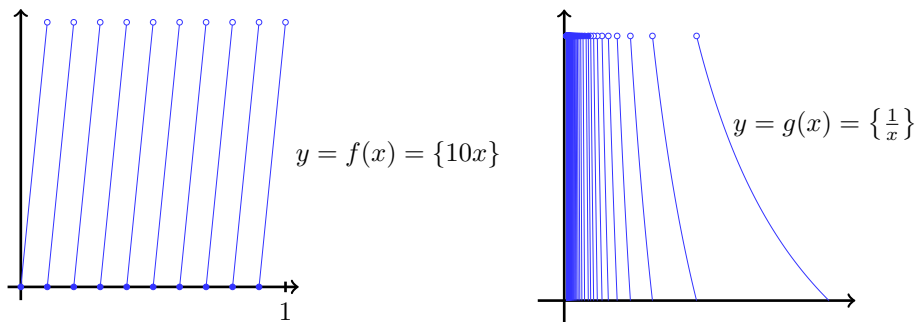
Isso já é uma vantagem da representação por frações contínuas (além de não depender de escolhas artificiais de base), pois o reconhecimento de racionais é mais simples que na representação decimal.

A representação decimal de números reais está intimamente ligada à função $f : [0, 1) \rightarrow [0, 1)$ dada por $f(x) = \{10x\} = 10x - \lfloor 10x \rfloor$, mais precisamente, à *dinâmica* da função f . Por dinâmica da função f queremos dizer o estudo de suas composições sucessivas: para cada ponto $x \in [0, 1)$, estamos interessados na sequência $x, f(x), f(f(x)), \dots \in [0, 1)$, cujos termos são os chamados *iterados* sucessivos da f . De fato, se $x \in [0, 1)$ tem representação decimal $0, a_1 a_2 a_3 \dots$, então $a_1 = \lfloor 10x \rfloor$ e $f(x) = 0, a_2 a_3 a_4 \dots$. Assim, definindo $f^1 = f$ e $f^{n+1} = f \circ f^n$, temos $f^n(x) = 0, a_{n+1} a_{n+2} a_{n+3} \dots$ para todo $n \geq 1$. Assim, por exemplo, se $x = 1/3 = 0,333\dots$, temos $f(x) = 0,333\dots = x$ (nesse caso, dizemos que $x = 1/3$ é um *ponto fixo* de f); se $x = 4/33 = 0,121212\dots$, temos $f(x) = 0,212121\dots$ e $f(f(x)) = 0,121212\dots = x$ (nesse caso dizemos que $x = 4/33$ é um *ponto periódico* de período 2 de f) e, se $x \in [0, 1]$ é irracional, os seus iterados por f serão todos distintos, pois sua representação decimal não será periódica a partir de nenhum dígito.

Já a representação em frações contínuas está intimamente ligada à dinâmica da função $g : (0, 1) \rightarrow [0, 1)$, dada por $g(x) = \left\{ \frac{1}{x} \right\} = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor$, também conhecida como *transformação de Gauss*: se $\alpha = [0; a_1, a_2, a_3, \dots] \in (0, 1)$, então $a_1 = \left\lfloor \frac{1}{\alpha} \right\rfloor$ e $g(\alpha) = [0; a_2, a_3, a_4, \dots]$. Assim, definindo, como antes $g^1 = g$ e $g^{n+1} = g \circ g^n$ para todo $n \geq 1$, temos $g^n(\alpha) = [0; a_{n+1}, a_{n+2}, a_{n+3}, \dots]$, para todo $n \geq 1$.

Mais informações sobre a relação entre frações contínuas e a dinâmica da transformação de Gauss pode ser encontrada em [46].

Representamos abaixo os gráficos de $f(x) = \{10x\}$ e $g(x) = \{\frac{1}{x}\}$.



Seja $x = [a_0; a_1, a_2, \dots]$. Sejam $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}_{>0}$ primos entre si tais que $\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n]$, $n \geq 0$. Esta fração $\frac{p_n}{q_n}$ é chamada de n -ésima *reduzida* ou *convergente* da fração contínua de x . O seguinte resultado será fundamental no que seguirá.

Proposição 3.1. *Dada uma sequência (finita ou infinita) $t_0, t_1, t_2, \dots \in \mathbb{R}$ tal que $t_k > 0$, para todo $k \geq 1$, definimos sequências (x_m) e (y_m) por $x_0 = t_0$, $y_0 = 1$, $x_1 = t_0 t_1 + 1$, $y_1 = t_1$, $x_{m+2} = t_{m+2} x_{m+1} + x_m$, $y_{m+2} = t_{m+2} y_{m+1} + y_m$, para todo $m \geq 0$. Temos então*

$$[t_0; t_1, t_2, \dots, t_n] = t_0 + \frac{1}{t_1 + \frac{1}{t_2 + \dots + \frac{1}{t_n}}} = \frac{x_n}{y_n}, \forall n \geq 0.$$

Além disso, $x_{n+1} y_n - x_n y_{n+1} = (-1)^n$, para todo $n \geq 0$.

DEMONSTRAÇÃO: A prova será por indução em n . Para $n = 0$ temos $[t_0] = t_0 = t_0/1 = x_0/y_0$. Para $n = 1$, temos $[t_0; t_1] = t_0 + 1/t_1 = \frac{t_0 t_1 + 1}{t_1} = x_1/y_1$ e, para $n = 2$, temos

$$\begin{aligned} [t_0; t_1, t_2] &= t_0 + \frac{1}{t_1 + 1/t_2} = t_0 + \frac{t_2}{t_1 t_2 + 1} = \frac{t_0 t_1 t_2 + t_0 + t_2}{t_1 t_2 + 1} \\ &= \frac{t_2(t_0 t_1 + 1) + t_0}{t_2 t_1 + 1} = \frac{t_2 x_1 + x_0}{t_2 y_1 + y_0} = \frac{x_2}{y_2}. \end{aligned}$$

Suponha que a afirmação seja válida para n . Para $n + 1$ em lugar de n temos

$$\begin{aligned}
 [t_0; t_1, t_2, \dots, t_n, t_{n+1}] &= [t_0; t_1, t_2, \dots, t_n + \frac{1}{t_{n+1}}] \\
 &= \frac{(t_n + \frac{1}{t_{n+1}})x_{n-1} + x_{n-2}}{(t_n + \frac{1}{t_{n+1}})y_{n-1} + y_{n-2}} \\
 &= \frac{t_{n+1}(t_n x_{n-1} + x_{n-2}) + x_{n-1}}{t_{n+1}(t_n y_{n-1} + y_{n-2}) + y_{n-1}} \\
 &= \frac{t_{n+1}x_n + x_{n-1}}{t_{n+1}y_n + y_{n-1}} = \frac{x_{n+1}}{y_{n+1}}.
 \end{aligned}$$

Vamos agora mostrar, por indução, a segunda afirmação. Temos

$$x_1 y_0 - x_0 y_1 = (t_0 t_1 + 1) - t_0 t_1 = 1 = (-1)^0$$

e, se $x_{n+1} y_n - x_n y_{n+1} = (-1)^n$ para algum valor de n , então

$$\begin{aligned}
 x_{n+2} y_{n+1} - x_{n+1} y_{n+2} &= (t_{n+2} x_{n+1} + x_n) y_{n+1} - (t_{n+2} y_{n+1} + y_n) x_{n+1} \\
 &= -(x_{n+1} y_n - x_n y_{n+1}) = -(-1)^n = (-1)^{n+1}.
 \end{aligned}$$

□

Nos próximos resultados, $x = [a_0; a_1, a_2, a_3, \dots]$ será um número real, e $(\frac{p_n}{q_n})_{n \in \mathbb{N}}$, $\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n]$ será a sequência de reduzidas da fração contínua de x .

Corolário 3.2. *As sequências (p_n) e (q_n) satisfazem as recorrências*

$$p_{n+2} = a_{n+2} p_{n+1} + p_n \quad e \quad q_{n+2} = a_{n+2} q_{n+1} + q_n$$

para todo $n \geq 0$, com $p_0 = a_0$, $p_1 = a_0 a_1 + 1$, $q_0 = 1$ e $q_1 = a_1$. Além disso,

$$p_{n+1} q_n - p_n q_{n+1} = (-1)^n$$

para todo $n \geq 0$.

DEMONSTRAÇÃO: As sequências (p_n) e (q_n) definidas pelas recorrências acima satisfazem, pela proposição anterior, as igualdades

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n] \text{ e } p_{n+1} q_n - p_n q_{n+1} = (-1)^n, \forall n \geq 0.$$

Como $p_{n+1}q_n - p_nq_{n+1} = (-1)^n$, para todo $n \in \mathbb{N}$, temos que os p_n, q_n dados pelas recorrências acima são primos entre si. Além disso, também segue da recorrência que $q_n > 0, \forall n \geq 0$. Esses fatos implicam que $(\frac{p_n}{q_n})_{n \in \mathbb{N}}$ é a sequência de reduzidas da fração contínua de x . \square

Corolário 3.3. *Temos, para todo $n \in \mathbb{N}$,*

$$x = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} \quad e \quad \alpha_n = \frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}}$$

DEMONSTRAÇÃO: A primeira igualdade segue da proposição anterior pois $x = [a_0; a_1, a_2, \dots, a_{n-1}, \alpha_n]$ e a segunda é consequência direta da primeira. \square

Proposição 3.4. *Temos*

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2}$$

onde

$$\beta_{n+1} = \frac{q_{n-1}}{q_n} = [0; a_n, a_{n-1}, a_{n-2}, \dots, a_1].$$

Em particular,

$$\frac{1}{(a_{n+1} + 2)q_n^2} < \left| x - \frac{p_n}{q_n} \right| = \frac{1}{(\alpha_{n+1} + \beta_{n+1})q_n^2} < \frac{1}{a_{n+1}q_n^2}.$$

DEMONSTRAÇÃO: Pelo corolário anterior temos

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{(\alpha_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{-(p_nq_{n-1} - p_{n-1}q_n)}{(\alpha_{n+1}q_n + q_{n-1})q_n} = \frac{-(-1)^{n-1}}{(\alpha_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{(-1)^n}{(\alpha_{n+1}q_n + q_{n-1})q_n} = \frac{(-1)^n}{(\alpha_{n+1} + q_{n-1}/q_n)q_n^2} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2}. \end{aligned}$$

Em particular,

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{(\alpha_{n+1} + \beta_{n+1})q_n^2},$$

e, como $\lfloor \alpha_{n+1} \rfloor = a_{n+1}$ e $0 < \beta_{n+1} < 1$, segue que $a_{n+1} < \alpha_{n+1} + \beta_{n+1} < a_{n+1} + 2$, o que implica a última afirmação.

A expansão de β_{n+1} como fração contínua segue de

$$\frac{q_{n-1}}{q_n} = \frac{q_{n-1}}{a_n q_{n-1} + q_{n-2}} \implies \frac{q_{n-1}}{q_n} = \frac{1}{a_n + \frac{q_{n-2}}{q_{n-1}}}$$

aplicado recursivamente. \square

Observação 3.5. Como $\lim_{n \rightarrow \infty} q_n = +\infty$ (pois (q_n) é estritamente crescente), segue desta proposição que

$$\lim_{n \rightarrow \infty} \frac{p_n}{q_n} = x,$$

o que permite recuperar x a partir de a_0, a_1, a_2, \dots , e dá sentido à igualdade $x = [a_0; a_1, a_2, \dots]$ quando a fração contínua de x é infinita (i.e., quando x é irracional).

Observação 3.6. A proposição anterior implica que, para todo α irracional, a desigualdade $|\alpha - p/q| < 1/q^2$ tem infinitas soluções racionais p/q . Este fato é conhecido como o Teorema de Dirichlet.

É interessante notar que, se $\alpha = r/s \in \mathbb{Q}$, a desigualdade $|\alpha - p/q| < 1/q^2$ tem apenas um número finito de soluções racionais p/q . De fato, $|r/s - p/q| < 1/q^2$ equivale a $|qr - ps| < s/q$, o que implica que $q \leq s$.

A seguinte proposição mostra que os convergentes pares formam uma sequência crescente, e que os convergentes ímpares formam uma sequência decrescente. Além disso todos os convergentes ímpares são maiores do que todos os convergentes pares.

Proposição 3.7. Para todo $k \geq 0$, temos

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq x \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}.$$

DEMONSTRAÇÃO: O resultado segue dos seguintes fatos gerais. Para

todo $n \geq 0$, temos que

$$\begin{aligned} \frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} &= \frac{a_{n+2}p_{n+1} + p_n}{a_{n+2}q_{n+1} + q_n} - \frac{p_n}{q_n} \\ &= \frac{a_{n+2}(p_{n+1}q_n - p_nq_{n+1})}{q_n(a_{n+2}q_{n+1} + q_n)} = \frac{(-1)^n a_{n+2}}{q_{n+2}q_n} \end{aligned}$$

é positivo para n par e negativo para n ímpar. Além disso, para todo $n \geq 0$, temos que $x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1}q_n + q_{n-1})q_n}$ é positivo para n par e negativo para n ímpar. \square

Proposição 3.8. *Sejam a_0, a_1, \dots, a_n inteiros com $a_k > 0$, $\forall k \geq 1$, e seja $(p_k/q_k)_{k \geq 0}$ a sequência de reduzidas da fração contínua $[a_0; a_1, a_2, \dots, a_n]$. Então o conjunto dos números reais cuja representação por frações contínuas começa com a_0, a_1, \dots, a_n é o intervalo*

$$\begin{aligned} I(a_0, a_1, \dots, a_n) &= \left\{ \frac{p_n}{q_n} \right\} \cup \{[a_0, a_1, \dots, a_n, \alpha], \alpha > 1\} \\ &= \begin{cases} \left[\frac{p_n}{q_n}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}} \right) & \text{se } n \text{ é par} \\ \left(\frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{p_n}{q_n} \right] & \text{se } n \text{ é ímpar.} \end{cases} \end{aligned}$$

Além disso, a função $G : (1, +\infty) \rightarrow I(a_0, a_1, \dots, a_n)$ dada por $G(\alpha) = [a_0; a_1, a_2, \dots, a_n, \alpha]$ é monótona, sendo crescente para n ímpar e decrescente para n par.

DEMONSTRAÇÃO: É suficiente notar que, como na prova do corolário anterior, $G(\alpha) = [a_0; a_1, a_2, \dots, a_n, \alpha] = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}} = \frac{p_n}{q_n} + \frac{(-1)^n}{(\alpha q_n + q_{n-1})q_n}$, e portanto G é crescente para n ímpar e decrescente para n par. Assim, como $G(1) = \frac{p_n + p_{n-1}}{q_n + q_{n-1}}$ e $\lim_{\alpha \rightarrow +\infty} G(\alpha) = \frac{p_n}{q_n}$, temos

$$G((1, +\infty)) = \begin{cases} \left(\frac{p_n}{q_n}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}} \right) & \text{se } n \text{ é par} \\ \left[\frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{p_n}{q_n} \right) & \text{se } n \text{ é ímpar.} \end{cases}$$

Portanto,

$$\begin{aligned}
 I(a_0, a_1, \dots, a_n) &= \left\{ \frac{p_n}{q_n} \right\} \cup \{[a_0, a_1, \dots, a_n, \alpha], \alpha > 1\} \\
 &= \left\{ \frac{p_n}{q_n} \right\} \cup G((1, +\infty)) \\
 &= \begin{cases} \left[\frac{p_n}{q_n}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}} \right] & \text{se } n \text{ é par} \\ \left(\frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{p_n}{q_n} \right] & \text{se } n \text{ é ímpar.} \end{cases}
 \end{aligned}$$

□

Proposição 3.9. *Dados inteiros a_0, a_1, a_2, \dots , com $a_k > 0, \forall k \geq 1$, existe um único número real α (que é irracional) cuja representação por frações contínuas é $[a_0; a_1, a_2, \dots]$.*

DEMONSTRAÇÃO: Considere as sequências (p_n) e (q_n) definidas pelas recorrências

$$p_{n+2} = a_{n+2}p_{n+1} + p_n \quad \text{e} \quad q_{n+2} = a_{n+2}q_{n+1} + q_n$$

para todo $n \geq 0$, com $p_0 = a_0$, $p_1 = a_0a_1 + 1$, $q_0 = 1$ e $q_1 = a_1$. Temos, como na proposição 3.7,

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}, \forall k \geq 0.$$

Assim, considerando os intervalos fechados

$$I_k = \left[\frac{p_{2k}}{q_{2k}}, \frac{p_{2k+1}}{q_{2k+1}} \right],$$

temos $I_{k+1} \subset I_k, \forall k \geq 0$, e portanto, como

$$|I_k| = \frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = \frac{p_{2k+1}q_{2k} - p_{2k}q_{2k+1}}{q_{2k+1}q_{2k}} = \frac{(-1)^{2k}}{q_{2k+1}q_{2k}} = \frac{1}{q_{2k+1}q_{2k}}$$

tende a 0 quando k tende a infinito, existe $\alpha \in \mathbb{R}$ tal que

$$\bigcap_{k \geq 0} I_k = \{\alpha\}.$$

Como, para todo $k \geq 0$,

$$[a_0; a_1, a_2, \dots, a_{2k}] = \frac{p_{2k}}{q_{2k}} \leq \alpha \leq \frac{p_{2k+1}}{q_{2k+1}} = [a_0; a_1, a_2, \dots, a_{2k}, a_{2k+1}]$$

e, da proposição anterior, $[a_0; a_1, a_2, \dots, a_{2k}]$ e $[a_0; a_1, a_2, \dots, a_{2k}, a_{2k+1}]$ pertencem a $I(a_0; a_1, a_2, \dots, a_{2k})$, que é um intervalo, segue que $\alpha \in I(a_0; a_1, a_2, \dots, a_{2k})$, e portanto a fração contínua de α começa com a_0, a_1, \dots, a_{2k} , para todo $k \geq 0$, donde a representação por frações contínuas de α é $[a_0; a_1, a_2, \dots]$.

Note que, como a representação por frações contínuas de α é infinita, α é irracional. \square

Exemplo 3.10. Temos

- $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, \dots]$, portanto

$$\frac{p_0}{q_0} = 3, \quad \frac{p_1}{q_1} = \frac{22}{7}, \quad \frac{p_2}{q_2} = \frac{333}{106}, \quad \frac{p_3}{q_3} = \frac{355}{113} \dots$$

- $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots, 1, 1, 2n, \dots]$ (veja o exerc. 3.9).

- $\sqrt{2} = [1; 2, 2, 2, \dots]$ pois

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2} + 1} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}} = \dots$$

- $\frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, \dots]$ pois

$$\frac{1+\sqrt{5}}{2} = 1 + \frac{1}{\frac{1+\sqrt{5}}{2}} = 1 + \frac{1}{1 + \frac{1}{\frac{1+\sqrt{5}}{2}}} = \dots$$

Isto prova em particular que $\sqrt{2}$ e $\frac{1+\sqrt{5}}{2}$ são irracionais, pois suas frações contínuas são infinitas. Daí segue também que $\sqrt{2} - 1 = [0; 2, 2, 2, \dots]$ e $\frac{\sqrt{5}-1}{2} = [0; 1, 1, 1, \dots]$ são pontos fixos da transformação de Gauss g .

3.1 Reduzidas e Boas Aproximações

Teorema 3.11. *Temos, para todo $n \in \mathbb{N}$,*

$$\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

Além disso,

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2} \quad \text{ou} \quad \left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{2q_{n+1}^2}.$$

DEMONSTRAÇÃO: O número x sempre pertence ao segmento de extremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$ cujo comprimento é

$$\left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \left| \frac{(-1)^n}{q_n q_{n+1}} \right| = \frac{1}{q_n q_{n+1}} \implies \left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Além disso, se

$$\left| x - \frac{p_n}{q_n} \right| \geq \frac{1}{2q_n^2} \quad \text{e} \quad \left| x - \frac{p_{n+1}}{q_{n+1}} \right| \geq \frac{1}{2q_{n+1}^2},$$

então

$$\frac{1}{q_n q_{n+1}} = \left| x - \frac{p_n}{q_n} \right| + \left| x - \frac{p_{n+1}}{q_{n+1}} \right| \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} \implies q_{n+1} = q_n,$$

absurdo. □

Observação 3.12. *De fato $\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{a_{n+1} q_n^2}$. Quanto maior for a_{n+1} melhor será a aproximação $\frac{p_n}{q_n}$ de x .*

Teorema 3.13 (Hurwitz, Markov). *Para todo α irracional e todo inteiro $n \geq 1$, temos*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}$$

para pelo menos um racional

$$\frac{p}{q} \in \left\{ \frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}} \right\}.$$

Em particular, a desigualdade acima tem infinitas soluções racionais p/q .

DEMONSTRAÇÃO: Suponha que o teorema seja falso. Então, pela proposição 3.4, existe α irracional, $n \geq 1$ com $\alpha_n + \beta_n \leq \sqrt{5}$, $\alpha_{n+1} + \beta_{n+1} \leq \sqrt{5}$ e $\alpha_{n+2} + \beta_{n+2} \leq \sqrt{5}$. Devemos portanto ter $a_{n+1} = a_{n+2} = 1$ já que claramente $a_k \leq 2$ para $k = n, n+1, n+2$ e se algum $a_k = 2$ com $k = n+1, n+2$, teríamos $a_k + \beta_k \geq 2 + \frac{1}{3} > \sqrt{5}$, absurdo.

Sejam $x = 1/\alpha_{n+2}$ e $y = \beta_{n+1}$. As desigualdades acima se traduzem em

$$\frac{1}{1+x} + \frac{1}{y} \leq \sqrt{5}, \quad 1+x+y \leq \sqrt{5} \quad \text{e} \quad \frac{1}{x} + \frac{1}{1+y} \leq \sqrt{5}.$$

Temos

$$\begin{aligned} 1+x+y \leq \sqrt{5} &\implies 1+x \leq \sqrt{5}-y \\ &\implies \frac{1}{1+x} + \frac{1}{y} \geq \frac{1}{\sqrt{5}-y} + \frac{1}{y} = \frac{\sqrt{5}}{y(\sqrt{5}-y)} \end{aligned}$$

e portanto $y(\sqrt{5}-y) \geq 1 \implies y \geq \frac{\sqrt{5}-1}{2}$. Por outro lado temos

$$\begin{aligned} x \leq \sqrt{5}-1-y &\implies \frac{1}{x} + \frac{1}{1+y} \geq \frac{1}{\sqrt{5}-1-y} + \frac{1}{1+y} \\ &= \frac{\sqrt{5}}{(1+y)(\sqrt{5}-1-y)} \end{aligned}$$

e portanto $(1+y)(\sqrt{5}-1-y) \geq 1 \implies y \leq \frac{\sqrt{5}-1}{2}$, e portanto devemos ter $y = \frac{\sqrt{5}-1}{2}$, o que é absurdo pois $y = \beta_{n+1} = \frac{q_{n-1}}{q_n} \in \mathbb{Q}$. \square

Observação 3.14. Em particular provamos que $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$ tem infinitas soluções racionais $\frac{p}{q}$, para todo α irracional. O número $\sqrt{5}$ é o maior com essa propriedade. De fato, se

$$\varepsilon > 0, \quad \alpha = \frac{1+\sqrt{5}}{2} \quad \text{e} \quad \left| \alpha - \frac{p}{q} \right| < \frac{1}{(\sqrt{5}+\varepsilon)q^2},$$

temos

$$\begin{aligned} \left| q \left(\frac{1 + \sqrt{5}}{2} \right) - p \right| &< \frac{1}{(\sqrt{5} + \varepsilon)q} \\ \Rightarrow \left| q \left(\frac{1 + \sqrt{5}}{2} \right) - p \right| \left| q \left(\frac{1 - \sqrt{5}}{2} \right) - p \right| &< \frac{\left| \frac{1 - \sqrt{5}}{2} - \frac{p}{q} \right|}{\sqrt{5} + \varepsilon}, \end{aligned}$$

ou seja,

$$|p^2 - pq - q^2| < \left| \frac{1 + \sqrt{5}}{2} - \frac{p}{q} - \sqrt{5} \right| / (\sqrt{5} + \varepsilon).$$

Se q é grande, $1/q^2$ é pequeno, e $\frac{1+\sqrt{5}}{2} - \frac{p}{q}$ é muito próximo de 0, donde o lado direito da desigualdade é muito próximo de $\frac{\sqrt{5}}{\sqrt{5}+\varepsilon} < 1$, absurdo, pois $|p^2 - pq - q^2| \geq 1$, de fato se $p^2 - pq - q^2 = 0$ teríamos

$$\left(\frac{p}{q} \right)^2 - \left(\frac{p}{q} \right) - 1 = 0 \Rightarrow \frac{p}{q} \in \left\{ \frac{1 + \sqrt{5}}{2}, \frac{1 - \sqrt{5}}{2} \right\},$$

o que é absurdo, pois $\frac{p}{q} \in \mathbb{Q}$.

Outra maneira de ver que, para todo $\varepsilon > 0$, $\left| \frac{1+\sqrt{5}}{2} - \frac{p}{q} \right| < \frac{1}{(\sqrt{5}+\varepsilon)q^2}$ tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$ é observar que as melhores aproximações racionais de $\frac{1+\sqrt{5}}{2}$ são as reduzidas $\frac{p_n}{q_n}$ de sua fração contínua $[1; 1, 1, 1, \dots]$ (ver próxima seção), para as quais temos $\left| \frac{1+\sqrt{5}}{2} - \frac{p_n}{q_n} \right| = \frac{1}{(\alpha_{n+1} + \beta_{n+1})q_n^2}$, com $\alpha_{n+1} + \beta_{n+1}$ se aproximando cada vez mais de

$$[1; 1, 1, 1, \dots] + [0; 1, 1, 1, \dots] = \frac{1 + \sqrt{5}}{2} + \frac{\sqrt{5} - 1}{2} = \sqrt{5}.$$

3.2 Boas Aproximações são Reduzidas

O próximo teorema (e seu corolário 3.17) caracteriza as reduzidas em termos do erro reduzido da aproximação de x por p/q , o qual é, por definição, $|qx - p|$, a razão entre $|x - p/q|$ e o erro máximo da aproximação

por falta com denominador q , que é $1/q$.

Teorema 3.15. *Para todo $p, q \in \mathbb{Z}$, com $0 < q < q_{n+1}$ temos*

$$|q_n x - p_n| \leq |q x - p|.$$

Além disso, se $0 < q < q_n$ a desigualdade acima é estrita.

DEMONSTRAÇÃO: Como $\text{mdc}(p_n, q_n) = 1$, temos que se $\frac{p}{q} = \frac{p_n}{q_n}$ então $p = kp_n$ e $q = kq_n$ para algum inteiro $k \neq 0$ e neste caso o resultado é claro. Assim, podemos supor que $\frac{p}{q} \neq \frac{p_n}{q_n}$ de modo que

$$\left| \frac{p}{q} - \frac{p_n}{q_n} \right| \geq \frac{1}{qq_n} > \frac{1}{q_n q_{n+1}}$$

já que $q < q_{n+1}$. Assim, $\frac{p}{q}$ está fora do intervalo de extremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$ e portanto

$$\left| x - \frac{p}{q} \right| \geq \min \left\{ \left| \frac{p}{q} - \frac{p_n}{q_n} \right|, \left| \frac{p}{q} - \frac{p_{n+1}}{q_{n+1}} \right| \right\} \geq \frac{1}{qq_{n+1}}$$

o que implica

$$|q x - p| \geq \frac{1}{q_{n+1}} \geq |q_n x - p_n|.$$

Além disso, a igualdade só pode ocorrer se $x = \frac{p_{n+1}}{q_{n+1}}$, donde $a_{n+1} \geq 2$, e $q_{n+1} > 2q_n$, pois numa fração contínua finita, como no algoritmo de Euclides, o último coeficiente a_n é sempre maior que 1. Nesse caso, se $q < q_n$, teremos

$$\begin{aligned} \left| x - \frac{p}{q} \right| &\geq \left| \frac{p}{q} - \frac{p_n}{q_n} \right| - \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| \\ &\geq \frac{1}{qq_n} - \frac{1}{q_n q_{n+1}} = \frac{q_{n+1} - q}{qq_n q_{n+1}} > \frac{1}{qq_{n+1}} \end{aligned}$$

o que implica

$$|q x - p| > \frac{1}{q_{n+1}} \geq |q_n x - p_n|.$$

□

Corolário 3.16. *Para todo $q < q_n$,*

$$\left| x - \frac{p_n}{q_n} \right| < \left| x - \frac{p}{q} \right|$$

Corolário 3.17. *Se $|qx - p| < |q'x - p'|$, para todo p' e $q' \leq q$ tais que $\frac{p}{q} \neq \frac{p'}{q'}$, então p/q é uma reduzida da fração contínua de x .*

DEMONSTRAÇÃO: Tome n tal que $q_n \leq q < q_{n+1}$. Pelo teorema, $|q_n x - p_n| \leq |qx - p|$, e portanto $p/q = p_n/q_n$. \square

Teorema 3.18. *Se $|x - \frac{p}{q}| < \frac{1}{2q^2}$ então $\frac{p}{q}$ é uma reduzida da fração contínua de x .*

DEMONSTRAÇÃO: Seja n tal que $q_n \leq q < q_{n+1}$. Suponha que $\frac{p}{q} \neq \frac{p_n}{q_n}$. Como na demonstração do teorema anterior, $|x - \frac{p}{q}| \geq \frac{1}{qq_{n+1}}$ e assim $\frac{p}{q}$ está fora do intervalo de extremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$. Temos duas possibilidades:

(a) Se $q \geq \frac{q_{n+1}}{2}$ então $|x - \frac{p}{q}| \geq \frac{1}{qq_{n+1}} \geq \frac{1}{2q^2}$, absurdo.

(b) Se $q < \frac{q_{n+1}}{2}$,

$$\begin{aligned} \left| x - \frac{p}{q} \right| &\geq \left| \frac{p_n}{q_n} - \frac{p}{q} \right| = \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| \\ &\geq \frac{1}{qq_n} - \frac{1}{q_n q_{n+1}} = \frac{q_{n+1} - q}{qq_n q_{n+1}} \\ &> \frac{1}{2qq_n} \geq \frac{1}{2q^2} \end{aligned}$$

o que também é um absurdo. \square

Dado $\alpha \in \mathbb{R}$, definimos a *ordem* de α por

$$\text{ord } \alpha \stackrel{\text{def}}{=} \sup \left\{ \nu > 0 \mid \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\nu} \text{ tem infinitas soluções } \frac{p}{q} \in \mathbb{Q} \right\}.$$

Observemos que a ordem de todo número irracional pode ser calculada a partir de sua fração contínua.

Teorema 3.19. *Seja α um número irracional, e sejam $[a_0; a_1, a_2, a_3 \dots]$ sua fração contínua e $\{\frac{p_n}{q_n}\}$ suas convergentes. Então*

$$\text{ord } \alpha = 1 + \limsup_{n \rightarrow \infty} \frac{\ln q_{n+1}}{\ln q_n} = 2 + \limsup_{n \rightarrow \infty} \frac{\ln a_{n+1}}{\ln q_n}.$$

DEMONSTRAÇÃO: Sabemos que as melhores aproximações por racionais são obtidas a partir das convergentes da fração contínua, assim para calcular a ordem, basta calcular a ordem gerada pelos convergentes. Seja $s_n > 0$ um número real tal que $\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{q_n^{s_n}}$. Pelo teorema 3.11 sabemos que $\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}$ e

$$\left| \alpha - \frac{p_n}{q_n} \right| > \frac{1}{2} \left(\left| \alpha - \frac{p_n}{q_n} \right| + \left| \alpha - \frac{p_{n+1}}{q_{n+1}} \right| \right) = \frac{1}{2} \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{1}{2q_n q_{n+1}}.$$

Logo temos que

$$\frac{1}{2q_n q_{n+1}} \leq \frac{1}{q_n^{s_n}} \leq \frac{1}{q_n q_{n+1}},$$

e tomando o logaritmo obtemos

$$\ln 2 + \ln q_n + \ln q_{n+1} \geq s_n \ln q_n \geq \ln q_n + \ln q_{n+1}.$$

Portanto $\text{ord } \alpha = \limsup_{n \rightarrow \infty} s_n = 1 + \limsup_{n \rightarrow \infty} \frac{\ln q_{n+1}}{\ln q_n}$. Para mostrar a segunda igualdade, observemos que $q_{n+1} = a_{n+1}q_n + q_{n-1}$, assim

$$a_{n+1}q_n < q_{n+1} < (a_{n+1} + 1)q_n,$$

agora tomando o logaritmo e dividindo por $\ln q_n$ obtemos

$$\frac{\ln a_{n+1}}{\ln q_n} + 1 < \frac{\ln q_{n+1}}{\ln q_n} < \frac{\ln(a_{n+1} + 1)}{\ln q_n} + 1,$$

portanto $\limsup_{n \rightarrow \infty} \frac{\ln q_{n+1}}{\ln q_n} = 1 + \limsup_{n \rightarrow \infty} \frac{\ln a_{n+1}}{\ln q_n}$. □

Observe que usando a fração contínua de e (ver exercícios), é possível provar que $\text{ord}(e) = 2$.

3.3 Frações Contínuas Periódicas

Nesta seção provaremos que os números reais com fração contínua periódica são exatamente as raízes de equações do segundo grau com coeficientes inteiros.

Lembramos que na representação de x por fração contínua, a_n , α_n são definidos por recursão por

$$\alpha_0 = x, \quad a_n = \lfloor \alpha_n \rfloor, \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}$$

e temos

$$\alpha_n = \frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}}, \quad \forall n \in \mathbb{N}.$$

Isso dá uma prova explícita do fato de que se a fração contínua de x é periódica, então x é raiz de uma equação do segundo grau com coeficientes inteiros. De fato, se $\alpha_{n+k} = \alpha_n$, $n \in \mathbb{N}$, $k \in \mathbb{N}_{>0}$ segue que

$$\frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}} = \frac{p_{n+k-2} - q_{n+k-2}x}{q_{n+k-1}x - p_{n+k-1}},$$

então $Ax^2 + Bx + C = 0$, onde

$$A = q_{n-1}q_{n+k-2} - q_{n-2}q_{n+k-1}$$

$$B = p_{n+k-1}q_{n-2} + p_{n-2}q_{n+k-1} - p_{n+k-2}q_{n-1} - p_{n-1}q_{n+k-2}$$

$$C = p_{n-1}p_{n+k-2} - p_{n-2}p_{n+k-1}.$$

Note que o coeficiente de x^2 é não-nulo, pois $\frac{q_{n-1}}{q_{n-2}}$ é uma fração irredutível de denominador q_{n-2} , pois $p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^n$, e $\frac{q_{n+k-1}}{q_{n+k-2}}$ é uma fração irredutível de denominador $q_{n+k-2} > q_{n-2}$, donde $\frac{q_{n-1}}{q_{n-2}} \neq \frac{q_{n+k-1}}{q_{n+k-2}}$, logo $q_{n-1}q_{n+k-2} - q_{n-2}q_{n+k-1} \neq 0$.

Vamos provar agora um resultado devido a Lagrange segundo o qual se x é uma *irracionalidade quadrática*, isto é, se x é um irracional do tipo $r \pm \sqrt{s}$, $r, s \in \mathbb{Q}$, $s > 0$, então a fração contínua de x é periódica, i.e., existem $n \in \mathbb{N}$ e $k \in \mathbb{N}_{>0}$ com $\alpha_{n+k} = \alpha_n$. Neste caso, existem a , b , c inteiros tais que $ax^2 + bx + c = 0$, com $b^2 - 4ac > 0$ e $\sqrt{b^2 - 4ac}$ irracional. Como $x = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$, temos

$$ax^2 + bx + c = 0$$

$$\implies a \left(\frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}} \right)^2 + b \left(\frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}} \right) + c = 0$$

$$\implies A_n \alpha_n^2 + B_n \alpha_n + C_n = 0,$$

onde

$$\begin{aligned} A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \\ B_n &= 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2} \\ C_n &= ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2. \end{aligned}$$

Note que $C_n = A_{n-1}$. Vamos provar que existe $M > 0$ tal que $0 < |A_n| \leq M$ para todo $n \in \mathbb{N}$, e portanto $0 < |C_n| \leq M$, $\forall n \in \mathbb{N}$:

$$A_n = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 = aq_{n-1}^2 \left(x - \frac{p_{n-1}}{q_{n-1}} \right) \left(\bar{x} - \frac{p_{n-1}}{q_{n-1}} \right),$$

onde x e \bar{x} são as raízes de $aX^2 + bX + c = 0$, mas

$$\begin{aligned} \left| x - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{q_{n-1}^2} \leq 1 &\implies |A_n| = aq_{n-1}^2 \left| x - \frac{p_{n-1}}{q_{n-1}} \right| \left| \bar{x} - \frac{p_{n-1}}{q_{n-1}} \right| \\ &\leq a \left(|\bar{x} - x| + \left| x - \frac{p_{n-1}}{q_{n-1}} \right| \right) \\ &\leq M \stackrel{\text{def}}{=} a(|\bar{x} - x| + 1). \end{aligned}$$

Notemos agora que, para qualquer $n \in \mathbb{N}$,

$$B_n^2 - 4A_nC_n = (p_{n-1}q_{n-2} - p_{n-2}q_{n-1})^2(b^2 - 4ac) = b^2 - 4ac.$$

Portanto

$$\begin{aligned} B_n^2 &\leq 4A_nC_n + b^2 - 4ac \leq 4M^2 + b^2 - 4ac \\ \implies B_n &\leq M' \stackrel{\text{def}}{=} \sqrt{4M^2 + b^2 - 4ac}. \end{aligned}$$

Provamos assim que A_n , B_n e C_n estão uniformemente limitados, donde há apenas um número finito de possíveis equações $A_nX^2 + B_nX + C_n = 0$, e portanto de possíveis valores de α_n . Assim, necessariamente $\alpha_{n+k} = \alpha_n$ para alguma escolha de $n \in \mathbb{N}$, $k \in \mathbb{N}_{>0}$.

3.4 Os Espectros de Markov e Lagrange

Seja α um número irracional. De acordo com o teorema de Dirichlet, a desigualdade $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$ tem uma infinidade de soluções racionais

p/q . Markov e Hurwitz melhoraram este resultado, provando que, para todo irracional α , a desigualdade $\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5} \cdot q^2}$ tem uma infinidade de soluções racionais, e que $\sqrt{5}$ é a melhor constante com esta propriedade: para $\alpha = \frac{1 + \sqrt{5}}{2}$, e para qualquer $\varepsilon > 0$, a desigualdade $\left| \alpha - \frac{p}{q} \right| < \frac{1}{(\sqrt{5} + \varepsilon)q^2}$ tem apenas um número finito de soluções (veja o Teorema 3.13). Entretanto, fixado α irracional, pode-se esperar resultados melhores, o que nos leva a associar a cada α a sua constante de melhor aproximação

$$\begin{aligned} k(\alpha) &= \sup \left\{ k > 0 \mid \left| \alpha - \frac{p}{q} \right| < \frac{1}{kq^2} \text{ tem infinitas soluções racionais } p/q \right\} \\ &= \limsup_{p, q \in \mathbb{Z}, q \rightarrow \infty} (|q(q\alpha - p)|^{-1}) \in \mathbb{R} \cup \{+\infty\}. \end{aligned}$$

Nossa discussão inicial mostra que $k(\alpha) \geq \sqrt{5}$ para todo $\alpha \in \mathbb{R}$, e

$$k\left(\frac{1 + \sqrt{5}}{2}\right) = \sqrt{5}.$$

Não é difícil provar que $k(\alpha) = +\infty$ para quase todo $\alpha \in \mathbb{R}$. Estaremos interessados nos $\alpha \in \mathbb{R}$ tais que $k(\alpha) < +\infty$, e, mais particularmente, na imagem da função k , isto é, no conjunto $L = \{k(\alpha) \mid \alpha \in \mathbb{R} \setminus \mathbb{Q} \text{ e } k(\alpha) < +\infty\}$. Este conjunto é conhecido como o *espectro de Lagrange*.

Segue da proposição 3.4 (e do Teorema 3.18) uma fórmula para $k(\alpha)$: escrevemos α em fração contínua, $\alpha = [a_0, a_1, a_2, \dots]$ e definimos, para $n \in \mathbb{N}$, $\alpha_n = [a_n, a_{n+1}, a_{n+2}, \dots]$ e $\beta_n = [0, a_{n-1}, a_{n-2}, \dots, a_1]$. Temos então $k(\alpha) = \limsup_{n \rightarrow \infty} (\alpha_n + \beta_n)$. Em particular, $k(\alpha) < \infty \iff (a_n)$ é limitado.

É interessante observar que se mudássemos um pouco as funções envolvidas na definição do espectro de Lagrange ele passaria a ser um conjunto bem menos interessante: se para $f: \mathbb{R} \rightarrow \mathbb{R}_+$ decrescente considerarmos o conjunto $k_f(\alpha)$ definido por

$$\sup \left\{ k > 1 \mid \left| \alpha - \frac{p}{q} \right| < \frac{f(q)}{k} \text{ tem infinitas soluções racionais } \frac{p}{q} \right\}$$

então, caso tenhamos $\lim_{q \rightarrow +\infty} q^2 f(q) = 0$, a imagem de k_f seria $(0, +\infty]$ (ou $[0, +\infty]$, se consideramos $\sup(\emptyset) = 0$ neste contexto) e, caso $\lim_{q \rightarrow +\infty} q^2 f(q) = +\infty$, então a imagem de k_f seria $\{+\infty\}$.

O conjunto L codifica uma série de propriedades diofantinas de números reais, e vem sendo estudado há bastante tempo. Talvez o primeiro resultado não-trivial sobre ele se deva a Markov, que provou em 1879 (ver [96] e [97]) que

$$L \cap (-\infty, 3) = \left\{ k_1 = \sqrt{5} < k_2 = 2\sqrt{2} < k_3 = \frac{\sqrt{221}}{5} < \dots \right\},$$

onde (k_n) é uma sequência convergente a 3 tal que $k_n \notin \mathbb{Q}$ mas $k_n^2 \in \mathbb{Q}$ para todo n (na verdade Markov provou que os k_n são exatamente os números da forma $\sqrt{9 - \frac{4}{z^2}}$, onde z é um inteiro positivo tal que existem inteiros positivos x, y de modo que (x, y, z) é uma solução da equação de Markov $x^2 + y^2 + z^2 = 3xyz$ - veja a seção 4.3.1 e o excelente artigo [21]). Assim, o “começo” do espectro de Lagrange é discreto. Essa afirmação não é verdadeira para todo o conjunto L . Marshall Hall provou em 1947 ([64]) que L contém toda uma semi-reta (por exemplo $[6, +\infty)$), e G. Freiman determinou em 1975 a maior semi-reta que está contida em L , que é

$$\left[\frac{2221564096 + 283748\sqrt{462}}{491993569}, +\infty \right).$$

Estes dois últimos resultados baseam-se fortemente no estudo de somas de conjuntos de Cantor regulares, cuja relação com o espectro de Lagrange tem origem na fórmula que apresentamos para $k(\alpha)$.

Por exemplo, o resultado que M. Hall enuncia em seu artigo [64] é o seguinte: se $C(4)$ é o conjunto de Cantor regular dos reais de $[0, 1]$ em cuja fração contínua aparecem apenas os coeficientes 1, 2, 3 e 4 então $C(4) + C(4) = [\sqrt{2} - 1, 4(\sqrt{2} - 1)]$, do qual não é difícil deduzir que $L \supset [6, +\infty)$ usando a fórmula para $k(\alpha)$.

De $k(\alpha) = \limsup_{n \rightarrow \infty} (\alpha_n + \beta_n)$ podemos obter a seguinte caracterização do espectro de Lagrange: seja $\Sigma = (\mathbb{N}^*)^{\mathbb{N}}$, o conjunto das sequências bi-infinitas de inteiros positivos, e $\sigma: \Sigma \rightarrow \Sigma$ o shift definido por $\sigma((a_n)_{n \in \mathbb{Z}}) = (a_{n+1})_{n \in \mathbb{Z}}$. Se $f: \Sigma \rightarrow \mathbb{R}$ é definida por

$$f((a_n)_{n \in \mathbb{Z}}) = \alpha_0 + \beta_0 = [a_0, a_1, a_2, \dots] + [0; a_{-1}, a_{-2}, \dots]$$

então $L = \{\limsup_{n \rightarrow +\infty} f(\sigma^n \underline{\theta}), \underline{\theta} \in \Sigma\}$. Outro conjunto de números reais de nosso interesse é o *espectro de Markov*, que é o conjunto $M =$

$\{\sup_{n \rightarrow \infty} f(\sigma^n \underline{\theta}), \underline{\theta} \in \Sigma\}$. O espectro de Markov M tem a seguinte interpretação aritmética:

$$\left\{ \left(\inf_{(x,y) \in \mathbb{Z}^2 \setminus (0,0)} |f(x,y)| \right)^{-1}, f(x,y) = ax^2 + bxy + cy^2, b^2 - 4ac = 1 \right\}.$$

São fatos conhecidos que L e M são subconjuntos fechados da reta e que $L \subset M$ (ver [45]). Na referência [108] são provados resultados sobre propriedades geométricas (relativas a geometria fractal) dos espectros de Markov e Lagrange, que envolvem resultados delicados sobre somas de conjuntos de Cantor regulares.

Problemas Propostos

3.1. *Seja n um número natural. Determine os possíveis valores de x tais que $\frac{1}{x} = [1, 1, \dots, 1, x]$, onde aparecem n uns na fração contínua.*

3.2. *Seja*

$$\frac{p_n}{q_n} = \frac{1}{1 + \frac{1^2}{2 + \frac{3^2}{2 + \frac{5^2}{\ddots 2 + \frac{(2n-3)^2}{2}}}}}$$

a n -ésima convergente da fração contínua

$$\frac{1}{1 + \frac{1^2}{2 + \frac{3^2}{2 + \frac{5^2}{2 + \frac{7^2}{\ddots}}}}}$$

Demonstrar que $\frac{p_n}{q_n} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots + (-1)^{n-1} \frac{1}{2n-1}$.

3.3. *Demonstre que, para todo inteiro positivo a , temos as seguintes expansões em frações contínuas periódicas:*

$$(a) \sqrt{a^2 + 1} = [a, 2a].$$

$$(b) \sqrt{a^2 - 1} = [a - 1, \overline{1, 2a - 2}].$$

$$(c) \sqrt{a^2 - 2} = [a - 1, \overline{1, a - 2, 1, 2a - 2}].$$

$$(d) \sqrt{a^2 - a} = [a - 1, \overline{2, 2a - 2}].$$

3.4. Encontre as frações contínuas de $\sqrt{a^2 + 4}$ e $\sqrt{a^2 - 4}$.

3.5. Seja $\alpha = [a_0; a_1, a_2, \dots] \in \mathbb{R}$. Prove que, se $q_n \leq q < q_{n+1}$, $\text{mdc}(p, q) = 1$ e $p/q \neq p_n/q_n$ então $|\alpha - p/q| \leq |\alpha - p_n/q_n|$ se, e somente se, $\frac{p}{q} = \frac{p_{n+1} - r p_n}{q_{n+1} - r q_n}$, onde $r \in \mathbb{N}$ é tal que vale uma das seguintes condições:

$$(i) \quad 0 < r < a_{n+1}/2;$$

$$(ii) \quad r = a_{n+1}/2 \text{ e } \alpha_{n+2}\beta_{n+1} \geq 1.$$

3.6. Seja $\alpha = [a_0; a_1, a_2, \dots] \in \mathbb{R}$. Prove que, se $q_n \leq q < q_{n+1}$, $\text{mdc}(p, q) = 1$ e $p/q \neq p_n/q_n$ então $|\alpha - p/q| < 1/q^2$ se, e somente se vale pelo menos uma das seguintes condições:

$$(i) \quad a_{n+1} \geq 2, \quad \frac{p}{q} = \frac{p_{n+1} - p_n}{q_{n+1} - q_n} \text{ e } a_{n+1} - 2 + \beta_{n+1} < \alpha_{n+2};$$

$$(ii) \quad a_{n+1} \geq 2, \quad \frac{p}{q} = \frac{p_n + p_{n-1}}{q_n + q_{n-1}} \text{ e } (\alpha_{n+1} - 2)\beta_{n+1} < 1.$$

3.7. Seja $\alpha = [a_0; a_1, a_2, \dots]$ um número real.

(a) Prove que, se $\text{ord } \alpha > 2$ então existe $\lambda > 1$ tal que, para infinitos inteiros positivos n , temos $a_n \geq \lambda^n$.

(b) Prove que $\text{ord } \alpha \geq 1 + \exp(\limsup_{n \rightarrow \infty} \frac{\log \log(a_n + 1)}{n})$.

(c) Mostre que, para todo $c \geq 2$, existe $\alpha \in \mathbb{R}$ tal que $\text{ord } \alpha = 1 + \exp(\limsup_{n \rightarrow \infty} \frac{\log \log(a_n + 1)}{n}) = c$.

(d) Determine $\text{ord } \alpha$ se $a_n = 2^n, \forall n \geq 0$.

3.8. Prove que, para todo $\alpha \in \mathbb{R}$, $\limsup_{n \rightarrow +\infty} \cos^n(n\alpha) = 1$.

3.9. Este exercício, baseado em [36], tem como objetivo calcular a fração contínua de e .

(a) São dadas as sequências $\{A_n\}$, $\{B_n\}$ e $\{C_n\}$ definidas por

$$\begin{aligned} A_n &= \int_0^1 \frac{x^n(x-1)^n}{n!} e^x dx, \\ B_n &= \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x dx, \\ C_n &= \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x dx. \end{aligned}$$

Mostrar que para todo $n \geq 1$ se cumprem as relações

$$(i) \quad A_n + B_{n-1} + C_{n-1} = 0,$$

$$(ii) \quad B_n - 2nA_n + C_{n-1} = 0,$$

$$(iii) \quad A_n - B_n + C_n = 0.$$

(b) Dadas as sequências $\{p_n\}$ e $\{q_n\}$ definidas recursivamente como $p_0 = q_0 = p_1 = 1$, $q_1 = 0$ e

$$\begin{aligned} p_{3n} &= p_{3n-1} + p_{3n-2}, & q_{3n} &= q_{3n-1} + q_{3n-2} \\ p_{3n+1} &= 2np_{3n} + p_{3n-1}, & q_{3n+1} &= 2nq_{3n} + q_{3n-1} \\ p_{3n+2} &= p_{3n+1} + p_{3n}, & q_{3n+2} &= q_{3n+1} + q_{3n} \end{aligned}$$

Mostrar por indução que para todo $n \geq 0$ se cumprem as relações

$$A_n = q_{3n}e - p_{3n}, \quad B_n = p_{3n+1} - q_{3n+1}e, \quad e \quad C_n = p_{3n+2} - q_{3n+2}e.$$

(c) Mostrar que

$$e = \lim_{n \rightarrow \infty} \frac{p_n}{q_n} = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots, 1, 1, 2n, \dots].$$

3.10. Prove que

$$\left| e - \frac{p}{q} \right| < \frac{\log \log q}{2q^2 \log q} \text{ tem infinitas soluções } \frac{p}{q} \in \mathbb{Q}, \text{ mas, para todo } \varepsilon > 0,$$

$$\left| e - \frac{p}{q} \right| < \frac{\log \log q}{(2 + \varepsilon)q^2 \log q} \text{ tem apenas um número finito de soluções } \frac{p}{q} \in \mathbb{Q}.$$

3.11. Seja $\{a_n\}_{n \in \mathbb{N}}$ a sequência definida por $a_n = n\sqrt{5} - \lfloor n\sqrt{5} \rfloor$. Determine os valores de $n \leq 2011$ tais que a_n seja respectivamente máximo e mínimo.

3.12. *Mostre que se $f: \mathbb{R} \rightarrow \mathbb{R}_+$ decrescente e*

$$k_f(\alpha) := \sup \left\{ k > 0 \mid \left| \alpha - \frac{p}{q} \right| < \frac{f(q)}{k} \text{ tem infinitas soluções racionais } \frac{p}{q} \right\}$$

então, caso tenhamos $\lim_{q \rightarrow +\infty} q^2 f(q) = 0$, a imagem de k_f é $(0, +\infty]$ (ou $[0, +\infty]$, se consideramos $\sup(\emptyset) = 0$ neste contexto) e, caso $\lim_{q \rightarrow +\infty} q^2 f(q) = +\infty$, então a imagem de k_f é $\{+\infty\}$.

3.13. *Dizemos que dois números irracionais α e β são $GL_2(\mathbb{Z})$ -equivalentes se existem inteiros a, b, c, d com $|ad - bc| = 1$ tais que $\beta = \frac{a\alpha + b}{c\alpha + d}$.*

Mostre que, se as frações contínuas de α e β são $\alpha = [a_0; a_1, a_2, \dots]$ e $\beta = [b_0; b_1, b_2, \dots]$ então α e β são $GL_2(\mathbb{Z})$ -equivalentes se, e somente se, existem $r \in \mathbb{Z}$ e $n_0 \in \mathbb{N}$ tais que $b_n = a_{n+r}, \forall n \geq n_0$.

Conclua que $k(\alpha) = k(\beta)$ sempre que α e β são $GL_2(\mathbb{Z})$ -equivalentes.

3.14. *Use o fato de que $C(4) + C(4) = [\sqrt{2} - 1, 4(\sqrt{2} - 1)]$ e a fórmula para $k(\alpha)$ para mostrar que $L \supset [6, +\infty)$.*

Capítulo 4

Equações Diofantinas

Uma *equação diofantina* é uma equação polinomial para a qual procuramos soluções inteiras ou racionais. Nos capítulos anteriores estudamos equações diofantinas de grau 1, como $ax + by = c$ (onde a , b e c são inteiros dados e queremos identificar todos os pares (x, y) que satisfazem a equação). Neste capítulo estudaremos várias outras equações diofantinas, começando com $x^2 + y^2 = z^2$ (ternas pitagóricas), passando por vários outros polinômios particulares e concluindo com a equação de Pell $x^2 - Ay^2 = 1$.

Com isso, pode-se considerar que estudamos de forma bastante completa equações diofantinas de grau 2 com duas variáveis. O leitor deve naturalmente se perguntar se não existe uma teoria mais geral. Este é essencialmente o décimo problema de Hilbert: dada uma equação diofantina com qualquer número de variáveis e com coeficientes inteiros, descrever um processo que determine, em um número finito de passos, se a equação admite solução inteira. Considera-se que este problema foi resolvido por Martin Davis, Yuri Matiyasevich, Hilary Putnam e Julia Robinson, não por eles terem descrito um tal processo mas por eles terem demonstrado que não existe um algoritmo que, dada uma equação diofantina, decida se a equação admite solução inteira. O décimo problema de Hilbert é um caso raro em que a solução de um famoso problema de matemática é acessível a um público bastante amplo: uma excelente exposição está em [49].

O leitor deve observar que existem muitos problemas famosos em equações diofantinas. O mais famoso é provavelmente aquele foi durante séculos conhecido como o último teorema de Fermat, até sua demons-

tração ser completada por Andrew Wiles e seu aluno Richard Taylor: provar que para $n \geq 3$ qualquer solução inteira de $x^n + y^n = z^n$ é trivial (no sentido de que $xyz = 0$); discutiremos abaixo alguns casos fáceis deste teorema.

4.1 Ternas Pitagóricas

As triplas de números inteiros positivos (a, b, c) que satisfazem a equação

$$a^2 + b^2 = c^2$$

são denominadas *triplas ou ternas pitagóricas*, já que correspondem aos comprimentos dos lados de um triângulo retângulo de lados inteiros pelo teorema de Pitágoras.

Vamos encontrar todas as ternas pitagóricas (a, b, c) . Podemos supor que a, b, c são primos relativos dois a dois, pois se houver um primo p tal que $p \mid \text{mdc}(a, b)$, por exemplo, então $p \mid a^2 + b^2 = c^2 \implies p \mid c$, logo $(\frac{a}{p}, \frac{b}{p}, \frac{c}{p})$ também é tripla pitagórica. Uma tripla pitagórica cujos termos são primos relativos dois a dois se denomina *tripla pitagórica primitiva*.

Daqui a e b não podem ser pares ao mesmo tempo, portanto podemos supor sem perda de generalidade que a é ímpar. Além disso, como $(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4}$ e $(2k)^2 \equiv 0 \pmod{4}$, quadrados perfeitos são congruentes ou a 0 ou a 1 módulo 4. Portanto b não pode ser ímpar pois caso contrário $c^2 \equiv a^2 + b^2 \equiv 2 \pmod{4}$, um absurdo. Resumindo, temos que b é par e c é ímpar. Por outro lado,

$$b^2 = c^2 - a^2 = (c - a)(c + a).$$

Temos $\text{mdc}(c - a, c + a) = \text{mdc}(2c, c + a) = 2$ pois $\text{mdc}(a, c) = 1 \implies \text{mdc}(c, c + a) = 1$ e $c + a$ é par. Logo $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são coprimos e seu produto é um quadrado perfeito. Pelo teorema Fundamental da Aritmética, cada um destes fatores deve ser o quadrado de um número natural. Assim,

$$\frac{c + a}{2} = m^2, \quad \frac{c - a}{2} = n^2, \quad b = 2mn,$$

com $\text{mdc}(m, n) = 1$. Escrevendo a, b, c em termos de m e n , obtemos portanto

Proposição 4.1. *As ternas pitagóricas primitivas (a, b, c) são da forma*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

com $\text{mdc}(m, n) = 1$ e $m + n$ ímpar.

A condição de $m + n$ ser ímpar garante a primitividade da tripla: como $\text{mdc}(m, n) = 1$ temos $\text{mdc}(m^2, m^2 + n^2) = 1$ e portanto $\text{mdc}(a, c) = \text{mdc}(m^2 - n^2, m^2 + n^2) = \text{mdc}(2m^2, m^2 + n^2) = \text{mdc}(2, m^2 + n^2)$, que é igual a 1 se, e só se, $m^2 + n^2$ é ímpar, isto é, se m e n têm paridades distintas. Todas as demais triplas pitagóricas podem ser obtidas a partir de uma tripla pitagórica primitiva, multiplicando seus termos por uma constante.

Como uma aplicação do resultado anterior, consideremos o seguinte

Exemplo 4.2. *Encontrar todas as triplas de inteiros positivos (a, b, c) tais que a^2 , b^2 e c^2 estão em progressão aritmética.*

SOLUÇÃO: O problema se reduz a encontrar todas as triplas (a, b, c) tais que

$$a^2 + c^2 = 2b^2$$

e, como no caso das ternas pitagóricas, basta considerar o caso em que a, b, c são dois a dois primos entre si. Temos que a e c têm igual paridade (logo são ímpares pois $\text{mdc}(a, c) = 1$ por hipótese) e portanto existem inteiros r e s tais que $c = r + s$ e $a = r - s$ (é só fazer $r = \frac{c+a}{2}$ e $s = \frac{c-a}{2}$). Substituindo temos que

$$a^2 + c^2 = (r - s)^2 + (r + s)^2 = 2(r^2 + s^2) = 2b^2.$$

Logo (r, s, b) é uma tripla pitagórica, que é primitiva pois qualquer divisor comum de r e s é um divisor comum de a e c . Portanto existem inteiros m e n tais que $r = m^2 - n^2$, $s = 2mn$ e $b = m^2 + n^2$ (ou $r = 2mn$ e $s = m^2 - n^2$, que fornecerá uma outra solução simétrica). Conclui-se que

$$a = m^2 - n^2 - 2mn, \quad b = m^2 + n^2, \quad c = m^2 - n^2 + 2mn,$$

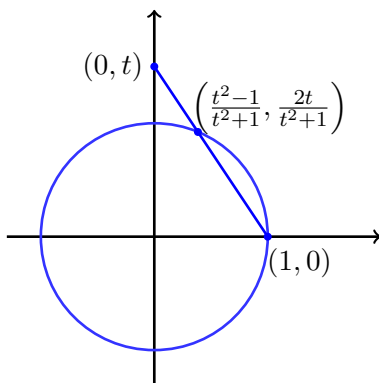
e é fácil verificar que tal tripla cumpre o pedido. □

As soluções inteiras primitivas da equação $x^2 + y^2 = z^2$ estão claramente em bijeção, via $(x, y, z) \mapsto (x/z, y/z)$, com as soluções *racionais* da equação $x^2 + y^2 = 1$. Estas, por sua vez, podem ser facilmente obtidas através do seguinte método geométrico:

Teorema 4.3. *Os pontos racionais (x, y) (isto é, com ambas as coordenadas $x, y \in \mathbb{Q}$) da circunferência de equação $x^2 + y^2 = 1$ são todos os pontos da forma*

$$(x, y) = (1, 0) \quad e \quad (x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right) \quad \text{com } t \in \mathbb{Q}.$$

DEMONSTRAÇÃO: Considere a reta passando pelos pontos $(1, 0)$ e $(0, t)$ com $t \in \mathbb{Q}$, ou seja, a reta de equação $y = -t(x - 1)$. Esta reta intercepta a circunferência em dois pontos: $(1, 0)$ e $(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$, como mostra a figura:



Agora observe que $(0, t) \mapsto (\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$ estabelece uma bijeção entre os pontos racionais do eixo y e os pontos racionais P da circunferência $x^2 + y^2 = 1$, menos o ponto $(1, 0)$. De fato, é claro que se $t \in \mathbb{Q}$ então $(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$ é um ponto racional da circunferência. Reciprocamente, dado um ponto racional $P \neq (1, 0)$ da circunferência, temos que a reta que une P a $(1, 0)$ admite uma equação com coeficientes racionais, logo intercepta o eixo y em um ponto $(0, t)$ com $t \in \mathbb{Q}$. Isto completa a demonstração. \square

Assim, substituindo $t = \frac{m}{n}$ com $m, n \in \mathbb{Z}$ e $\text{mdc}(m, n) = 1$, obtemos as soluções racionais $(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2})$, que correspondem às ternas

pitagóricas $(m^2 - n^2, 2mn, m^2 + n^2)$.

Problemas Propostos

4.1. *Encontrar todos os triângulos ABC tais que $\angle A = 2\angle B$ e seus lados a , b e c são inteiros.*

4.2. *Se no problema anterior fixamos $b = n$, quantos triângulos satisfazem as condições acima?*

4.3. *Dado um número inteiro n , de quantos triângulos retângulos com lados inteiros é n o comprimento de um cateto?*

4.4. *Dado um número inteiro n , de quantos triângulos retângulos com lados inteiros é n o comprimento da hipotenusa?*

4.5. *Demonstrar que a equação $x^2 + y^2 = 3z^2$ não tem soluções inteiras positivas.*

4.6. *Encontrar todas as soluções inteiras da equação $x^2 + y^2 = 5z^2$.*

4.7. *Encontrar infinitas triplas primitivas de números (a, b, c) tais que a^3 , b^3 e c^3 estão em progressão aritmética.*

4.8. *Encontrar infinitas triplas primitivas de números (a, b, c) tais que a^4 , b^4 e c^4 estão em progressão aritmética.*

4.9. *Demonstrar que todas as soluções inteiras de $x^2 + y^2 + z^2 = t^2$ são dadas por*

$$x = d(m^2 - n^2 - p^2 + q^2)$$

$$y = d(2mn - 2pq)$$

$$z = d(2mp + 2nq)$$

$$t = d(m^2 + n^2 + p^2 + q^2).$$

4.10 (APMO2002). *Encontrar todos os pares m, n de inteiros positivos tais que $m^2 - n$ divide $m + n^2$ e $n^2 - m$ divide $m^2 + n$.*

Dica: Mostre que $|m - n| \leq 1$.

4.11 (APMO1999). *Encontrar todos os pares m, n de inteiros tais que $m^2 + 4n$ e $n^2 + 4m$ são ambos quadrados perfeitos.*

Dica: Mostre que n e m não podem ser simultaneamente positivos.

4.12 (AusPol1994). *Encontrar todas as soluções inteiras de*

$$\frac{(a+b)(b+c)(c+a)}{2} + (a+b+c)^3 = 1 - abc.$$

4.13 (IMO1982). *Demonstre que se n é um inteiro positivo tal que a equação*

$$x^3 - 3xy^2 + y^3 = n$$

tem uma solução com x, y inteiros, então ela tem ao menos três soluções inteiras. Mostre que esta equação não possui soluções inteiras para $n = 2891$.

Dica: Considerar a equação módulo 7.

4.14 (OlbM2001). *Seja n um inteiro positivo. Demonstrar que o número de soluções inteiras (x, y) da equação*

$$x^2 - xy + y^2 = n$$

é finita múltiplo de 6.

4.2 Equações Diofantinas Quadráticas e Somas de Quadrados

Vamos provar um resultado devido a Legendre que fornece um critério para determinar quando uma equação do tipo $ax^2 + by^2 + cz^2 = 0$ tem solução não nula e que dá uma generalização natural das triplas pitagóricas.

Teorema 4.4 (Legendre). *Sejam a, b, c inteiros livres de quadrados, primos entre si, dois a dois, e não todos do mesmo sinal. A equação $ax^2 + by^2 + cz^2 = 0$ tem solução $(x, y, z) \neq (0, 0, 0)$ com x, y e z inteiros se, e somente se, $-bc$ é quadrado módulo a , $-ac$ é quadrado módulo b e $-ab$ é quadrado módulo c .*

DEMONSTRAÇÃO: Vamos primeiro mostrar a necessidade. Basta ver pela simetria da equação que $-bc$ é quadrado módulo a . De fato, podemos supor que x, y e z são primos relativos dois a dois, pois se $d \mid \text{mdc}(x, y)$ então d^2 divide cz^2 , mas c é livre de quadrados, portanto $d \mid z$. Agora como $by^2 + cz^2 \equiv 0 \pmod{a}$ segue que $b^2y^2 \equiv -bcz^2$

(mod a). Note que z deve ser primo com a , pois se p é primo tal que $p \mid a$ e $p \mid z$, teremos que $p \mid by^2$, mas $\text{mdc}(a, b) = 1$, segue que $p \mid y$ o que contradiz o fato de y e z serem primos entre si. Assim, z é invertível módulo a , e logo $(byz^{-1})^2 \equiv -bc \pmod{a}$.

Provemos agora a suficiência. Podemos supor, sem perda de generalidade, que $a < 0$, $b < 0$ e $c > 0$. Por hipótese, existe $u \in \mathbb{Z}$ tal que $u^2 \equiv -bc \pmod{a}$. Assim, módulo a , temos que

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \equiv b^{-1}((by)^2 + bcz^2) \\ &\equiv b^{-1}((by)^2 - u^2z^2) \equiv b^{-1}(by - uz)(by + uz) \\ &\equiv (y - b^{-1}uz)(by + uz) \\ &\equiv L_1(x, y, z)M_1(x, y, z) \end{aligned}$$

onde $L_1(x, y, z) = d_1x + e_1y + f_1z$, $M_1(x, y, z) = g_1x + h_1y + i_1z$, com $d_1 = g_1 = 0$, $e_1 = 1$, $f_1 = -b^{-1}u$, $h_1 = b$ e $i_1 = u$. Do mesmo modo,

$$ax^2 + by^2 + cz^2 \equiv L_2(x, y, z)M_2(x, y, z) \pmod{b}$$

e

$$ax^2 + by^2 + cz^2 \equiv L_3(x, y, z)M_3(x, y, z) \pmod{c},$$

onde $L_k(x, y, z) = d_kx + e_ky + f_kz$, $M_k(x, y, z) = g_kx + h_ky + i_kz$, $k = 2, 3$. Como a, b e c são primos entre si dois a dois, podemos pelo teorema chinês dos restos encontrar duas formas lineares $L(x, y, z) = dx + ey + fz$, $M(x, y, z) = gx + hy + iz$ tais que $L \equiv L_1 \pmod{a}$, $L \equiv L_2 \pmod{b}$ e $L \equiv L_3 \pmod{c}$, e $M \equiv M_1 \pmod{a}$, $M \equiv M_2 \pmod{b}$ e $M \equiv M_3 \pmod{c}$ (basta resolver o sistema de congruências coeficiente a coeficiente). Logo

$$ax^2 + by^2 + cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}.$$

Consideremos agora todas as triplas $(x, y, z) \in \mathbb{Z}^3$ com $0 \leq x \leq \sqrt{|bc|}$, $0 \leq y \leq \sqrt{|ac|}$ e $0 \leq z \leq \sqrt{|ab|}$. Temos $(\lfloor \sqrt{|bc|} \rfloor + 1)(\lfloor \sqrt{|ac|} \rfloor + 1)(\lfloor \sqrt{|ab|} \rfloor + 1) > abc$ de tais triplas, donde pelo Princípio da Casa dos Pombos existem duas triplas distintas dentre elas, (x_1, y_1, z_1) e (x_2, y_2, z_2) , com $L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc} \iff L(x_1 - x_2, y_1 - y_2, z_1 - z_2) \equiv 0 \pmod{abc}$, donde, fazendo $\tilde{x} = x_1 - x_2$, $\tilde{y} = y_1 - y_2$ e $\tilde{z} = z_1 - z_2$, temos

$$a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \equiv L(\tilde{x}, \tilde{y}, \tilde{z})M(\tilde{x}, \tilde{y}, \tilde{z}) \equiv 0 \pmod{abc}.$$

Note que $(\tilde{x}, \tilde{y}, \tilde{z}) \neq (0, 0, 0)$, $|\tilde{x}| < \sqrt{|bc|}$, $|\tilde{y}| < \sqrt{|ac|}$ e $|\tilde{z}| < \sqrt{|ab|}$ (de fato, como a, b, c são dois a dois coprimos e livre de quadrados, não pode ocorrer a igualdade). Como $a, b < 0$ e $c > 0$ temos que

$$-2abc = a|bc| + b|ac| < a\tilde{x}^2 + b\tilde{y}^2 \leq a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \leq c\tilde{z}^2 < |ab|c = abc.$$

Como $abc \mid a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2$, devemos então ter $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = 0$, o que resolve o problema, ou $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = -abc$, mas, nesse caso, temos

$$\begin{aligned} 0 &= (a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 + abc)(\tilde{z}^2 + ab) \\ &= a(\tilde{x}\tilde{z} + b\tilde{y})^2 + b(\tilde{y}\tilde{z} - a\tilde{x})^2 + c(\tilde{z}^2 + ab)^2, \end{aligned}$$

o que nos dá a solução $(\tilde{x}\tilde{z} + b\tilde{y}, \tilde{y}\tilde{z} - a\tilde{x}, \tilde{z}^2 + ab)$ com $\tilde{z}^2 + ab \neq 0$. \square

O teorema de Legendre permite determinar quando uma curva algébrica plana de grau 2, $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ com $A, B, C, D, E \in \mathbb{Q}$, possui algum *ponto racional* $(x, y) \in \mathbb{Q}^2$. De fato, fazendo $\tilde{x} = x + \frac{B}{2A}y$ (podemos supor que $A \neq 0$, se não fazemos uma mudança de coordenadas como $y = \tilde{y} + x$), a curva fica da forma $\tilde{A}\tilde{x}^2 + \tilde{C}\tilde{y}^2 + \tilde{D}\tilde{x} + \tilde{E}\tilde{y} + \tilde{F} = 0$, e, fazendo $\bar{x} = \tilde{x} + \frac{\tilde{D}}{2\tilde{A}}$ e $\bar{y} = \tilde{y} + \frac{\tilde{E}}{2\tilde{C}}$, a curva fica da forma $\bar{A}\bar{x}^2 + \bar{C}\bar{y}^2 + \bar{F} = 0$. Multiplicando pelo mmc dos denominadores dos coeficientes, podemos supor que \bar{A}, \bar{C} e \bar{F} são inteiros, e, escrevendo $\bar{A} = k^2\hat{A}$, $\bar{C} = l^2\hat{C}$ e $\bar{F} = m^2\hat{F}$, com \hat{A}, \hat{C} e \hat{F} livre de quadrados, obtemos fazendo $\hat{x} = \frac{k}{m}\bar{x}$ e $\hat{y} = \frac{l}{m}\bar{y}$ a expressão $\hat{A}\hat{x}^2 + \hat{C}\hat{y}^2 + \hat{F} = 0$. Assim fazendo $\hat{x} = \frac{p}{q}$ e $\hat{y} = \frac{r}{q}$, obtemos a equação

$$\hat{A}p^2 + \hat{C}r^2 + \hat{F}q^2 = 0.$$

Podemos supor $\text{mdc}(\hat{A}, \hat{C}, \hat{F}) = 1$ (se não dividimos por $\text{mdc}(\hat{A}, \hat{C}, \hat{F})$) e que $\text{mdc}(p, r, q) = 1$. Além disso, se $\text{mdc}(\hat{A}, \hat{C}) = d$ devemos ter $d \mid \hat{F}q^2$, e logo $d \mid q$ (pois d é livre de quadrados), donde $q = dq'$, e obtemos a equação

$$\frac{\hat{A}}{d}p^2 + \frac{\hat{C}}{d}r^2 + (\hat{F}d)q'^2 = 0$$

com $\frac{\hat{A}}{d}, \frac{\hat{C}}{d}, \hat{F}d$ livres de quadrados e

$$\left| \frac{\hat{A}\hat{C}}{d}\hat{F}d \right| = \left| \frac{\hat{A}\hat{C}\hat{F}}{d} \right| < |\hat{A}\hat{C}\hat{F}| \quad \text{se } d > 1.$$

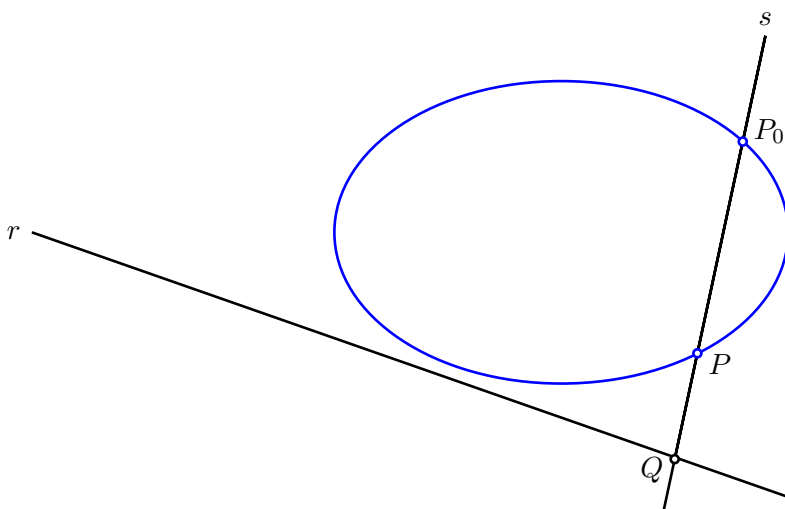
Após algumas reduções deste tipo, obtemos uma equação equivalente como nas hipóteses do teorema de Legendre, que pode então ser usado para decidir a existência de um ponto racional na curva. Note que a hipótese sobre a, b, c não terem o mesmo sinal no teorema de Legendre equivale à existência de pontos reais não triviais na curva.

Se há algum ponto racional (x_0, y_0) numa tal curva, então há infinitos. Isto pode ser visto a partir do exemplo a seguir, que ilustra o método geométrico que permite encontrar todos os pontos racionais explicitamente.

Exemplo 4.5. *Encontre todos os pontos racionais da elipse*

$$\frac{x^2}{5/2} + \frac{y^2}{5/3} = 1.$$

SOLUÇÃO: É fácil encontrar um destes pontos racionais, digamos $(x, y) = (1, 1)$. Para encontrar os demais, começamos traçando uma reta r de coeficientes racionais paralela à reta tangente à elipse no ponto $P_0 = (1, 1)$. Derivando a equação da elipse em relação à x , obtemos $\frac{2x}{5/2} + \frac{2yy'}{5/3} = 0$ e assim $y' = -2/3$ para $(x, y) = (1, 1)$. Portanto podemos tomar (por exemplo) a reta r de equação $y = -\frac{2}{3}x - 2$. Agora, para um ponto $P \neq P_0$ da elipse, seja s a reta que liga P a $P_0 = (1, 1)$; como esta reta não é paralela a r , temos que r e s determinam um ponto Q , como na figura a seguir.



Vamos mostrar que a associação $P \mapsto Q$ define uma bijeção entre os pontos racionais da elipse, excetuando o ponto P_0 , e os pontos racionais da reta r .

Em primeiro lugar, se P é um ponto racional da elipse então a equação da reta s , que liga dois pontos racionais P e P_0 , possui coeficientes racionais. Logo Q será um ponto racional, sendo a intersecção de duas retas r e s cujas equações têm coeficientes racionais.

Reciprocamente, suponha que $Q = (a, b)$ é um ponto racional de r . Então a equação da reta s , determinada pelos pontos racionais P_0 e Q , terá coeficientes racionais: $y - 1 = \frac{b-1}{a-1} \cdot (x - 1)$. Como a equação da elipse também tem coeficientes racionais, a intersecção $P \neq P_0$ de s com a elipse será um ponto racional, já que isolando y na equação de s e substituindo na equação da elipse obtemos uma equação quadrática com coeficientes racionais

$$\frac{2}{5}x^2 + \frac{3}{5}\left(1 + \frac{b-1}{a-1} \cdot (x-1)\right)^2 - 1 = 0.$$

Sabemos que a abscissa $x = 1$ de P_0 é uma das raízes, logo a outra raiz (que é a abscissa de P) é racional também pelas relações de Girard. Como P pertence à reta s cuja equação tem coeficientes racionais, a ordenada de P também será racional, ou seja, P será um ponto racional.

Após algumas contas, obtemos a seguinte fórmula para P em função de $Q = (a, b)$:

$$P = \left(\frac{10a^2 + 90a + 21}{10a^2 + 24a + 87}, \frac{10a^2 - 20a - 111}{10a^2 + 24a + 87} \right).$$

Assim, os pontos racionais P da elipse são obtidos fazendo a percorrer todos os racionais $a \in \mathbb{Q}$ juntamente com $a = \infty$, i.e., o limite para $a \rightarrow \infty$ na expressão acima, que fornece o ponto inicial $P_0 = (1, 1)$, que corresponde ao “ponto no infinito” de r , intersecção de r com a reta s tangente à elipse no ponto P_0 (no plano projetivo, é claro!). Veja mais detalhes na seção 9.1. \square

4.2.1 Somas de Dois Quadrados

Nesta seção, caracterizamos os números que são somas de dois quadrados.

Teorema 4.6. *Os únicos números que podem se expressar como soma de dois quadrados são os da forma $n = 2^s d^2 l$ onde s é um natural e l é um número livre de quadrados tais que seus fatores primos são da forma $4k + 1$.*

Começamos observando que se p é um primo da forma $4k + 3$ que divide $n = a^2 + b^2$, então $p \mid a$ e $p \mid b$. De fato, se isto não ocorresse, b seria invertível módulo p , logo de $a^2 \equiv -b^2 \pmod{p}$ teríamos que -1 é resíduo quadrático módulo p , o que é absurdo pois $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$ já que $p \equiv 3 \pmod{4}$. Logo $p^2 \mid n$ e repetindo o processo com $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$ no lugar de n , concluímos que todo primo da forma $4k + 3$ aparece com expoente par na fatoração canônica de n . Assim, apenas os números da forma descrita no teorema podem ser soma de dois quadrados.

Agora todo natural n pode se expressar como $n = k^2 m$ onde k e m são inteiros positivos e m é livre de quadrados, donde se m pode se escrever como soma de dois quadrados $m = a^2 + b^2$ então o mesmo ocorre para $n = (ak)^2 + (bk)^2$. Além disso, se temos dois números que são soma de dois quadrados, digamos $m = a^2 + b^2$ e $n = c^2 + d^2$, então a seguinte identidade de números complexos

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) = |a + bi|^2 \cdot |c + di|^2 \\ &= |(a + bi)(c + di)|^2 = |(ac - bd) + (ad + bc)i|^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

mostra que seu produto também será soma de dois quadrados. Assim, para mostrar que todo n da forma descrita no teorema é soma de dois quadrados, basta mostrar que 2 e todo primo da forma $4k + 1$ são somas de dois quadrados. Se $p = 2$ temos que $2 = 1^2 + 1^2$ é soma de dois quadrados. Para o outro caso, precisamos do seguinte

Lema 4.7 (Lema de Thue). *Se $m > 1$ é um número natural e a é um inteiro primo relativo com m então existem números naturais x e y não nulos menores do que ou iguais a \sqrt{m} e tais que algum dos números $ax \pm y$ é divisível por m .*

DEMONSTRAÇÃO: Seja $q = \lfloor \sqrt{m} \rfloor$, então $q + 1 > \sqrt{m}$ e portanto $(q + 1)^2 > m$. Consideremos todos os $(q + 1)^2$ números da forma $ax - y$

onde x e y tomam os valores $0, 1, \dots, q$. Como só existem m restos ao se dividir um número por m , pelo Princípio da Casa dos Pombos dois dos números anteriores, digamos $ax_1 - y_1$ e $ax_2 - y_2$, são congruentes módulo m . Portanto a diferença $a(x_1 - x_2) - (y_1 - y_2)$ é divisível por m . Temos

$$0 \leq x_i, y_i \leq \sqrt{m} \implies |x_1 - x_2|, |y_1 - y_2| \leq \sqrt{m}.$$

Se $x_1 - x_2 = 0$ então $y_1 - y_2$ será divisível por m , o que implica $y_1 = y_2$, mas os pares (x_1, y_1) e (x_2, y_2) são diferentes, uma contradição. De igual forma, se $y_1 - y_2 = 0$ então $a(x_1 - x_2)$ será divisível por m , mas a e m são primos relativos, logo $m \mid x_1 - x_2$ e assim $x_1 = x_2$, outra contradição. Logo $x = |x_1 - x_2|$ e $y = |y_1 - y_2|$ satisfazem as condições do enunciado. \square

Retomando o nosso problema inicial, se p é um número primo da forma $4k + 1$, então $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$, logo existe a tal que $p \mid a^2 + 1$. Aplicando o lema anterior, existem inteiros $0 < x, y < \sqrt{p}$ tais que algum dos números $ax \pm y$ é divisível por p , portanto o número $(ax + y)(ax - y) = a^2x^2 - y^2$ é divisível por p . Daqui

$$x^2 + y^2 = x^2 + a^2x^2 - a^2x^2 + y^2 = x^2(a^2 + 1) - (a^2x^2 - y^2)$$

é divisível por p , mas como $0 < x, y < \sqrt{p}$ então $0 < x^2 + y^2 < 2p$, portanto $p = x^2 + y^2$. Isto encerra a prova do teorema. Para outras demonstrações, veja os teoremas 4.19 e 6.12.

O método anterior pode ser aplicado para obter outras representações de números primos.

Exemplo 4.8. *Sejam $d \in \{1, 2, 3, 7\}$ e p é primo ímpar tal que $\left(\frac{-d}{p}\right) = 1$, então existem $e, f \in \mathbb{N}$ tais que $p = e^2 + df^2$.*

SOLUÇÃO: Seja $a \in \mathbb{N}$ tal que $a^2 \equiv -d \pmod{p}$. Pelo lema de Thue, existem inteiros x, y tais que $(x + ay)(x - ay) \equiv 0 \pmod{p} \iff p \mid x^2 + dy^2$ e $0 < x^2 + dy^2 < (d + 1)p$. Assim, temos

$$x^2 + dy^2 = kp \quad \text{com } k \in \{1, 2, \dots, d\}.$$

Observemos que se $k = d$, x é múltiplo de d e fazendo $x = dz$ temos que $dz^2 + y^2 = p$. Assim podemos desconsiderar este caso e se $d = 1$ ou $d = 2$ o problema está resolvido. Consideremos agora os outros valores de d :

1. Se $d = 3$ então $x^2 + 3y^2 = p$ ou $2p$. No caso $x^2 + 3y^2 = 2p$ temos que x e y têm a mesma paridade, assim se x, y são pares temos que $4 \mid x^2 + 3y^2 = 2p$, que é contraditório, e no caso em que x, y ímpares temos que $x^2 \equiv y^2 \equiv 1 \pmod{8}$, portanto $2p = x^2 + 3y^2 \equiv 4 \pmod{8}$, que também é contraditório. Assim concluímos que $x^2 + 3y^2 = p$.
2. Se $d = 7$ então $x^2 + 7y^2 = ip$ com $i \in \{1, 2, 3, 4, 5, 6\}$. No caso que x, y são ímpares, como $x^2 \equiv y^2 \equiv 1 \pmod{8}$, temos que $x^2 + 7y^2 \equiv 0 \pmod{8}$, o que é contraditório, e no caso em que x, y são pares, dividimos toda a expressão por 4, logo podemos supor que i é ímpar. Assim resta considerar os casos em que $i = 3$ ou 5. Mas -7 não é resto quadrático módulo 3 nem 5, portanto $x^2 + 7y^2 = p$. □

4.2.2 Somas de Quatro Quadrados e o Problema de Waring

Uma pergunta natural é: quantos quadrados precisamos somar para se obter qualquer inteiro positivo? Foi conjecturado por Bachet que todo número natural pode ser escrito como soma de 4 quadrados. Esta conjectura foi primeiramente provada por Fermat usando a técnica de descenso infinito, mas a primeira prova publicada é devida a Lagrange (1770) e usa a identidade dos quatro quadrados de Euler. Para a prova vamos precisar dos seguintes lemas.

Lema 4.9 (Identidade de Euler). *Para todo a, b, c, d, w, x, y, z temos que*

$$\begin{aligned} (a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = & (aw + bx + cy + dz)^2 \\ & + (ax - bw - cz + dy)^2 \\ & + (ay + bz - cw - dx)^2 \\ & + (az - by + cx - dw)^2. \end{aligned}$$

DEMONSTRAÇÃO: Por comprovação direta. Uma outra maneira é utilizar a seguinte identidade de matrizes complexas (a barra denota conjugado):

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -(\alpha\delta + \beta\bar{\gamma}) & \alpha\gamma - \beta\bar{\delta} \end{pmatrix}.$$

Calculando determinantes, obtemos

$$(|\alpha|^2 + |\beta|^2)(|\gamma|^2 + |\delta|^2) = |\alpha\gamma - \beta\bar{\delta}|^2 + |\alpha\delta + \beta\bar{\gamma}|^2.$$

Substituindo $\alpha = a - bi$, $\beta = -c - di$, $\gamma = w + xi$ e $\delta = y + zi$, obtemos a identidade acima. \square

Esta identidade fica mais natural (e pode ser demonstrada) usando *quatérnios*: ela se traduz em dizer que $|zw| = |z||w|$ se z e w são quatérnios. O conjunto dos quatérnios é \mathbb{R}^4 (com a soma e a norma euclidiana) onde escrevemos $(a, b, c, d) = a + bi + cj + dk$ e definimos a multiplicação por

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Se identificarmos $a + bi + cj + dk$ com a matriz

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

obtemos uma identificação entre quatérnios e as matrizes da demonstração acima.

Lema 4.10. *Se $2m$ é soma de dois quadrados, então m também é soma de dois quadrados.*

DEMONSTRAÇÃO: Como $2m = x^2 + y^2$ então x e y têm a mesma paridade. Portanto $m = (\frac{x+y}{2})^2 + (\frac{x-y}{2})^2$. \square

Lema 4.11. *Se p é primo ímpar, então existem inteiros a, b, k tais que $a^2 + b^2 + 1 = kp$.*

DEMONSTRAÇÃO: Considere os conjuntos

$$A = \left\{ a^2 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \leq a \leq \frac{p-1}{2} \right\} \quad \text{e}$$

$$B = \left\{ -b^2 - 1 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \leq b \leq \frac{p-1}{2} \right\}$$

Como cada conjunto possui $\frac{p+1}{2}$ elementos de $\mathbb{Z}/(p)$ então $A \cap B \neq \emptyset$, isto é, existem a e b tais que $a^2 \equiv -b^2 - 1 \pmod{p}$. \square

Teorema 4.12. *Todo inteiro positivo n pode se escrever como soma de 4 quadrados.*

DEMONSTRAÇÃO: Pelo lema 4.9, basta provar o resultado para os números primos. Como $2 = 1^2 + 1^2$ podemos supor p primo ímpar. Pelo lema 4.11 sabemos que existem a, b, c, d e m inteiros com $m > 0$ tais que $mp = a^2 + b^2 + c^2 + d^2$. Assim, para terminar a demonstração, basta provar que se $m > 1$ então existe um $0 < n < m$ tal que np pode se escrever como soma de 4 quadrados. De fato se m é par, então nenhum, dois ou quatro dos números a, b, c, d são pares, assim aplicando apropriadamente o lema 4.10 basta tomar $n = \frac{m}{2}$. Portanto podemos supor que m é ímpar maior que 1. Sejam w, x, y, z inteiros tais que

$$\begin{aligned} w &\equiv a \pmod{m} \\ x &\equiv b \pmod{m} \\ y &\equiv c \pmod{m} \\ z &\equiv d \pmod{m} \end{aligned}$$

onde $w, x, y, z \in (-\frac{m}{2}, \frac{m}{2})$, logo

$$w^2 + x^2 + y^2 + z^2 < 4 \cdot \frac{m^2}{4} = m^2 \quad \text{e} \quad w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}.$$

Portanto $w^2 + x^2 + y^2 + z^2 = nm$ com $0 < n < m$. Pela escolha de w, x, y, z temos que os números $ax - bw - cz + dy$, $ay + bz - cw - dx$ e $az - by + cx - dw$ são divisíveis por m e $aw + bx + cy + dz \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$, portanto pelo lema 4.9 temos que

$$\begin{aligned} np &= \frac{1}{m^2}(mp)(nm) = \frac{1}{m^2}(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) \\ &= \left(\frac{aw + bx + cy + dz}{m}\right)^2 + \left(\frac{ax - bw - cz + dy}{m}\right)^2 \\ &\quad + \left(\frac{ay + bz - cw - dx}{m}\right)^2 + \left(\frac{az - by + cx - dw}{m}\right)^2 \end{aligned}$$

é soma de 4 quadrados, como desejado. \square

Em geral, para $n \in \mathbb{N}$ podemos nos perguntar se existe um inteiro positivo s (dependendo de n) tal que qualquer número natural se escreve como soma de s n -ésimas potências. Este problema é conhecido como *problema de Waring* e foi respondido afirmativamente por Hilbert em

1909. Denote por $g(n)$ o menor destes números s . O teorema anterior prova que $g(2) \leq 4$ e de fato $g(2) = 4$ já que mostraremos na próxima seção que nenhum número da forma $4^k(8s + 7)$ pode se escrever como soma de três quadrados. Sabe-se que $g(3) = 9$ (Wieferich e Kempner), $g(4) = 19$ (Balasubramanian, Dress e Deshouillers), $g(5) = 37$ (Jingrun) e $g(6) = 73$ (Pillai). Em geral, temos a seguinte

Conjetura 4.13 (Euler). *Para todo $n \geq 2$ temos que*

$$g(n) = 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 2.$$

De fato podemos provar que

Teorema 4.14 (Euler).

$$g(n) \geq 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 2.$$

DEMONSTRAÇÃO: Consideremos o número $m = 2^n \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 1$ e escrevamo-lo como soma de n -ésimas potências. Como $m < 3^n$, então nesta soma só podem aparecer potências de 1 e 2. Se k é o número de potências de 2 nesta soma, temos que $m - 2^n k$ termos são iguais a 1, assim há $(m - 2^n k) + k = m - (2^n - 1)k$ termos nesta soma. Por outra parte, $k \leq \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 1$, logo

$$\begin{aligned} m - (2^n - 1)k &\geq 2^n \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 1 - (2^n - 1) \left(\left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 1 \right) \\ &= 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 2. \end{aligned}$$

□

4.2.3 Somas de Três Quadrados

O seguinte teorema, provado por Gauß, mostra quando um número é soma de três quadrados.

Teorema 4.15 (Teorema dos Três Quadrados de Gauß). *Um inteiro $n \geq 0$ é soma de três quadrados se, e somente se, n não é da forma $4^a(8b+7)$, com $a, b \in \mathbb{N}$.*

DEMONSTRAÇÃO: Notemos inicialmente que, como $k^2 \bmod 8 \in \{\bar{0}, \bar{1}, \bar{4}\}$ para todo $k \in \mathbb{N}$, uma soma de três quadrados não pode ser congruente a $7 \bmod 8$. Além disso, se $x, y, z \in \mathbb{Z}$ e $x^2 + y^2 + z^2 \equiv 0 \pmod{4}$ então x, y, z devem ser pares o que, usado repetidamente, mostra que se $x^2 + y^2 + z^2 = 4^a(8b+7)$ então $2^a \mid \text{mdc}(x, y, z)$ e logo $(\frac{x}{2^a})^2 + (\frac{y}{2^a})^2 + (\frac{z}{2^a})^2 = 8b+7$, o que é um absurdo pelo já provado, mostrando a necessidade da condição.

Para provar a suficiência vamos primeiro mostrar o seguinte

Lema 4.16. *Se $n \in \mathbb{N}$ é soma de 3 quadrados de números racionais, então n é soma de três quadrados de inteiros.*

DEMONSTRAÇÃO: Se $n = x_1^2 + x_2^2 + x_3^2$ com $x_1, x_2, x_3 \in \mathbb{Q}$ e sendo $q \in \mathbb{N}$ um denominador comum para x_1, x_2, x_3 temos que $q^2 n = p_1^2 + p_2^2 + p_3^2$, onde $p_1 = qx_1$, $p_2 = qx_2$ e $p_3 = qx_3$ são inteiros. Seja $d > 0$ o menor inteiro positivo para o qual existem $y_1, y_2, y_3 \in \mathbb{N}$ com

$$y_1^2 + y_2^2 + y_3^2 = d^2 n.$$

Queremos mostrar que $d = 1$. Suponhamos por absurdo que $d > 1$. Escrevemos $y_1 = dy'_1 + z_1$, $y_2 = dy'_2 + z_2$ e $y_3 = dy'_3 + z_3$, com $y'_i, z_i \in \mathbb{Z}$, $|z_i| \leq d/2$, $i = 1, 2, 3$. Definimos

$$\begin{aligned} a &= y_1'^2 + y_2'^2 + y_3'^2 - n, & b &= 2(nd - y_1 y'_1 - y_2 y'_2 - y_3 y'_3) \\ d' &= ad + b & y''_i &= ay_i + by'_i \quad i = 1, 2, 3 \end{aligned}$$

Temos então

$$\begin{aligned} \sum_{1 \leq i \leq 3} y''_i{}^2 &= a^2 \sum_{1 \leq i \leq 3} y_i^2 + 2ab \sum_{1 \leq i \leq 3} y_i y'_i + b^2 \sum_{1 \leq i \leq 3} y_i'^2 \\ &= a^2 d^2 n + ab(2nd - b) + b^2(a + n) \\ &= (ad + b)^2 n = d'^2 n \end{aligned}$$

e

$$\begin{aligned}
dd' &= ad^2 + bd = d^2 \left(\sum_{1 \leq i \leq 3} y_i'^2 - n \right) + 2d \left(nd - \sum_{1 \leq i \leq 3} y_i y_i' \right) \\
&= \sum_{1 \leq i \leq 3} y_i^2 - 2d \sum_{1 \leq i \leq 3} y_i y_i' + d^2 \sum_{1 \leq i \leq 3} y_i'^2 = \sum_{1 \leq i \leq 3} (y_i - dy_i')^2 \\
&= \sum_{1 \leq i \leq 3} z_i^2 \leq \frac{3}{4} d^2,
\end{aligned}$$

donde $0 \leq d' \leq \frac{3}{4}d < d$, o que contradiz a minimalidade de d . Note que se $d' = 0$, então $\sum_{1 \leq i \leq 3} z_i^2 = dd' = 0$, donde $z_1 = z_2 = z_3 = 0$ e logo $y_1'^2 + y_2'^2 + y_3'^2 = n$, absurdo. \square

Para concluir a prova do teorema dos 3 quadrados, dado $n \in \mathbb{N}$ que não seja da forma $4^a(8b + 7)$, dividindo-o por uma potência de 4 conveniente podemos supor $n \bmod 8 \in \{\bar{1}, \bar{2}, \bar{3}, \bar{5}, \bar{6}\}$. Basta provar então que existem um inteiro $m > 0$ e racionais x, y, z, t com $t \neq 0$ tais que $x^2 + y^2 = m$ e $nt^2 - z^2 = m$, pois $n = (\frac{x}{t})^2 + (\frac{y}{t})^2 + (\frac{z}{t})^2$ será soma de 3 quadrados de racionais e, pelo lema, soma de 3 quadrados de inteiros.

Podemos supor que n é livre de quadrados: sempre podemos escrever $n = a^2 \cdot \tilde{n}$, onde \tilde{n} é livre de quadrados, e se $\tilde{n} = x^2 + y^2 + z^2$ então $n = (ax)^2 + (ay)^2 + (az)^2$. Além disso, como n não é múltiplo de 4, a é ímpar, e logo $a^2 \equiv 1 \pmod{8}$, donde $n = a^2 \tilde{n} \equiv \tilde{n} \pmod{8}$.

Temos agora alguns casos:

1. Se $n \equiv 1 \pmod{4}$ ou seja $n \bmod 8 \in \{\bar{1}, \bar{5}\}$, tomamos m primo $m \equiv 1 \pmod{4}$ e $m \equiv -1 \pmod{n}$. Tal primo existe pois, pelo teorema chinês dos restos, existe um a com $a \equiv 1 \pmod{4}$ e $a \equiv -1 \pmod{n}$ e pelo teorema de Dirichlet (ver apêndice A) existem infinitos primos congruentes com $a \bmod 4n$. Como $m \equiv 1 \pmod{4}$ e m é primo, existem x, y tais que $x^2 + y^2 = m$.

Por outro lado, existem t e z racionais com $nt^2 - z^2 = m$ se, e somente se, existem u, v e w inteiros não nulos tais que $nu^2 - v^2 - mw^2 = 0$. Pelo teorema de Legendre, isso equivale a n ser quadrado módulo m e $-m$ ser quadrado módulo n , mas $-m \equiv 1 = 1^2 \pmod{n}$. Além disso, se $n = p_1 p_2 \cdots p_k$ com os p_i primos, usando o fato que $m \equiv 1 \pmod{4}$ e pela lei de reciprocidade quadrática

obtemos

$$\left(\frac{n}{m}\right) = \prod_{1 \leq i \leq k} \left(\frac{p_i}{m}\right) = \prod_{1 \leq i \leq k} \left(\frac{m}{p_i}\right).$$

Mas $m \equiv -1 \pmod{n}$, em particular $m \equiv -1 \pmod{p_i}$, assim $\left(\frac{m}{p_i}\right) = \left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i-1}{2}}$. Mas o número de fatores p_i de n congruentes com $3 \pmod{4}$ é par pois $n \equiv 1 \pmod{4}$, portanto $\left(\frac{n}{m}\right) = 1$.

2. Se n é par, ou seja $n \bmod 8 \in \{\bar{2}, \bar{6}\}$, temos que $n = 2p_1 \cdots p_k$, onde os p_i são primos ímpares distintos. Tomemos como antes m primo, $m \equiv 1 \pmod{4}$ e $m \equiv -1 \pmod{n/2}$; ainda temos o direito de escolher a classe de congruência de m módulo 8, que pode ser 1 ou 5. Lembramos que se $m \equiv 1 \pmod{8}$ então $\left(\frac{2}{m}\right) = 1$ e se $m \equiv 5 \pmod{8}$ então $\left(\frac{2}{m}\right) = -1$. Temos como antes $-m \equiv 1 \pmod{n}$, donde $-m$ é um quadrado módulo n . Basta mostrar que m pode ser escolhido de modo que n seja quadrado módulo m . Temos

$$\begin{aligned} \left(\frac{n}{m}\right) &= \left(\frac{2}{m}\right) \prod_{1 \leq i \leq k} \left(\frac{p_i}{m}\right) = \left(\frac{2}{m}\right) \prod_{1 \leq i \leq k} \left(\frac{m}{p_i}\right) \\ &= \left(\frac{2}{m}\right) \prod_{1 \leq i \leq k} \left(\frac{-1}{p_i}\right). \end{aligned}$$

Basta então escolher a classe de congruência de m módulo 8 de modo que $\left(\frac{2}{m}\right) = \prod_{1 \leq i \leq k} \left(\frac{-1}{p_i}\right)$ para que tenhamos $\left(\frac{n}{m}\right) = 1$, como queríamos.

3. Se $n \equiv 3 \pmod{8}$, tomamos $m = 2q$ com q primo, $q \equiv 1 \pmod{4}$ e $2q \equiv -1 \pmod{n}$. Temos como antes $-m \equiv 1 \pmod{n}$, donde $-m$ é um quadrado módulo n . Vamos mostrar que n é quadrado módulo m , como n é quadrado módulo 2, basta mostrar que é quadrado módulo q . Sendo $n = p_1 \cdots p_k$, com p_i primos, temos

$$\begin{aligned} \left(\frac{n}{q}\right) &= \prod_{1 \leq i \leq k} \left(\frac{p_i}{q}\right) = \prod_{1 \leq i \leq k} \left(\frac{q}{p_i}\right) \\ &= \prod_{1 \leq i \leq k} \left(\frac{2}{p_i}\right) \left(\frac{2q}{p_i}\right) = \prod_{1 \leq i \leq k} \left(\frac{2}{p_i}\right) \left(\frac{-1}{p_i}\right) \end{aligned}$$

e

$$\left(\frac{2}{p_i}\right) \left(\frac{-1}{p_i}\right) = \begin{cases} 1 & \text{se } p_i \bmod 8 \in \{\bar{1}, \bar{3}\} \\ -1 & \text{se } p_i \bmod 8 \in \{\bar{5}, \bar{7}\} \end{cases}$$

Como $1 \cdot 1 \equiv 3 \cdot 3 \equiv 5 \cdot 5 \equiv 7 \cdot 7 \equiv 1 \pmod{8}$, $1 \cdot 3 \equiv 5 \cdot 7 \equiv 3 \pmod{8}$, $1 \cdot 5 \equiv 3 \cdot 7 \equiv 5 \pmod{8}$ e $1 \cdot 7 \equiv 3 \cdot 5 \equiv 7 \pmod{8}$, n deve ter uma quantidade par de fatores pertencentes a $\{\bar{5}, \bar{7}\} \pmod{8}$, pois caso contrário $n \pmod{8} \in \{\bar{5}, \bar{7}\}$. Assim temos $\left(\frac{n}{q}\right) = 1$.

Com isto, encerramos a prova do teorema dos três quadrados. \square

4.2.4 Teorema de Minkowski

Nesta seção veremos como algumas técnicas geométricas podem ser utilizadas no estudo de somas de quadrados. Começamos com uma

Definição 4.17. Um reticulado Λ em \mathbb{R}^n é um conjunto da forma

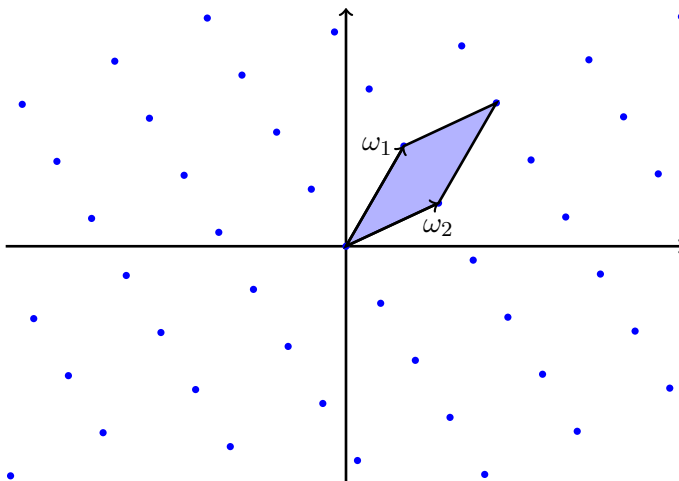
$$\Lambda = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n = \{a_1\omega_1 + \cdots + a_n\omega_n \mid a_i \in \mathbb{Z}\}$$

para alguma base $\omega_1, \dots, \omega_n$ de \mathbb{R}^n . Definimos o volume deste reticulado como $\text{vol}(\Lambda) = |\det(\omega_1, \dots, \omega_n)|$, ou seja, como o volume do conjunto

$$P = \{r_1\omega_1 + \cdots + r_n\omega_n \mid r_i \in \mathbb{R}, 0 \leq r_i < 1\}$$

chamado de paralelogramo fundamental associado à base $\omega_1, \dots, \omega_n$.

Por exemplo, a figura a seguir mostra um reticulado em \mathbb{R}^2 . Note que $\text{vol}(\Lambda)$ independe da escolha da base que gera Λ , pois quaisquer duas destas bases estão relacionadas por uma matriz de mudança de base de determinante ± 1 .



Dado um reticulado $\Lambda \subset \mathbb{R}^n$, escrevemos

$$a \equiv b \pmod{\Lambda} \iff a - b \in \Lambda \quad (a, b \in \mathbb{R}^n)$$

Esta relação define uma relação de equivalência em \mathbb{R}^n e um conjunto de representantes do quociente \mathbb{R}^n/Λ é dado justamente pelo paralelogramo fundamental.

O principal resultado desta seção é o seguinte

Teorema 4.18 (Minkowski). *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado e $V \subset \mathbb{R}^n$ é um subconjunto mensurável tal que*

1. *V é simétrico com relação à origem (i.e. $v \in V \implies -v \in V$);*
2. *V é convexo;*
3. *$\text{vol}(V) > 2^n \text{vol}(\Lambda)$.*

Então existe um ponto em $V \cap \Lambda$ diferente da origem.

DEMONSTRAÇÃO: Seja P o paralelogramo fundamental determinado por uma base $\omega_1, \dots, \omega_n$ de Λ e seja $\frac{1}{2}V = \{\frac{v}{2} \mid v \in V\}$. Considerando o quociente $\frac{1}{2}V/\Lambda$, podemos particionar $\frac{1}{2}V$ em uma quantidade enumerável de subconjuntos mensuráveis U_i tais que existam $\tau_i \in \Lambda$ com $\tau_i + U_i \subset P$. Como $\text{vol}(\frac{1}{2}V) = \frac{1}{2^n} \text{vol}(V) > \text{vol}(\Lambda) = \text{vol}(P)$, pelo princípio da casa dos pombos contínuo existem $i \neq j$ tais que $(\tau_i + \frac{1}{2}U_i) \cap (\tau_j + \frac{1}{2}U_j) \neq \emptyset$, isto é, existem dois pontos *distintos* $v, w \in V$ tais que $\frac{v}{2} \equiv \frac{w}{2} \pmod{\Lambda} \iff \frac{v-w}{2} \in \Lambda$ com $\frac{v-w}{2} \neq 0$. Mas $\frac{v-w}{2} \in V$ também, pois $w \in V \implies -w \in V$ e $v, -w \in V \implies \frac{v-w}{2} \in V$ pelas hipóteses 1 e 2, respectivamente. Assim, $0 \neq \frac{v-w}{2} \in \Lambda \cap V$. \square

Agora podemos apresentar duas novas provas curtas dos teoremas que caracterizam primos que são soma de dois e quatro quadrados.

Teorema 4.19. *Todo primo p da forma $4k+1$ é soma de dois quadrados.*

DEMONSTRAÇÃO: Como antes, temos que existe um inteiro x tal que $x^2 \equiv -1 \pmod{p}$ pois $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$. Considere o reticulado em \mathbb{R}^2

$$\Lambda \stackrel{\text{def}}{=} \{(a, b) \in \mathbb{Z}^2 \mid a \equiv bx \pmod{p}\}.$$

Temos que o volume de Λ é p (fixado b , a é determinado módulo p , logo Λ contém um em cada p pontos de \mathbb{Z}^2). Portanto, pelo teorema de Minkowski, existe um ponto $(a, b) \neq (0, 0)$ em Λ que pertence ao círculo com centro na origem e cujo raio é $\sqrt{3p/2}$ pois a área deste círculo é $3p\pi/2 > 2^2p = 2^2 \text{vol}(\Lambda)$. Assim, $0 < a^2 + b^2 < 3p/2$ e

$$a^2 + b^2 \equiv b^2(x^2 + 1) \pmod{p} \iff a^2 + b^2 \equiv 0 \pmod{p}$$

Ou seja, $a^2 + b^2 = p$. □

Teorema 4.20. *Todo primo p é soma de quatro quadrados.*

DEMONSTRAÇÃO: Pelo lema 4.11, temos que existem inteiros u, v tais que $u^2 + v^2 + 1 \equiv 0 \pmod{p}$. Considere o reticulado em \mathbb{R}^4 dado por

$$\Lambda \stackrel{\text{def}}{=} \{(a, b, c, d) \in \mathbb{Z}^4 \mid a \equiv cu + dv \pmod{p} \text{ e } b \equiv cv - du \pmod{p}\}.$$

Temos que Λ tem volume p^2 (fixados c e d , a e b ficam determinados módulo p , logo Λ contém um a cada p^2 pontos em \mathbb{Z}^4). A esfera de raio r em \mathbb{R}^4 tem volume $\pi^2 r^4/2$. Tomando $r = \sqrt{19p/10}$, como $\pi^2(\frac{19p}{10})^2/2 > 2^4 \text{vol}(\Lambda) = 16p^2$ pelo teorema de Minkowski existe um ponto $(a, b, c, d) \in \Lambda$ tal que $0 < a^2 + b^2 + c^2 + d^2 \leq 19p/10 < 2p$. Porém

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv (c^2 + d^2)(u^2 + v^2 + 1) \pmod{p} \\ \iff a^2 + b^2 + c^2 + d^2 &\equiv 0 \pmod{p} \end{aligned}$$

Logo $a^2 + b^2 + c^2 + d^2 = p$. □

Problemas Propostos

4.15. *Encontre todos os pontos racionais das seguintes cônicas.*

(a) $x^2 + 2y^2 = 3$

(b) $x^2 - y^2 = 1$

(c) $x^2 + xy + y^2 = 2$

(d) $13x^2 - xy - y^2 = 1$

$$(e) \ x^2 + y^2 + 2xy + x - y = 20$$

$$(f) \ 3x^2 - 7y^2 = 1$$

4.16. *Demonstrar que se um número pode ser escrito como soma de dois quadrados de forma única, a menos da ordem dos somandos, então tal número é primo.*

4.17 (Scholz). *Prove a seguinte generalização do lema de Thue. Seja n um número natural positivo e e, f números naturais tais que $ef > n$ com $e > 1$ e $f < n$. Então para todo a com $\text{mdc}(a, n) = 1$ a congruência $ay \equiv \pm x \pmod{n}$ tem solução com $0 < x < e$ e $0 < y < f$.*

4.18. *Seja $p > 5$ um número primo. Mostrar que $p = x^2 + 5y^2$ tem soluções inteiras se e somente se $p \equiv 1$ ou $9 \pmod{20}$.*

4.19. *Suponha que $3^n = q2^n + r$ com $r < 2^n$ e $r + q \geq 2^n$. Então*

$$g(n) \geq 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^n \right\rfloor - 3.$$

Observe que a conjectura de Euler implica que, para todo n , $r + q < 2^n$.

4.20 (IMO1992). *Seja n um inteiro positivo. Denotemos por $S(n)$ o maior inteiro tal que, para todo $k \leq S(n)$, n^2 pode se escrever como soma de k quadrados positivos.*

1. *Mostre que $S(n) \leq n^2 - 14$ para cada $n \geq 4$.*
2. *Encontre um inteiro n tal que $S(n) = n^2 - 14$.*
3. *Demonstre que existem infinitos inteiros n tais que $S(n) = n^2 - 14$.*

4.3 Descenso Infinito de Fermat

Dada uma equação

$$f(x_1, \dots, x_n) = 0,$$

o método do descenso infinito (quando aplicável) permite mostrar que esta equação não possui soluções inteiras positivas ou, sob certas condições, até mesmo encontrar todas as suas soluções inteiras. Se o conjunto de soluções de f

$$A = \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid f(x_1, \dots, x_n) = 0\}$$

é diferente de vazio, então gostaríamos de considerar a solução “mínima” em certo sentido. Em outras palavras, queremos construir uma função $\phi: A \rightarrow \mathbb{N}$ e considerar a solução $(x_1, \dots, x_n) \in A$ com $\phi(x_1, \dots, x_n)$ mínimo. O descenso consiste em obter, a partir desta solução mínima, uma ainda menor, o que nos conduz claramente a uma contradição, provando que A é de fato vazio.

Para ilustrar este método consideremos o seguinte

Exemplo 4.21 (Fermat). *Demonstrar que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas.*

SOLUÇÃO: Suponhamos que $x^4 + y^4 = z^2$ possui uma solução inteira com $x, y, z > 0$. Logo existe uma solução (a, b, c) na qual c é mínimo. Em particular, temos que a e b são primos entre si, pois se $d = \text{mdc}(a, b) > 1$ poderíamos substituir (a, b, c) por $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2})$ e obter uma solução com c menor. De $(a^2)^2 + (b^2)^2 = c^2$ temos portanto que (a^2, b^2, c) é uma tripla pitagórica primitiva e assim existem inteiros positivos m e n primos relativos tais que

$$a^2 = m^2 - n^2, \quad b^2 = 2mn \quad \text{e} \quad c = m^2 + n^2.$$

Temos da primeira equação que (a, n, m) é uma tripla pitagórica primitiva e portanto m é ímpar. Assim, de $b^2 = 2mn$ concluímos que b , e portanto n , é par. Observando ainda que $b^2 = (2n)m$ é um quadrado perfeito e $\text{mdc}(2n, m) = 1$, concluímos que tanto $2n$ como m são quadrados perfeitos, donde podemos encontrar inteiros positivos s e t tais que

$$2n = 4s^2 \quad \text{e} \quad m = t^2.$$

Por outra parte, dado que $a^2 + n^2 = m^2$, então existirão inteiros positivos i e j , primos entre si, tais que

$$a = i^2 - j^2, \quad n = 2ij \quad \text{e} \quad m = i^2 + j^2.$$

Portanto $s^2 = \frac{n}{2} = ij$, logo i e j serão quadrados perfeitos, digamos $i = u^2$ e $j = v^2$.

Logo temos que $m = i^2 + j^2$, $i = u^2$, $j = v^2$ e $m = t^2$, assim

$$t^2 = u^4 + v^4,$$

isto é, (u, v, t) é outra solução da equação original. Porém

$$t \leq t^2 = m \leq m^2 < m^2 + n^2 = c$$

e $t \neq 0$ porque m é diferente de 0. Isto contradiz a minimalidade de c , o que conclui a demonstração. \square

Observemos além disso que, uma vez que esta equação não possui soluções inteiras positivas, então a equação $x^4 + y^4 = z^4$ e, mais geralmente $x^{4n} + y^{4n} = z^{4n}$, não possuem soluções inteiras positivas.

Exemplo 4.22 (IMO1981). *Encontrar todas as soluções inteiras positivas da equação*

$$m^2 - mn - n^2 = \pm 1.$$

SOLUÇÃO: Note que $m^2 = n^2 + mn \pm 1 \geq n^2 \implies m \geq n$, com igualdade se, e só se, $(m, n) = (1, 1)$, que é claramente uma solução. Agora seja (m, n) uma solução com $m > n$. Demonstremos que $(n, m-n)$ também é solução. Para isto observemos que

$$\begin{aligned} n^2 - n(m-n) - (m-n)^2 &= n^2 - nm + n^2 - m^2 + 2mn - n^2 \\ &= n^2 + nm - m^2 \\ &= -(m^2 - nm - n^2) = \mp 1, \end{aligned}$$

Assim, se temos uma solução (m, n) , podemos encontrar uma cadeia descendente de soluções, e este processo parará quando atingirmos uma solução (a, b) com $a = b$, ou seja, a solução $(1, 1)$. Invertendo o processo, encontraremos portanto todas as soluções, isto é, se (m, n) é solução então $(m+n, m)$ é solução. Portanto todas as soluções positivas são

$$(1, 1), (2, 1), (3, 2), \dots, (F_{n+1}, F_n), \dots$$

onde F_n representa o n -ésimo termo da sequência de Fibonacci. \square

Exemplo 4.23 (IMO2003). *Determine todos os pares de inteiros positivos (a, b) para os quais*

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

é um inteiro positivo.

SOLUÇÃO: Seja (a, b) uma solução inteira positiva. Logo $2ab^2 - b^3 + 1 \geq 1$, e portanto $a \geq \frac{b}{2}$. No caso $a = \frac{b}{2}$, é claro que obtemos uma solução. Para qualquer outra solução, $a > \frac{b}{2}$ e nesse caso $a^2 \geq 2ab^2 - b^3 + 1 = b^2(2a - b) + 1 > b^2 \implies a > b$.

Agora se $\frac{a^2}{2ab^2 - b^3 + 1} = k \in \mathbb{N}$, então a é raiz do polinômio com coeficientes inteiros

$$x^2 - 2kb^2x + k(b^3 - 1) = 0.$$

Mas este polinômio possui outra solução inteira $a_1 = 2kb^2 - a = \frac{k(b^3 - 1)}{a} \geq 0$, assim (a_1, b) também é solução do problema se $b > 1$. Supondo que a é a maior raiz, de $a \geq a_1$ teremos que $a \geq kb^2$ e assim

$$a_1 = \frac{k(b^3 - 1)}{a} \leq \frac{k(b^3 - 1)}{kb^2} < b.$$

Desta forma, ou $b = 1$ ou $a_1 = \frac{b}{2}$ e neste último caso $k = \frac{b^2}{4}$ e $a = \frac{b^4}{2} - \frac{b}{2}$. Portanto as soluções do problema são $(a, b) = (l, 2l)$, $(2l, 1)$ ou $(8l^4 - l, 2l)$, com $l \in \mathbb{N}$. \square

4.3.1 Equação de Markov

A equação de Markov é a equação diofantina em inteiros positivos

$$x^2 + y^2 + z^2 = 3xyz.$$

É óbvio que $(1, 1, 1)$ e $(1, 1, 2)$ são soluções da equação. Além disso, como a equação é simétrica, podemos considerar, sem perda de generalidade, somente as soluções com as coordenadas $x \leq y \leq z$ ordenadas de forma não decrescente.

Assim suponhamos que (x, y, z) é uma solução com $x \leq y \leq z$ com $z > 1$. O polinômio quadrático

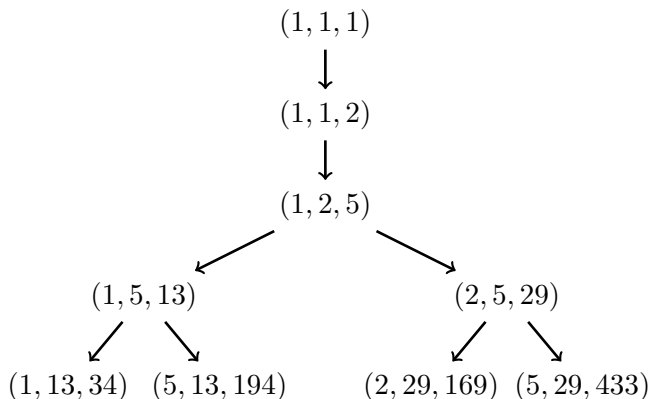
$$T^2 - 3xyT + (x^2 + y^2) = 0$$

possui duas soluções, e uma delas é z , assim a outra é $z' = 3xy - z = \frac{x^2 + y^2}{z} \in \mathbb{Z} \setminus \{0\}$. Vejamos que se $y > 1$ então $z' < y$, e assim (z', x, y) é também solução (menor) da equação de Markov. Para isto, suponhamos por contradição que $\frac{x^2 + y^2}{z} = z' \geq y$, isto é, $yz \leq x^2 + y^2 \leq 2y^2$, em particular $z \leq 2y$. Segue que

$$5y^2 \geq y^2 + z^2 = 3xyz - x^2 = x(3yz - x) \geq xy(3z - 1),$$

e portanto $5y \geq x(3z - 1)$. Observemos que se $x \geq 2$, então $5y \geq 2(3z - 1) \geq 5z$ e portanto $x = y = z = 2$, que não é solução, o que é contraditório. Logo $x = 1$ e $\frac{1+y^2}{y} \geq z$, assim $\frac{1}{y} + y \geq z \geq y$. Portanto ou temos $\frac{1}{y} + y = z$, e neste caso $y = 1$ e $z = 2$, o que contradiz $y > 1$, ou $y = z$ e substituindo na equação original temos que $1 + y^2 + y^2 = 3y^2$, o que implica que $z = y = 1$, o que contradiz o fato de $z > 1$.

Do fato anterior, temos que dada uma solução da equação de Markov (x, y, z) com $z \geq 2$ é sempre possível encontrar uma solução menor (z', x, y) e este processo somente para quando chegamos à solução $(1, 1, 1)$, isto é, estamos gerando uma árvore de soluções da seguinte forma:



Um importante problema em aberto relacionado com a equação de Markov é o *problema da unicidade*, proposto por Frobenius há cerca de 100 anos em [55] (veja também [28]): para quaisquer inteiros positivos x_1, x_2, y_1, y_2, z com $x_1 \leq y_1 \leq z$ e $x_2 \leq y_2 \leq z$ tais que (x_1, y_1, z) e (x_2, y_2, z) são soluções da equação de Markov temos necessariamente $(x_1, y_1) = (x_2, y_2)$?

Se o problema da unicidade admitir uma solução afirmativa, para cada t real, sua pré-imagem $k^{-1}(t)$ pela função k definida na seção 3.4 consistirá de uma única classe de $GL_2(\mathbb{Z})$ -equivalência (veja o exercício 3.10).

4.3.2 Último Teorema de Fermat

Um dos mais famosos problemas na história da Matemática e talvez um dos que mais inspirou o desenvolvimento de novas teorias é o

chamado *último teorema de Fermat*.

Pierre de Fermat, que tinha o costume de fazer anotações nas margens de sua cópia do livro de Diofanto, enunciou o teorema que afirma ser impossível encontrar inteiros positivos x, y, z tais que

$$x^n + y^n = z^n \quad (*)$$

quando n é um inteiro maior do que 2: “encontrei uma demonstração verdadeiramente maravilhosa para isto, mas a margem é demasiado pequena para contê-la”.

Para mostrar a inexistência de soluções de $(*)$, basta considerar os expoentes primos. Muitos casos particulares foram mostrados ao longo da história, os quais se dividem em dois tipos: o primeiro, quando $p \nmid xyz$, e o segundo, mais difícil, quando $p \mid xyz$. De fato, Sophie Germain provou o primeiro caso para todo primo p tal que $2p + 1$ também é primo (veja a proposição 7.2). Legendre provou o teorema para p primo quando $4p + 1, 8p + 1, 10p + 1, 14p + 1$ ou $16p + 1$ é primo; com isto, provou o último teorema de Fermat para todo $p < 100$. Em 1849, Kummer obteve uma prova para todos os chamados *primos regulares*. Em 1909 Wieferich provou que se a equação de Fermat tem solução para p , então $2^{p-1} \equiv 1 \pmod{p^2}$; tais primos são chamados *primos de Wieferich*. Mirimanoff e Vandiver provaram respectivamente que p deve satisfazer $3^{p-1} \equiv 1 \pmod{p^2}$ e $5^{p-1} \equiv 1 \pmod{p^2}$, e Frobenius provou este mesmo resultado para 11 e 17 no lugar de 3 e 5.

A demonstração do último teorema de Fermat somente foi obtida depois de mais de trezentos anos após sua formulação. Tal demonstração, devida a Andrew Wiles e Richard Taylor ([151] e [146]), insere-se no contexto mais geral da chamada *conjectura de Taniyama-Shimura-Weil* sobre curvas elípticas (veja o capítulo 9 para uma introdução a curvas elípticas), que implica a solução do último teorema de Fermat, como conjecturado por G. Frey em 1985 e provado por K. Ribet em 1986. Esta demonstração envolve ideias bastante avançadas e está muito longe do escopo deste livro. Para uma introdução às técnicas utilizadas na prova, veja [39].

Para dar uma ideia da dificuldade deste problema, vejamos uma prova baseada na de Leonhard Euler para o caso $n = 3$. A demonstração original dada por Euler para o caso $n = 3$ é incompleta já que supõe a fatoração única em irredutíveis para extensões de \mathbb{Z} (veja mais detalhes sobre este ponto no teorema 6.17). Começamos com um

Lema 4.24. *Todas as soluções de $s^3 = a^2 + 3b^2$ em inteiros positivos tais que $\text{mdc}(a, b) = 1$ e s é ímpar são dadas por*

$$s = m^2 + 3n^2, \quad a = m^3 - 9mn^2, \quad b = 3m^2n - 3n^3,$$

com $m + n$ ímpar e $\text{mdc}(m, 3n) = 1$.

DEMONSTRAÇÃO: É fácil verificar que tais números fornecem uma solução da equação e, além disso,

$$\begin{aligned} \text{mdc}(a, b) &= \text{mdc}(m(m^2 - 9n^2), 3n(m^2 - n^2)) \\ &= \text{mdc}(m^2 - 9n^2, m^2 - n^2) = \text{mdc}(8n^2, m^2 - n^2) = 1. \end{aligned}$$

Reciprocamente, suponhamos que (a, b, s) é solução da equação. Seja p um número primo tal que $p \mid s$. Note que, como $\text{mdc}(a, b) = 1$ e s é ímpar, $p \nmid a$, $p \nmid b$ e $p > 3$. Então $a^2 \equiv -3b^2 \pmod{p}$ e como b é invertível módulo p temos

$$\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod{6}$$

pela lei de reciprocidade quadrática. Pelo exemplo 4.8 (ou teorema 6.17) sabemos que existem inteiros m_1 e n_1 tais que $p = m_1^2 + 3n_1^2$, e teremos que $p^3 = c^2 + 3d^2$ onde $c = m_1^3 - 9m_1n_1^2$ e $d = 3m_1^2n_1 - 3n_1^3$. Note que $\text{mdc}(p, m_1) = \text{mdc}(p, n_1) = 1$ e $p > 3$ e portanto $\text{mdc}(p, c) = \text{mdc}(p, d) = 1$, como na demonstração acima de que $\text{mdc}(a, b) = 1$.

Procederemos por indução sobre o número de divisores primos de s . Se $s = 1$ o resultado é evidente. O caso em que s tem um divisor primo é exatamente o resultado anterior. Agora, suponhamos que o resultado valha para todo s que tenha k fatores primos (não necessariamente distintos). Se s tem $k + 1$ fatores primos, digamos $s = pt$ com p primo ($p > 3$), observemos que

$$t^3p^6 = s^3p^3 = (a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2.$$

Além disso como

$$\begin{aligned} (ad + bc)(ad - bc) &= (ad)^2 - (bc)^2 = d^2(a^2 + 3b^2) - b^2(c^2 + 3d^2) \\ &= p^3(t^3d^2 - b^2), \end{aligned}$$

então $p^3 \mid (ad + bc)(ad - bc)$. Se p divide os dois fatores, teremos que $p \mid ad$ e $p \mid bc$. Lembre que $\text{mdc}(p, c) = \text{mdc}(p, d) = 1$, o que implica que $p \mid a$ e $p \mid b$, o que contradiz a hipótese $\text{mdc}(a, b) = 1$. Assim, p^3 divide exatamente um dos fatores, e tomando adequadamente os sinais teremos que

$$u = \frac{ac \pm 3bd}{p^3}, \quad v = \frac{ad \mp bc}{p^3}$$

são inteiros tais que $t^3 = u^2 + 3v^2$. Como t tem k fatores primos segue por hipótese de indução que

$$t = m_2^2 + 3n_2^2, \quad u = m_2^3 - 9m_2n_2^2, \quad v = 3m_2^2n_2 - 3n_2^3.$$

Agora, dado que $a = uc + 3vd$ e $b = \pm(ud - vc)$, substituindo t, u, v, c e d em termos de m_i e n_i ($i = 1, 2$) em s, a e b e fazendo $m = m_1m_2 + 3n_1n_2$, $n = m_1n_2 - m_2n_1$, obteremos o que queríamos demonstrar. \square

O método utilizado por Euler para demonstrar o caso $n = 3$ é basicamente o método de descenso infinito.

Proposição 4.25. *A equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras com $xyz \neq 0$.*

DEMONSTRAÇÃO: Suponhamos que a equação $x^3 + y^3 = z^3$ possui uma solução com $x, y, z > 0$ e escolhemos esta solução de tal forma que xyz seja mínimo. Como qualquer fator comum de dois destes números é também fator do terceiro, podemos afirmar que x, y, z são primos relativos dois a dois. Em particular um de tais números será par.

Note que $x = y$ é impossível pois caso contrário $2x^3 = z^3$ e o expoente da maior potência de 2 do lado direito seria múltiplo de 3, enquanto que do lado esquerdo não. Assim, sem perda de generalidade, podemos assumir que $x > y$.

Suponha primeiro que x e y são ímpares e z par, podemos escrever $x = p + q$ e $y = p - q$ com $p > 0$ e $q > 0$ primos relativos (pois x e y são primos relativos) e de diferente paridade, assim

$$\begin{aligned} x^3 + y^3 &= (x + y)(x^2 - xy + y^2) \\ &= 2p((p + q)^2 - (p + q)(p - q) + (p - q)^2) \\ &= 2p(p^2 + 3q^2). \end{aligned}$$

Portanto $2p(p^2 + 3q^2)$ é um cubo perfeito. De igual forma, no caso em que z é ímpar e x ou y é par, podemos supor sem perda de generalidade que y é ímpar, e substituindo $z = q + p$ e $y = q - p$ obteremos

$$\begin{aligned} x^3 &= z^3 - y^3 = 2p((p+q)^2 + (p+q)(q-p) + (q-p)^2) \\ &= 2p(p^2 + 3q^2). \end{aligned}$$

Como $p^2 + 3q^2$ é ímpar e $2p(p^2 + 3q^2)$ é um cubo perfeito temos que p será par. Calculando o máximo comum divisor entre p e $p^2 + 3q^3$, obtemos

$$\text{mdc}(p, p^2 + 3q^2) = \text{mdc}(p, 3q^2) = \text{mdc}(p, 3).$$

Portanto há dois casos: $\text{mdc}(p, 3) = 1$ e $\text{mdc}(p, 3) = 3$.

No primeiro, existem naturais a e b tais que $a^3 = 2p$ e $b^3 = p^2 + 3q^2$. Neste caso sabemos, pelo lema 4.24, que existem inteiros m e n de diferente paridade e primos relativos tais que

$$b = m^2 + 3n^2, \quad p = m^3 - 9mn^2, \quad q = 3m^2n - 3n^3.$$

Logo $a^3 = 2m(m - 3n)(m + 3n)$. Observemos que os números $2m$, $m - 3n$ e $m + 3n$ são primos relativos, logo existem inteiros e , f e g tais que $2m = e^3$, $m - 3n = f^3$ e $m + 3n = g^3$. Em particular, teremos que $f^3 + g^3 = e^3$. Como

$$efg = a^3 = 2p \leq x + y < xyz,$$

teremos uma solução menor, o que contradiz a escolha de x, y, z .

No caso em que $3 \mid p$, então $p = 3r$ com $\text{mdc}(r, q) = 1$, logo $z^3 = 18r(3r^2 + q^2)$ ou $x^3 = 18r(3r^2 + q^2)$ e portanto existem inteiros positivos a e b tais que $18r = a^3$ e $3r^2 + q^2 = b^3$. De novo, existiriam inteiros m e n tais que

$$b = m^2 + 3n^2, \quad q = m^3 - 9mn^2, \quad r = 3m^2n - 3n^3.$$

Daqui segue que $a^3 = 27(2n)(m - n)(m + n)$. De igual forma teremos que os números $2n$, $m - n$ e $m + n$ são primos relativos, portanto existem inteiros positivos e , f e g tais que

$$2n = e^3, \quad m - n = f^3, \quad m + n = g^3.$$

Segue que $e^3 + f^3 = g^3$, que também contradiz a minimalidade da solução (x, y, z) . \square

Exemplo 4.26. *Demonstrar que a equação $x^2 + 432 = y^3$ não tem soluções racionais diferentes de $(\pm 36, 12)$.*

SOLUÇÃO: Suponhamos que a equação possui uma solução (a, b) com $b \neq 12$. Como a e b são racionais, então $\frac{a}{36} = \frac{k}{n} \neq \pm 1$ e $\frac{b}{12} = \frac{m}{n} \neq 1$ com $k, m, n \in \mathbb{Z}$. Seja $u = n + k \neq 0$, $v = n - k \neq 0$ e $w = 2m$. Como

$$u^3 + v^3 - w^3 = 2n^3 + 6nk^2 - 8m^3$$

e $k = \frac{an}{36}$, $m = \frac{bn}{12}$, substituindo temos

$$u^3 + v^3 - w^3 = 2n^3 + \frac{n^3 a^2}{6^3} - \frac{n^3 b^3}{6^3} = \frac{n^3}{216}(432 + a^2 - b^3) = 0.$$

o que gera uma solução não trivial da equação $x^3 + y^3 = z^3$, um absurdo. \square

Problemas Propostos

4.21. *Seja p um primo. Prove que se x, y e z são inteiros com $x^3 + py^3 + p^2z^3 = 0$ então $x = y = z = 0$.*

4.22. *Demonstrar que não existe um triângulo retângulo com lados inteiros tal que sua área seja um quadrado perfeito.*

4.23. *Encontrar todos os pares (n, m) de números inteiros tais que $n \mid m^2 + 1$ e $m \mid n^2 + 1$.*

4.24 (IMO1987). *Seja n um inteiro maior ou igual a 2. Mostre que se $k^2 + k + n$ é primo para todo k tal que $0 \leq k \leq \sqrt{\frac{n}{3}}$, então $k^2 + k + n$ é primo para todo k tal que $0 \leq k \leq n - 2$.*

4.25 (IMO1988). *Dados inteiros a e b tais que o número $ab + 1$ divide $a^2 + b^2$, demonstrar que $\frac{a^2 + b^2}{ab + 1}$ é um quadrado perfeito.*

4.26 (IMO2007). *Prove que se a e b são inteiros positivos tais que $4ab - 1 \mid (4a^2 - 1)^2$ então $a = b$.*

4.27. *Demonstrar que a equação $3x^2 + 1 = y^3$ não tem soluções racionais diferentes de $x = \pm 1$ e $y = 1$.*

4.28. *Demonstrar que a equação $x^3 + y^3 + z^3 = 1$ possui infinitas soluções inteiras.*

4.29. *Demonstrar que a equação $x^3 + y^3 + z^3 = n$ com $n = 9k \pm 4$ não possui soluções inteiras.*

Observação: Em 1999 foi encontrada a solução

$$(-283059965, -2218888517, 2220422932),$$

para $n = 30$ e em 2000 foi encontrada a solução

$$(60702901317, 23961292454, -61922712865)$$

para $n = 52$ (ver [9]). Em maio de 2013, os únicos valores de n menores que 100 para os quais não se sabia se existe ou não solução inteira eram 33, 42, e 74.

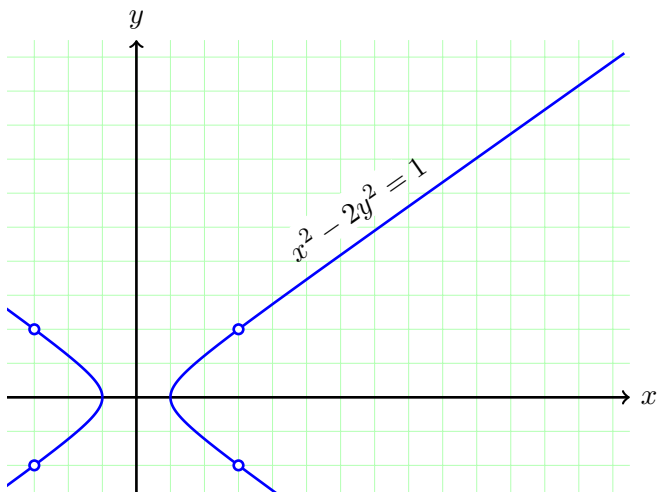
4.30. *Demonstrar que a equação $x^3 + y^3 + z^3 = t^3$ possui infinitas soluções inteiras positivas primitivas (i.e., com $\text{mdc}(x, y, z, t) = 1$).*

4.31. *Demonstrar que a equação $x^3 + y^3 = 2z^3$ não possui soluções inteiras positivas não triviais (i.e. além das com $x = y = z$).*

Dica: Como x, y são de igual paridade então $x = m + n$, $y = m - n$. Se $\text{mdc}(m, 3) = 1$ concluir que $\text{mdc}(m, m^2 + 3n^2) = 1$ e cada um deles é um cubo. Usar a caracterização das soluções da equação $s^3 = m^2 + 3n^2$ para chegar a uma solução menor que a inicial.

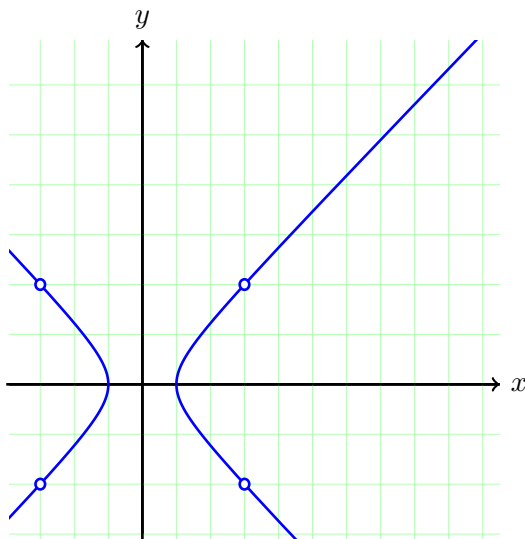
4.4 Equação de Pell

Seja A um inteiro positivo. Estamos interessados na equação $x^2 - Ay^2 = 1$, com x e y inteiros. Se A é um quadrado perfeito, digamos $A = k^2$, temos que $x^2 - Ay^2 = (x - ky)(x + ky) = 1$ admite apenas as soluções triviais $y = 0$, $x = \pm 1$, pois teríamos $x - ky = x + ky = \pm 1$. O caso interessante é quando A não é um quadrado perfeito, e portanto \sqrt{A} é um irracional (de fato, se $\sqrt{A} = \frac{p}{q}$, com $\text{mdc}(p, q) = 1$ e $q > 1$, teríamos $A = \frac{p^2}{q^2}$ o que é um absurdo, pois $\text{mdc}(p, q) = 1 \implies \text{mdc}(p^2, q^2) = 1$, donde p^2/q^2 não pode ser inteiro). Nesse caso, a equação $x^2 - Ay^2 = 1$ é conhecida como uma *equação de Pell*.



As soluções da equação de Pell correspondem a pontos inteiros sobre uma hipérbole. Na figura, a hipérbole é $x^2 - 2y^2 = 1$: o ponto $(3, 2)$ é um exemplo de ponto inteiro sobre a hipérbole pois $3^2 - 2 \cdot 2^2 = 1$ mas o ponto $(7, 5)$ está próximo à hipérbole mas não pertence a ela pois $7^2 - 2 \cdot 5^2 = -1 \neq 1$. Como veremos, o próximo ponto de coordenadas inteiras positivas sobre esta hipérbole é $(17, 12)$, que está fora da figura.

Outro ponto de vista é o de que estamos procurando pontos de uma hipérbole sobre um reticulado. Na próxima figura, a hipérbole é $u^2 - v^2 = 1$ e o reticulado consiste nos pontos da forma $(a, b\sqrt{2})$, a e b inteiros. As duas figuras só diferem por uma transformação linear.



Um terceiro ponto de vista, que será particularmente útil no que segue tem um caráter mais algébrico: sejam $\mathbb{Z}[\sqrt{A}] = \{x + y\sqrt{A}; x, y \in \mathbb{Z}\}$ e $\mathbb{Q}[\sqrt{A}] = \{x + y\sqrt{A}; x, y \in \mathbb{Q}\} \supset \mathbb{Z}[\sqrt{A}]$. Não é difícil ver que $\mathbb{Z}[\sqrt{A}]$ é um anel e $\mathbb{Q}[\sqrt{A}]$ é um corpo. Dado $\gamma = x + y\sqrt{A} \in \mathbb{Q}[\sqrt{A}]$ (com $x, y \in \mathbb{Q}$), podemos definir seu *conjugado* $\hat{\gamma} = x - y\sqrt{A}$, e sua *norma* $N(\gamma) = \gamma\hat{\gamma} = x^2 - Ay^2$.

Uma observação relevante é que, se $x, y, z, w \in \mathbb{Q}$ e $x + y\sqrt{A} = z + w\sqrt{A}$ então $x = z$ e $y = w$. De fato, se $y = w$ então claramente $x = z$, e se $y \neq w$, teríamos $\sqrt{A} = \frac{z-x}{y-w} \in \mathbb{Q}$, absurdo.

As soluções inteiras (x, y) da equação de Pell correspondem a elementos $x + y\sqrt{A} \in \mathbb{Z}[\sqrt{A}]$ (com $x, y \in \mathbb{Z}$) cuja norma $N(x + y\sqrt{A}) = x^2 - Ay^2$ é igual a 1.

Um fato muito importante sobre a norma é que $N: \mathbb{Q}[\sqrt{A}] \rightarrow \mathbb{Q}$ é uma função multiplicativa, isto é,

$$N((x + y\sqrt{A})(u + v\sqrt{A})) = N(x + y\sqrt{A})N(u + v\sqrt{A}) \quad \forall x, y, u, v \in \mathbb{Q}.$$

Isto segue do fato de que, dados $\alpha = x + y\sqrt{A}, \gamma = u + v\sqrt{A} \in \mathbb{Q}[\sqrt{A}]$, $\alpha\hat{\gamma} = \hat{\alpha}\gamma$ (o conjugado de $\alpha\gamma = (x + y\sqrt{A})(u + v\sqrt{A}) = (xu + Ayv) + (xv + yu)\sqrt{A}$ é $(xu + Ayv) - (xv + yu)\sqrt{A} = (x - y\sqrt{A})(u - v\sqrt{A}) = \hat{\alpha}\hat{\gamma}$). Com efeito,

$$N(\alpha\gamma) = \alpha\gamma\hat{\alpha}\hat{\gamma} = \alpha\hat{\alpha}\hat{\gamma}\gamma = N(\alpha)N(\gamma).$$

Alternativamente, podemos provar este fato diretamente:

$$\begin{aligned}
 N((x + y\sqrt{A})(u + v\sqrt{A})) &= N((xu + Ayv) + (xv + yu)\sqrt{A}) \\
 &= (xu + Ayv)^2 - A(xv + yu)^2 \\
 &= x^2u^2 + A^2y^2v^2 - A(x^2v^2 + y^2u^2) \\
 &= (x^2 - Ay^2)(u^2 - Av^2).
 \end{aligned}$$

É fácil ver (a partir da multiplicatividade da norma) que se a equação tem alguma solução (x_1, y_1) com $y_1 \neq 0$ então possui infinitas. Mais geralmente, se $x_1^2 - Ay_1^2 = \pm 1$, temos

$$N((x_1 + \sqrt{A}y_1)^n) = (x_1 - \sqrt{A}y_1)^n(x_1 + \sqrt{A}y_1)^n = (x_1^2 - Ay_1^2)^n = (\pm 1)^n.$$

Fazendo a substituição

$$x_n + \sqrt{A}y_n = (x_1 + \sqrt{A}y_1)^n = \sum_{i=0}^n \binom{n}{i} x_1^{n-i} (\sqrt{A})^i y_1^i$$

onde

$$x_n = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} x_1^{n-2i} A^i y_1^{2i} \quad \text{e} \quad y_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} x_1^{n-2i-1} A^i y_1^{2i+1}$$

obtemos $x_n^2 - Ay_n^2 = (\pm 1)^n$ para todo $n \in \mathbb{N}$.

De maneira mais ou menos equivalente, podemos dizer que se (x_1, y_1) é solução então a transformação linear

$$\begin{pmatrix} x_1 & y_1\sqrt{A} \\ y_1\sqrt{A} & x_1 \end{pmatrix}$$

preserva tanto a hipérbole $u^2 - v^2 = 1$ quanto o reticulado que consiste nos pontos da forma $(a, b\sqrt{A})$.

Vejam agora que a equação de Pell sempre possui solução.

Teorema 4.27. *A equação $x^2 - Ay^2 = 1$, com A diferente de um quadrado perfeito, possui solução não trivial em inteiros positivos, i.e., com $x + y\sqrt{A} > 1$.*

DEMONSTRAÇÃO: Como \sqrt{A} é irracional, a desigualdade $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$ tem infinitas soluções racionais p/q . Note que se $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$ então

$$\begin{aligned} |p^2 - Aq^2| &= q^2 \left| \sqrt{A} - \frac{p}{q} \right| \left| \frac{p}{q} + \sqrt{A} \right| < \left| \frac{p}{q} + \sqrt{A} \right| \\ &\leq 2\sqrt{A} + \left| \sqrt{A} - \frac{p}{q} \right| \leq 2\sqrt{A} + 1. \end{aligned}$$

Considerando infinitos pares de inteiros positivos (p_n, q_n) com $|\sqrt{A} - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$, teremos sempre $|p_n^2 - Aq_n^2| < 2\sqrt{A} + 1$, portanto temos um número finito de possibilidades para o valor (inteiro) de $p_n^2 - Aq_n^2$. Consequentemente, existe um inteiro $k \neq 0$ tal que $p_n^2 - Aq_n^2 = k$ para infinitos valores de n . Obtemos portanto duas sequências crescentes de pares de inteiros positivos $(u_r), (v_r)$, $r \in \mathbb{N}$ tais que $u_r^2 - Av_r^2 = k$ para todo r .

Como há apenas $|k|^2$ possibilidades para os pares $(u_r \bmod k, v_r \bmod k)$, existem inteiros a e b e infinitos valores de r tais que $u_r \equiv a \pmod{k}$ e $v_r \equiv b \pmod{k}$. Tomamos então $r < s$ com as propriedades acima. Seja

$$\begin{aligned} x + y\sqrt{A} &= \frac{u_s + v_s\sqrt{A}}{u_r + v_r\sqrt{A}} = \frac{(u_s + v_s\sqrt{A})(u_r - v_r\sqrt{A})}{u_r^2 - Av_r^2} \\ &= \frac{u_s u_r - Av_s v_r}{k} + \left(\frac{u_r v_s - u_s v_r}{k} \right) \sqrt{A}. \end{aligned}$$

Temos $u_s u_r - Av_s v_r \equiv u_r^2 - Av_r^2 = k \equiv 0 \pmod{k}$ e $u_r v_s - u_s v_r \equiv ab - ab = 0 \pmod{k}$ e portanto $x = \frac{u_s u_r - Av_s v_r}{k}$ e $y = \frac{u_r v_s - u_s v_r}{k}$ são inteiros. Por outro lado, $(x + y\sqrt{A})(u_r + v_r\sqrt{A}) = u_s + v_s\sqrt{A}$, donde $N(x + y\sqrt{A})N(u_r + v_r\sqrt{A}) = N(u_s + v_s\sqrt{A})$. Como $N(u_r + v_r\sqrt{A}) = N(u_s + v_s\sqrt{A}) = k$, segue que $N(x + y\sqrt{A}) = x^2 - Ay^2 = 1$. Além disso, como $s > r$, $u_s + v_s\sqrt{A} > u_r + v_r\sqrt{A}$, donde $x + y\sqrt{A} = \frac{u_s + v_s\sqrt{A}}{u_r + v_r\sqrt{A}} > 1$. \square

Dentre todas as soluções $(x, y) \in \mathbb{N}^2$ da equação de Pell $x^2 - y^2 A = 1$ com $x + y\sqrt{A} > 1$, existe uma *solução mínima* ou *fundamental*, i.e., com x e portanto y e $x + y\sqrt{A}$ mínimos. Denote por (x_1, y_1) esta solução mínima. Se, como antes, definimos $(x_n, y_n) \in \mathbb{N}^2$ pela relação $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$, temos que (x_n, y_n) , $n \geq 1$, são todas as soluções inteiras positivas da equação de Pell: de fato, já vimos que (x_n, y_n) são

soluções, e se (x', y') é uma outra solução, então como $x_1 + y_1\sqrt{A} > 1$ existe $n \geq 1$ tal que

$$(x_1 + y_1\sqrt{A})^n \leq x' + y'\sqrt{A} < (x_1 + y_1\sqrt{A})^{n+1}.$$

Multiplicando por $x_n - y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^{-n} > 0$, obtemos

$$\begin{aligned} 1 &\leq (x' + y'\sqrt{A})(x_n - y_n\sqrt{A}) = (x'x_n - y'y_nA) + (y'x_n - x'y_n)\sqrt{A} \\ &< x_1 + y_1\sqrt{A}. \end{aligned}$$

Como $N((x' + y'\sqrt{A})(x_n - y_n\sqrt{A})) = N(x' + y'\sqrt{A})N(x_n - y_n\sqrt{A}) = 1$, temos que $(x'x_n - y'y_nA, y'x_n - x'y_n)$ também é uma solução da equação de Pell, menor que a solução mínima. Temos que $x'x_n - y'y_nA \geq 0$, pois caso contrário $x'x_n - y'y_nA < 0 \iff \frac{x'}{y'} \frac{x_n}{y_n} < A$, porém

$$x_n^2 - y_n^2A = 1 \implies \left(\frac{x_n}{y_n}\right)^2 = A + \frac{1}{y_n^2} > A \implies \frac{x_n}{y_n} > \sqrt{A}$$

e analogamente $\frac{x'}{y'} > \sqrt{A}$, o que contradiz $\frac{x'}{y'} \frac{x_n}{y_n} < A$. Da mesma forma, $y'x_n - x'y_n \geq 0$ pois caso contrário

$$\begin{aligned} \frac{x_n}{y_n} < \frac{x'}{y'} &\implies A + \frac{1}{y_n^2} = \left(\frac{x_n}{y_n}\right)^2 < \left(\frac{x'}{y'}\right)^2 = A + \frac{1}{y'^2} \\ &\implies y' < y_n \implies x' < x_n \end{aligned}$$

o que contradiz o fato de $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n \leq x' + y'\sqrt{A}$. Resumindo, temos que $(x'x_n - y'y_nA, y'x_n - x'y_n) \in \mathbb{N}^2$ é uma solução menor do que a solução mínima, logo $x'x_n - y'y_nA = 1$ e $y'x_n - x'y_n = 0$, ou seja, $(x' + y'\sqrt{A})(x_1 - y_1\sqrt{A})^{-n} = 1 \iff x' + y'\sqrt{A} = x_n + y_n\sqrt{A}$, donde $(x', y') = (x_n, y_n)$, como queríamos.

Assim, as soluções com x e y inteiros positivos podem ser enumeradas por (x_n, y_n) , $n \geq 0$ de modo que, para todo n , $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$ e portanto

$$\begin{aligned} x_n &= \frac{(x_1 + y_1\sqrt{A})^n + (x_1 - y_1\sqrt{A})^n}{2} & \text{e} \\ y_n &= \frac{(x_1 + y_1\sqrt{A})^n - (x_1 - y_1\sqrt{A})^n}{2\sqrt{A}}. \end{aligned}$$

Observe que as sequências (x_n) e (y_n) acima satisfazem a recorrência $u_{n+2} = 2x_1u_{n+1} - u_n$, $\forall n \geq 1$.

A conjectura de Catalan afirma que as únicas potências perfeitas consecutivas são 8 e 9 e foi resolvida completamente em 2003 por Mihăilescu. Vejamos uma aplicação da equação de Pell em um caso particular.

Teorema 4.28 (Ko Chao). *Seja p um número primo com $p \geq 5$, então a equação*

$$x^2 - y^p = 1$$

não possui solução com x e y inteiros não nulos.

DEMONSTRAÇÃO: Suponhamos por contradição que a equação possui solução inteira não nula e sem perda de generalidade podemos supor $x > 0$ e $y > 0$.

No caso em que x é par e y é ímpar, fazendo $y^p = x^2 - 1 = (x - 1)(x + 1)$, como $\text{mdc}(x + 1, x - 1) = 1$, segue que $x - 1$ e $x + 1$ são potências p -ésimas, ou seja, existem inteiros s e t tais que $x - 1 = s^p$ e $x + 1 = t^p \implies t^p - s^p = 2$ com $s, t \in \mathbb{Z}$ e $p \geq 5$. Com isto a única solução é $t = 1$ e $s = -1$, mas isso implica que $x = 0$, o que foi descartado nas hipóteses.

Agora, no caso em que x é ímpar e y é par, temos que $x + 1$ e $x - 1$ são pares e $\text{mdc}(x + 1, x - 1) = 2$. Daqui podemos dividir o problema em dois subcasos:

No caso em que $\frac{x-1}{2}$ é ímpar, existem inteiros w e z tais que

$$\frac{x-1}{2} = w^p, \quad \frac{x+1}{2} = 2^{p-2}z^p \quad \text{e} \quad y = 2wz \quad \text{com} \quad \text{mdc}(w, 2z) = 1.$$

Assim

$$w^p = \frac{x+1}{2} - 1 = 2^{p-2}z^p - 1 \geq (2^{p-2} - 1)z^p,$$

isto é,

$$\left(\frac{w}{z}\right)^p \geq 2^{p-2} - 1 > 1,$$

portanto $w > z$.

Por outro lado

$$w^{2p} = \left(\frac{x-1}{2}\right)^2 = \frac{x^2 + 6x + 9 - 8(x+1)}{4} = \left(\frac{x+3}{2}\right)^2 - (2z)^p.$$

Assim obtemos a equação $(w^2)^p + (2z)^p = (\frac{x+3}{2})^2$. Como

$$\begin{aligned} \frac{(w^2)^p + (2z)^p}{w^2 + 2z} &= (w^2)^{p-1} - (w^2)^{p-2}(2z) + (w^2)^{p-3}(2z)^2 - \dots + (2z)^{p-1} \\ &\equiv p(w^2)^{p-1} \pmod{w^2 + 2z} \end{aligned}$$

e $\text{mdc}(w, 2z) = 1$ temos

$$\text{mdc}\left(w^2 + 2z, \frac{(w^2)^p + (2z)^p}{w^2 + 2z}\right) = \text{mdc}(w^2 + 2z, p(w^2)^{p-1}) \mid p,$$

logo se $p \nmid \frac{x+3}{2}$ temos que $w^2 + 2z$ é um quadrado. Mas $w^2 < w^2 + 2z < w^2 + 2w < (w+1)^2$ assim $w^2 + 2z$ não pode ser um quadrado, logo $p \mid \frac{x+3}{2}$ e além disso do fato que $p > 3$ segue que $p \nmid x$.

De forma similar, no caso que $\frac{x+1}{2} = w^p$ e $\frac{x-1}{2} = 2^{p-2}z^p$, usando a equação $(w^2)^p - (2z)^p = (\frac{x-3}{2})^2$, concluímos analogamente que $p \mid \frac{x-3}{2}$ e portanto $p \nmid x$.

Voltando à equação original temos que $x^2 = y^p + 1^p$. Como $p \nmid x$ e (como antes) $\text{mdc}\left(y + 1, \frac{y^p + 1}{y + 1}\right) \mid p$ temos que $y + 1 = s^2$. Logo $(s, 1)$ e $(x, y^{\frac{p-1}{2}})$ são soluções da equação de Pell

$$u^2 - yv^2 = 1.$$

Observe que $(s, 1)$ é uma solução fundamental pela minimalidade da segunda coordenada, donde existe um natural $m \in \mathbb{N}$ tal que

$$x + y^{\frac{p-1}{2}}\sqrt{y} = (s + \sqrt{y})^m.$$

Desenvolvendo a anterior identidade obtemos

$$\begin{aligned} x &= s^m + \binom{m}{2}s^{m-2}y + \binom{m}{4}s^{m-4}y^2 + \dots \\ y^{\frac{p-1}{2}} &= ms^{m-1} + \binom{m}{3}s^{m-3}y + \binom{m}{5}s^{m-5}y^2 + \dots \end{aligned}$$

Desta segunda equação temos que y divide o termo ms^{m-1} , ou seja, $ms^{m-1} \equiv 0 \pmod{y}$. Como y é par e s é ímpar segue que m é par. Novamente usando a segunda equação, como s em cada somando à direita está elevado a uma potência ímpar, temos que $s \mid y^{\frac{p-1}{2}}$. Mas $y + 1 = s^2$, assim $y \equiv -1 \pmod{s}$ e elevando a $\frac{p-1}{2}$ obtemos

$$0 \equiv y^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{s},$$

mas isto implica que $s = 1$ e neste caso $y = 0$. Portanto a única solução de $x^2 = y^p + 1$ é $x = \pm 1$ e $y = 0$. \square

4.4.1 Solução Inicial da Equação de Pell

Na prova da existência de soluções da equação de Pell, não mostramos um procedimento para encontrar explicitamente uma solução, que é o que faremos nesta seção.

Para determinar uma solução da equação $x^2 - Ay^2 = 1$, vamos considerar a fração contínua de \sqrt{A} . Isso é natural, pois, se x e y são inteiros positivos tais que $x^2 - Ay^2 = \pm 1$, temos

$$\left| \frac{x}{y} - \sqrt{A} \right| \left| \frac{x}{y} + \sqrt{A} \right| = \frac{1}{y^2} |x^2 - Ay^2| = \frac{1}{y^2}.$$

Por outro lado $|\frac{x}{y} + \sqrt{A}| > 2$. De fato, $|\frac{x}{y} + \sqrt{A}| \geq 2\sqrt{A} - |\frac{x}{y} - \sqrt{A}| > 2\sqrt{A} - \frac{1}{y^2}$: Se $A \geq 3$, segue que $|\frac{x}{y} + \sqrt{A}| > 2\sqrt{A} - \frac{1}{y^2} \geq 2\sqrt{A} - 1 \geq 2\sqrt{3} - 1 > 2$, e, se $A=2$, $y \geq 2$, donde $|\frac{x}{y} + \sqrt{A}| > 2\sqrt{A} - \frac{1}{y^2} \geq 2\sqrt{A} - \frac{1}{4} = 2\sqrt{2} - \frac{1}{4} > 2$. Portanto,

$$\left| \frac{x}{y} - \sqrt{A} \right| = \frac{1}{|\frac{x}{y} + \sqrt{A}| y^2} < \frac{1}{2y^2},$$

e logo, pelo teorema 3.18, $\frac{x}{y}$ é uma reduzida $\frac{p_n}{q_n}$ da fração contínua de \sqrt{A} .

Mais precisamente, vamos considerar a fração contínua de $\sqrt{A} + \lfloor \sqrt{A} \rfloor = [a_0; a_1, a_2, \dots]$ (a qual difere da fração contínua de \sqrt{A} apenas pelo primeiro termo $a_0 = 2\lfloor \sqrt{A} \rfloor$, que na fração contínua de \sqrt{A} é igual a $\lfloor \sqrt{A} \rfloor = a_0/2$).

Vamos mostrar que existem duas seqüências de inteiros positivos b_i e c_i de modo que

$$0 < \frac{\sqrt{A} - c_i}{b_i} < 1 \quad \text{e} \quad \frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2} \dots] \quad (*)$$

para todo $i \geq 0$. Começamos definindo $b_0 = 1$ e $c_0 = \lfloor \sqrt{A} \rfloor$. Note que $0 < \sqrt{A} - \lfloor \sqrt{A} \rfloor = \frac{\sqrt{A} - c_0}{b_0} < 1$. Em geral, definimos recursivamente $c_{i+1} = a_i b_i - c_i$ e $b_{i+1} = (A - c_{i+1}^2)/b_i$.

Mostremos inicialmente por indução que b_i e c_i são inteiros com $b_i \neq 0$ e tais que $b_i \mid A - c_i^2$ para todo i . Isto é claramente verdade para $i = 0$. Por hipótese de indução, temos que b_i e c_i são inteiros, logo $c_{i+1} = a_i b_i - c_i$ também será inteiro e $A - c_{i+1}^2 \neq 0$ já que A não é quadrado perfeito. Além disso,

$$A - c_{i+1}^2 = A - (a_i b_i - c_i)^2 = A - c_i^2 - b_i(a_i^2 b_i - 2a_i c_i)$$

será múltiplo de b_i já que $b_i \mid A - c_i^2$ por hipótese de indução. Assim $b_{i+1} = (A - c_{i+1}^2)/b_i$ será um inteiro não nulo tal que $b_{i+1} \mid A - c_{i+1}^2$.

Desta forma, temos

$$\frac{\sqrt{A} + c_i}{b_i} = a_i + \frac{\sqrt{A} - c_{i+1}}{b_i} = a_i + \frac{b_{i+1}}{\sqrt{A} + c_{i+1}} = a_i + \frac{1}{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}}}.$$

de modo que (*) será válida para todo i . Vamos provar agora que b_i e c_i são positivos. Para isto, vamos provar por indução que $b_i > 0$ e $0 < c_i < \sqrt{A}$, o que é verdadeiro para $i = 0$ pois $c_0 = \lfloor \sqrt{A} \rfloor$ e A não é quadrado perfeito. Além disso, pela definição de a_i temos

$$a_i < \frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2} \dots] < a_i + 1$$

donde obtemos $a_i b_i < \sqrt{A} + c_i < a_i b_i + b_i$ (já que $b_i > 0$ por hipótese de indução) e portanto

$$c_{i+1} = a_i b_i - c_i < \sqrt{A} < a_i b_i - c_i + b_i = c_{i+1} + b_i$$

e assim $c_{i+1} < \sqrt{A}$, o que implica $b_{i+1} = (A - c_{i+1}^2)/b_i > 0$ também. Agora suponha por absurdo que $c_{i+1} \leq 0$. Neste caso teríamos $b_i > \sqrt{A} - c_{i+1} \geq \sqrt{A}$, mas como $\sqrt{A} > c_i$ por hipótese de indução, teríamos $b_i > c_i$, donde $c_{i+1} = a_i b_i - c_i \geq b_i - c_i > 0$, o que é uma contradição. Portanto $c_{i+1} > 0$, completando a indução.

Finalmente, temos

$$\begin{aligned} \frac{\sqrt{A} - c_{i+1}}{b_{i+1}} &= \frac{\sqrt{A} - c_{i+1}}{(A - c_{i+1}^2)/b_i} = \frac{b_i}{\sqrt{A} + c_{i+1}} = \\ &= \frac{b_i}{\sqrt{A} + a_i b_i - c_i} = \frac{1}{a_i + (\sqrt{A} - c_i)/b_i} \in (0, 1), \end{aligned}$$

pois $a_i \geq 1$ e $(\sqrt{A} - c_i)/b_i > 0$.

Como $0 < c_i < \sqrt{A}$ e $b_i \mid A - c_i^2$, temos que as sequências $\{c_i\}$ e $\{b_i\}$ só assumem um número finito de valores. Além disso, podemos recuperar os valores de b_i e c_i a partir dos de b_{i+1} e c_{i+1} , para todo $i \geq 0$. De fato, $b_i = (A - c_{i+1}^2)/b_{i+1}$. Além disso, como $0 < \frac{\sqrt{A} - c_i}{b_i} < 1$, temos

$$a_i = \lfloor a_i + \frac{\sqrt{A} - c_i}{b_i} \rfloor = \lfloor \frac{\sqrt{A} + c_{i+1}}{b_i} \rfloor.$$

Finalmente, temos $c_i = a_i b_i - c_{i+1}$. Portanto estas sequências, assim como a fração contínua $\sqrt{A} + \lfloor \sqrt{A} \rfloor = [a_0; a_1, a_2, \dots]$, são *periódicas puras*, digamos de período k . Em particular $b_k = 1$ e $c_k = a_0$.

Note que como $a_0 = 2\lfloor \sqrt{A} \rfloor$, temos que a expansão em fração contínua de \sqrt{A} é $[a_0/2; a_1, a_2, \dots]$. Logo, para $i \geq 1$, denotando por p_i/q_i a i -ésima convergente desta fração contínua, temos

$$\sqrt{A} = \frac{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}} p_i + p_{i-1}}{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}} q_i + q_{i-1}},$$

e portanto

$$Aq_i + c_{i+1}\sqrt{A}q_i + \sqrt{A}b_{i+1}q_{i-1} = \sqrt{A}p_i + c_{i+1}p_i + b_{i+1}p_{i-1}.$$

Separando parte racional da parte irracional obtemos as equações

$$Aq_i = c_{i+1}p_i + b_{i+1}p_{i-1} \quad \text{e} \quad p_i = c_{i+1}q_i + b_{i+1}q_{i-1}.$$

Isolando c_{i+1} nas equações anteriores e igualando obtemos

$$\begin{aligned} \frac{Aq_i - b_{i+1}p_{i-1}}{p_i} &= \frac{p_i - b_{i+1}q_{i-1}}{q_i} \\ \iff Aq_i^2 - b_{i+1}p_{i-1}q_i &= p_i^2 - b_{i+1}q_{i-1}p_i \\ \iff p_i^2 - Aq_i^2 &= b_{i+1}(p_iq_{i-1} - p_{i-1}q_i) \\ \iff p_i^2 - Aq_i^2 &= (-1)^{i+1}b_{i+1} \end{aligned}$$

donde obtemos uma solução da equação $x^2 - Ay^2 = (-1)^{i+1}b_{i+1}$. Se k é o período teremos que $b_k = 1$ e portanto a equação $x^2 - Ay^2 = -1$ tem solução se k é ímpar, enquanto que $x^2 - Ay^2 = 1$ sempre tem solução (tomando $i + 1 = 2k$).

Por outro lado, se x e y são inteiros positivos tais que $x^2 - Ay^2 = \pm 1$, vimos que $\frac{x}{y}$ é uma reduzida $\frac{p_n}{q_n}$ da fração contínua de \sqrt{A} . Como $p_n^2 - Aq_n^2 = (-1)^{n+1}b_{n+1}$, segue que $b_{n+1} = 1$, mas, como $0 < \sqrt{A} - c_{n+1} = \frac{\sqrt{A} - c_{n+1}}{b_{n+1}} < 1$, segue que $c_{n+1} = \lfloor \sqrt{A} \rfloor$, donde $[a_{n+1}; a_{n+2}, a_{n+3} \dots] = \frac{\sqrt{A} + c_{n+1}}{b_{n+1}} = \sqrt{A} + \lfloor \sqrt{A} \rfloor$, e portanto $n+1$ é necessariamente múltiplo de período k .

Por exemplo, se queremos encontrar uma solução da equação $x^2 - 21y^2 = 1$, como

$$4 + \sqrt{21} = [\overline{8; 1, 1, 2, 1, 1}] \quad \text{e} \quad \sqrt{21} = [4; \overline{1, 1, 2, 1, 1, 8}]$$

onde a barra denota o período, temos que

$$\frac{p_5}{q_5} = 4 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}}} = \frac{55}{12}$$

$$\text{e } 55^2 - 21 \times 12^2 = 3025 - 3024 = 1.$$

4.4.2 A Equação $x^2 - Ay^2 = -1$

Suponha, como sempre, que A não é quadrado perfeito. Na seção anterior mostramos que a equação de Pell sempre possui solução. Em contrapartida, a equação $x^2 - Ay^2 = -1$ nem sempre possui solução, de fato se p é um divisor primo de A temos que $x^2 - Ay^2 \equiv x^2 \equiv -1 \pmod{p}$, assim uma condição necessária para a existência de solução é que todo divisor primo de A seja 2 ou da forma $4k+1$. Porém, esta condição ainda não é suficiente. O seguinte teorema dá uma relação entre as soluções fundamentais da equações $x^2 - Ay^2 = 1$ e $x^2 - Ay^2 = -1$ (como antes, a solução fundamental de $x^2 - Ay^2 = -1$, quando esta equação tem solução inteira, é o menor número da forma $a + b\sqrt{A}$ com a e b inteiros positivos tais que $a^2 - Ab^2 = -1$).

Proposição 4.29. *Suponha que a equação $x^2 - Ay^2 = -1$ admita solução inteira e seja $a + b\sqrt{A}$ sua solução fundamental. Seja $c + d\sqrt{A}$ a solução fundamental da equação $x^2 - Ay^2 = 1$. Então*

$$(a + b\sqrt{A})^2 = c + d\sqrt{A}, \quad a^2 = \frac{c-1}{2}.$$

DEMONSTRAÇÃO: Observemos que $(a + b\sqrt{A})^2$ é solução da equação $x^2 - Ay^2 = 1$. Suponhamos por contradição que não é a solução fundamental, isto é suponhamos que

$$(a + b\sqrt{A})^2 > c + d\sqrt{A} > 1$$

Como $(a + b\sqrt{A})(a - b\sqrt{A}) = -1 < 0$ temos que $1 > -a + b\sqrt{A} > 0$, de fato $-a + b\sqrt{A}$ é a maior solução positiva que tem x negativo e y positivo. Multiplicando a desigualdade anterior por $-a + b\sqrt{A}$, obtemos

$$\begin{aligned} (a + b\sqrt{A}) &> (c + d\sqrt{A})(-a + b\sqrt{A}) = (-ac + bdA) + (cb - ad)\sqrt{A} \\ &> -a + b\sqrt{A} > 0. \end{aligned}$$

Temos que $(-ac + bdA, cb - ad)$ é solução de $x^2 - Ay^2 = -1$. Observemos que $-ac + bdA, cb - ad$ não podem ser simultaneamente positivos, porque isto contradiz a escolha da solução fundamental. Também não podemos ter que $-ac + bdA < 0, cb - ad > 0$ porque $-a + b\sqrt{A}$ é a maior solução positiva de $x^2 - Ay^2 = -1$ com x negativo e y positivo. Por último, no caso $-ac + bdA > 0, cb - ad < 0$, isto é, $bdA > ac, ad > cb$, multiplicando a primeira desigualdade por d e a segunda por c obtemos $bd^2A > acd > c^2b$, assim $0 > b(c^2 - Ad^2) = b$, o que também é contraditório. Assim concluímos que $(a + b\sqrt{A})^2 = c + d\sqrt{A}$. Como $a^2 - Ab^2 = -1$, somando as igualdades temos $c - 1 = 2a^2$ logo $a^2 = (c - 1)/2$. \square

Vejamos agora que a condição sobre os fatores primos de A não é suficiente para garantir a existência de solução. Por exemplo, $x^2 - 34y^2 = -1$ não possui solução inteira. De fato, a solução fundamental de $x^2 - 34y^2 = 1$ é $35 + 6\sqrt{34}$, mas $\frac{35-1}{2} = 17$ não é quadrado, logo, pelo teorema anterior, $x^2 - 34y^2 = -1$ não possui soluções.

No caso em que A é um primo da forma $4k + 1$, a equação $x^2 - Ay^2 = -1$ sempre possui solução. Mais geralmente, temos o seguinte resultado, devido a Dirichlet.

Proposição 4.30 (Dirichlet). *Seja A produto de no máximo três primos distintos da forma $4k + 1$ tais que $\left(\frac{p}{q}\right) = -1$ para todo $p \neq q$ divisores primos de A . Então a equação $x^2 - Ay^2 = -1$ possui solução.*

DEMONSTRAÇÃO: Seja $x_0 + \sqrt{A}y_0$ a solução fundamental de $x^2 - Ay^2 = 1$. Como

$$1 = x_0^2 - Ay_0^2 \equiv x_0^2 - y_0^2 \pmod{4},$$

então x_0 é ímpar e y_0 é par. Além disso, do fato de que $(x_0 - 1)(x_0 + 1) = Ay_0^2$ e $x_0 + 1$ e $x_0 - 1$ só tem fator comum 2, segue que existem inteiros s e t primos relativos e inteiros a, b com $A = ab$ tais que

$$y_0 = 2st, \quad x_0 - 1 = 2as^2 \quad \text{e} \quad x_0 + 1 = 2bt^2$$

e assim $as^2 - bt^2 = -1$. Basta portanto mostrar que $a = 1$ (de modo que $b = A$). Para isto, observemos que $a \neq A$ porque caso contrário $b = 1$ e (t, s) seria uma solução menor do que a solução mínima (x_0, y_0) de $x^2 - Ay^2 = 1$. Por outro lado, se $1 < a < A$ temos dois possíveis casos:

1. a é primo, neste caso tomamos um divisor primo p de b e temos que $as^2 \equiv -1 \pmod{p}$. Logo $\left(\frac{-a}{p}\right) = 1$, mas p é da forma $4k + 1$ e portanto isto implica $\left(\frac{a}{p}\right) = 1$, o que contradiz a hipótese do teorema.
2. a é produto de dois primos e b é primo, neste caso se p é um divisor primo de a temos que $bt^2 \equiv 1 \pmod{p}$, assim $\left(\frac{b}{p}\right) = 1$, o que de novo contradiz a hipótese do teorema.

□

O resultado anterior foi generalizado por Richaud, Tano e outros. O seguinte teorema contém essencialmente todos estes resultados.

Teorema 4.31 (Nagell-Trotter). *Sejam p_1, \dots, p_n números primos distintos congruentes a 1 módulo 4 e $A = p_1 p_2 \dots p_n$.*

- Se n é ímpar e não existem índices diferentes i, j, k tais que $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_k}\right) = 1$, então $x^2 - Ay^2 = -1$ possui solução.
- Se n é par, $\left(\frac{p_1}{p_2}\right) = -1$, $\left(\frac{p_1}{p_j}\right) = 1, \forall j > 2$ e não existem índices diferentes $i, j, k \geq 2$ tais que $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_k}\right) = 1$, então $x^2 - Ay^2 = -1$ possui solução.
- Se $\left(\frac{p_1}{p_j}\right) = -1, \forall j \geq 2$, e não existem índices diferentes $i, j, k \geq 2$ tais que $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_k}\right) = -1$, então $x^2 - Ay^2 = -1$ possui solução.

DEMONSTRAÇÃO: Ver [147] ou [111].

□

4.4.3 Soluções da Equação $x^2 - Ay^2 = c$

Novamente assumimos que A não é quadrado perfeito. Seja $(x_1, y_1) \in (\mathbb{N}_{>0})^2$ a solução mínima de $x^2 - Ay^2 = 1$. Dado $c \in \mathbb{Z}$ não nulo, se existe alguma solução de $x^2 - Ay^2 = c$ com $(x, y) \in \mathbb{N}^2$, então existem infinitas: de fato, se $u + v\sqrt{A} = (x + y\sqrt{A})(x_1 + y_1\sqrt{A})^n$ com $n \in \mathbb{Z}$, então $u^2 - Av^2 = c$.

Por outro lado, nem sempre existe uma tal solução. Uma condição necessária para a existência de soluções é a seguinte: se p é um divisor primo de A , temos $x^2 \equiv c \pmod{p}$, assim para que exista solução c deve ser resíduo quadrático módulo p para todo divisor primo p de A . Infelizmente esta condição não é suficiente, por exemplo a equação $x^2 - 7y^2 = 11$ não possui solução já que olhando módulo 4

$$x^2 + y^2 \equiv x^2 - 7y^2 = 11 \equiv -1 \pmod{4},$$

o que é impossível. Entretanto $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1$.

As seguintes proposições ajudam a reduzir o trabalho necessário para decidir se $x^2 - Ay^2 = c$ tem alguma solução $(x, y) \in \mathbb{N}^2$.

Proposição 4.32. *Seja $\alpha = x_1 + y_1\sqrt{A} > 1$ onde (x_1, y_1) é a solução mínima de $x^2 - Ay^2 = 1$. Dado $c \in \mathbb{N}$ não nulo, se existem $x, y \in \mathbb{N}$ com $x^2 - Ay^2 = c$, então existem $r \in \mathbb{N}$ e $u, v \in \mathbb{N}$ com $u + v\sqrt{A} < \alpha\sqrt{|c|}$ e $u^2 - Av^2 = c$ tais que $x + y\sqrt{A} = (u + v\sqrt{A})\alpha^r$.*

DEMONSTRAÇÃO: Se $x + y\sqrt{A} < \alpha\sqrt{|c|}$, podemos tomar $(u, v) = (x, y)$ e $r = 0$. Suponhamos então que $x + y\sqrt{A} \geq \alpha\sqrt{|c|}$. Seja $\beta = x + y\sqrt{A} > 0$ com $N(\beta) = x^2 - Ay^2 = c$. Então $N(\beta \cdot \alpha^k) = c$ para todo $k \in \mathbb{Z}$. Podemos escolher um $k \in \mathbb{Z}$ tal que $\sqrt{|c|} \leq \beta \cdot \alpha^k < \alpha\sqrt{|c|}$. Definimos $\gamma = \beta \cdot \alpha^k$. Temos que $\gamma = u + v\sqrt{A}$ com $u, v \in \mathbb{Z}$ e logo $x + y\sqrt{A} = \beta = \gamma\alpha^r = (u + v\sqrt{A})\alpha^r$, com $r = -k$. Como $x + y\sqrt{A} \geq \alpha\sqrt{|c|} \geq u + v\sqrt{A}$, segue que $r \geq 0$, donde $r \in \mathbb{N}$.

Finalmente, vamos verificar que u, v são naturais: temos $c = N(\gamma) = u^2 - Av^2 = (u + v\sqrt{A})(u - v\sqrt{A})$, donde

$$|u - v\sqrt{A}| = \frac{|c|}{u + v\sqrt{A}} \leq \frac{|c|}{\sqrt{|c|}} = \sqrt{|c|} \leq u + v\sqrt{A}.$$

Temos assim $u - v\sqrt{A} \leq u + v\sqrt{A}$, donde $v \geq 0$ e simultaneamente $-u + v\sqrt{A} \leq u + v\sqrt{A}$, e logo $u \geq 0$. \square

Proposição 4.33. *Seja $\alpha = x_1 + y_1\sqrt{A} > 1$ onde (x_1, y_1) é a solução mínima de $x^2 - Ay^2 = 1$. Dado $c \in \mathbb{Z}$ não nulo, se existem $x, y \in \mathbb{N}$ com $x^2 - Ay^2 = c$, então existem $u, v \in \mathbb{N}$ com $u + v\sqrt{A} \leq \sqrt{\alpha|c|}$ e $u^2 - Av^2 = c$ (em particular, para esta solução $0 \leq u \leq \sqrt{\alpha|c|}$ e $0 \leq v \leq \sqrt{\alpha|c|/A}$).*

Além disso, dados $x, y \in \mathbb{N}$ com $x^2 - Ay^2 = c$, existem $r \in \mathbb{N}$ e $u, v \in \mathbb{N}$ com $u + v\sqrt{A} \leq \sqrt{\alpha|c|}$ e $u^2 - Av^2 = c$ tais que $x + y\sqrt{A} = (u + v\sqrt{A})\alpha^r$ ou $x + y\sqrt{A} = |u - v\sqrt{A}| \alpha^{r+1}$.

DEMONSTRAÇÃO: Se $x + y\sqrt{A} < \sqrt{\alpha|c|}$, podemos tomar $(u, v) = (x, y)$ e $r = 0$. Suponhamos então que $x + y\sqrt{A} \geq \sqrt{\alpha|c|}$.

Se $\gamma = r + s\sqrt{A}$ com $r, s \in \mathbb{Q}$ lembramos que $\hat{\gamma} = r - s\sqrt{A}$, e $N(\gamma) = N(\hat{\gamma}) = \gamma \cdot \hat{\gamma} = r^2 - As^2$.

Seja $\beta = x + y\sqrt{A} > 0$ com $N(\beta) = x^2 - Ay^2 = c$. Então $N(\beta \cdot \alpha^k) = c$ para todo $k \in \mathbb{Z}$. Podemos escolher um $k \in \mathbb{Z}$ tal que $\sqrt{|c|} \leq \beta \cdot \alpha^k < \alpha\sqrt{|c|}$. No caso que $\sqrt{|c|} \leq \beta \cdot \alpha^k \leq \sqrt{\alpha|c|}$ definimos $\gamma = \beta \cdot \alpha^k$ e no caso que $\sqrt{\alpha|c|} < \beta \cdot \alpha^k \leq \alpha\sqrt{|c|}$, podemos definir $\gamma = \alpha \cdot |c|/(\beta \cdot \alpha^k) = |\hat{\beta}| \alpha^{1-k}$; assim $N(\gamma) = N(\beta) = N(\hat{\beta}) = c$ e $\sqrt{|c|} < \gamma \leq \sqrt{\alpha|c|}$. Logo, sem perda de generalidade, podemos supor que $\sqrt{|c|} \leq \gamma \leq \sqrt{\alpha|c|}$. No primeiro caso temos $\beta = \gamma\alpha^r = (u + v\sqrt{A})\alpha^r$, com $r = -k \in \mathbb{Z}$, e, como $\beta = x + y\sqrt{A} \geq \sqrt{\alpha|c|} \geq \gamma$, temos $r \in \mathbb{N}$. No segundo caso, temos $\beta = |\beta| = |\hat{\gamma}| \alpha^{r+1} = |u - v\sqrt{A}| \alpha^{r+1}$, com $r = k - 2 \in \mathbb{Z}$, e, como $\beta = x + y\sqrt{A} \geq \sqrt{\alpha|c|} > \sqrt{|c|} \geq |c|/\gamma = |\hat{\gamma}|$, temos $r + 1 > 0$, donde $r \in \mathbb{N}$.

Temos que $\gamma = u + v\sqrt{A}$ com $u, v \in \mathbb{Z}$. Ainda precisamos verificar que u, v são naturais, mas

$$c = N(\gamma) = u^2 - Av^2 = (u + v\sqrt{A})(u - v\sqrt{A}).$$

Temos então

$$|u - v\sqrt{A}| = \frac{|c|}{u + v\sqrt{A}} \leq \frac{|c|}{\sqrt{|c|}} = \sqrt{|c|} \leq u + v\sqrt{A}.$$

Temos assim $u - v\sqrt{A} \leq u + v\sqrt{A}$, donde $v \geq 0$ e simultaneamente $-u + v\sqrt{A} \leq u + v\sqrt{A}$, e logo $u \geq 0$. \square

Exemplo 4.34. *Determine se a equação $x^2 - 10y^2 = 39$ possui solução.*

SOLUÇÃO: A equação $x^2 - 10y^2 = 1$ possui como solução fundamental $19 + 6\sqrt{10}$. Como $\sqrt{39(19 + 6\sqrt{10})} < 39$ e $\sqrt{\frac{39(19+6\sqrt{10})}{10}} < 13$, pela proposição anterior, e do fato que $x^2 > 39$, temos que uma possível solução satisfaz $7 \leq x \leq 39$ com x ímpar e $y \leq 12$, assim só precisamos testar 12 valores para y . De fato com $y = 1$, obtemos $x = 7$, e portanto a equação possui solução. \square

Exemplo 4.35. *Mostre que a equação $x^2 - 10y^2 = 11$ não possui solução inteira.*

SOLUÇÃO: Pelo mesmo processo anterior temos que

$$\sqrt{11(19 + 6\sqrt{10})} < 21 \quad \text{e} \quad \sqrt{\frac{11(19 + 6\sqrt{10})}{10}} < 7.$$

Considerando a equação módulo 4 obtemos $x^2 + 2y^2 \equiv 3 \pmod{4}$, mas esta relação somente é possível quando x e y são ímpares, portanto, se a equação tem solução, uma das soluções deve satisfazer $4 \leq x \leq 20$, $y \leq 6$ com x e y ímpares, assim só precisamos testar $y = 1, 3, 5$. Como nenhum dos números $11 + 10 = 21$, $11 + 90 = 101$ e $11 + 250 = 261$ é um quadrado perfeito, concluímos que a equação não possui soluções inteiras. \square

4.4.4 Soluções da Equação $mx^2 - ny^2 = \pm 1$

Suponha que mn não seja quadrado perfeito. Vejamos que se $mx_0^2 - ny_0^2 = \pm 1$ possui uma solução (x_0, y_0) então possui infinitas soluções. Temos

$$(\sqrt{m}x_0 + \sqrt{n}y_0)(\sqrt{m}x_0 - \sqrt{n}y_0) = \pm 1.$$

Como mn não é um quadrado perfeito, a equação de Pell $X^2 - mnY^2 = 1$ possui infinitas soluções; se (z, w) é uma delas, temos

$$(z + \sqrt{mn}w)(z - \sqrt{mn}w) = 1.$$

Multiplicando estas duas equações obtemos

$$(\sqrt{m}x_0 + \sqrt{n}y_0)(z + \sqrt{mn}w)(z - \sqrt{mn}w)(\sqrt{m}x_0 - \sqrt{n}y_0) = \pm 1,$$

que é equivalente a

$$\begin{aligned} & (\sqrt{m}(zx_0 + ny_0w) + \sqrt{n}(y_0z + mx_0w)) \\ & \times (\sqrt{m}(zx_0 + ny_0w) - \sqrt{n}(y_0z + mx_0w)) = \pm 1 \end{aligned}$$

portanto $x' = zx_0 + ny_0w$ e $y' = y_0z + mx_0w$ geram uma nova solução da equação $mx'^2 - ny'^2 = \pm 1$.

Reciprocamente, para toda solução (a, b) de $mx^2 - ny^2 = \pm 1$,

$$\begin{aligned} 1 &= (ma^2 - nb^2)^2 = (\sqrt{ma} + \sqrt{nb})^2(\sqrt{ma} - \sqrt{nb})^2 \\ &= (ma^2 + nb^2 + 2\sqrt{mnab})(ma^2 + nb^2 - 2\sqrt{mnab}) \\ &= (2ma^2 \mp 1)^2 - mn(2ab)^2. \end{aligned}$$

Assim $(2ma^2 \mp 1, 2ab)$ é solução da equação $x^2 - mny^2 = 1$. Por outra parte, fixando $A = mn$, o seguinte resultado mostra que nem para todo valor de m e n a equação $mx^2 - ny^2 = 1$ possui solução.

Teorema 4.36. *Seja $A \in \mathbb{Z}$ livre de quadrados e (x_1, y_1) a solução fundamental de $x^2 - Ay^2 = 1$.*

- *Se A é par, então x_1 é ímpar, e existe um único par de inteiros positivos (m, n) , com $A = mn$ e $(m, n) \neq (1, A)$, tal que a equação $mx^2 - ny^2 = 1$ possui solução. Além disso, a equação $m'x^2 - n'y^2 = 2$, com m', n' inteiros positivos tais que $A = m'n'$ possui solução apenas para $(m', n') = (2, A/2)$ e para $(m', n') = (m/2, 2n)$, caso m seja par ou $(m', n') = (2m, n/2)$, caso m seja ímpar (o que implica n par).*
- *Se A e x_1 são ímpares, então existe um único par de inteiros positivos (m, n) , com $A = mn$ e $(m, n) \neq (1, A)$, tal que a equação $mx^2 - ny^2 = 1$ possui solução. Além disso, a equação $m'x^2 - n'y^2 = 2$, com m', n' inteiros positivos tais que $A = m'n'$ não possui solução.*
- *Se A é ímpar e x_1 é par, então não existe nenhum par de inteiros positivos (m, n) , com $A = mn$ e $(m, n) \neq (1, A)$, tal que a equação*

$mx^2 - ny^2 = 1$ possui solução, mas existe um único par de inteiros positivos (m, n) , com $A = mn$, tal que a equação $mx^2 - ny^2 = 2$ possui solução.

DEMONSTRAÇÃO: Como (x_1, y_1) solução fundamental de $x^2 - Ay^2 = 1$, temos então $(x_1 - 1)(x_1 + 1) = x_1^2 - 1 = Ay_1^2$. Observemos que $\text{mdc}(x_1 - 1, x_1 + 1) = \text{mdc}(x_1 - 1, 2) = d$, onde $d = 1$ (se x_1 é par) ou $d = 2$ (se x_1 é ímpar). Segue que $\frac{x_1 - 1}{d}$ e $\frac{x_1 + 1}{d}$ são primos relativos, e $d^2 \mid Ay_1^2$. Mas A é livre de quadrados, donde concluímos que $d \mid y_1$.

Definamos $m = \text{mdc}(\frac{x_1 + 1}{d}, A)$ e $n = \text{mdc}(\frac{x_1 - 1}{d}, A)$, e assim m e n satisfazem $A = mn$ e

$$\frac{x_1 + 1}{dm} \frac{x_1 - 1}{dn} = \left(\frac{y_1}{d}\right)^2,$$

logo existem s, t primos relativos tais que $y_1 = dst$ e

$$\frac{x_1 + 1}{d} = ms^2 \quad \text{e} \quad \frac{x_1 - 1}{d} = nt^2,$$

donde subtraindo as equações obtemos $\frac{2}{d} = ms^2 - nt^2$, o que garante a existência de m e n como no enunciado. Além disso, no caso em que $d = 2$ (que equivale a termos x_1 ímpar), temos $\frac{2}{d} = 1$, e o par (m, n) é diferente de $(1, A)$ já que $t < y_1$ e (x_1, y_1) é a solução fundamental de $x^2 - Ay^2 = 1$.

Na outra direção, suponhamos que existam (m', n') e (a, b) tais que $A = m'n'$ e $m'a^2 - n'b^2 = e$ com $e = 1$ ou $e = 2$.

Vamos considerar inicialmente o caso em que $e = 1$. O par $(2m'a^2 - 1, 2ab)$ é solução de $x^2 - Ay^2 = 1$, isto é,

$$(\sqrt{m'}a + \sqrt{n'}b)^2 = (2m'a^2 - 1) + 2ab\sqrt{A} = (x_1 + y_1\sqrt{A})^k = x_k + y_k\sqrt{A}$$

para algum inteiro $k \in \mathbb{N}$. Se k é par, vemos que $\sqrt{m'}a + \sqrt{n'}b = x_{k/2} + y_{k/2}\sqrt{A}$, e a única possibilidade é $m' = 1$ e $n' = A$. No caso k ímpar, temos (como consequência da recorrência $x_{r+2} = 2x_1x_{r+1} - x_r, \forall r \geq 0$) $x_1 \equiv x_k = 2m'a^2 - 1 \equiv 1 \pmod{2}$. Além disso, do fato que

$$x_k = \sum_{j=0}^{(k-1)/2} \binom{k}{2j} x_1^{k-2j} A^j y_1^{2j} \equiv x_1^k \pmod{A}$$

temos que

$$\begin{aligned} m \mid \text{mdc}(x_1 + 1, A) \mid \text{mdc}(x_1^k + 1, A) &= \text{mdc}(x_k + 1, A) \\ &= \text{mdc}(2a^2m', A) \mid 2m' \end{aligned}$$

e

$$\begin{aligned} n \mid \text{mdc}(x_1 - 1, A) \mid \text{mdc}(x_1^k - 1, A) &= \text{mdc}(x_k - 1, A) \\ &= \text{mdc}(2b^2n', A) \mid 2n', \end{aligned}$$

onde as últimas afirmações seguem do fato de que $m'(a^2m') - Ab^2 = m'$ e $Aa^2 - n'(n'b^2) = n'$.

Quando A é ímpar, m e n são ímpares, donde $m \mid m'$, e $n \mid n'$, e como $A = mn \mid m'n' = A$ devemos ter $m = m'$ e $n = n'$.

No caso $e = 2$ temos que $(m'a^2 - 1, ab)$ é solução de $x^2 - Ay^2 = 1$. De fato, se $m'n' = A$ e $m'a^2 - n'b^2 = 2$, temos

$$\begin{aligned} m'a^2 - 1 + ab\sqrt{A} &= (a\sqrt{m'} + b\sqrt{n'})^2/2 \\ &= (x_1 + y_1\sqrt{A})^k = x_k + y_k\sqrt{A}, \end{aligned}$$

para algum $k \in \mathbb{N}$. Se k é par, vemos que $\sqrt{m'}a + \sqrt{n'}b = x_{k/2}\sqrt{2} + y_{k/2}\sqrt{2A}$, e a única possibilidade é $m' = 2$ e $n' = A/2$ (e logo A é par). No caso k ímpar, temos, como antes, $m \mid \text{mdc}(x_k + 1, A) = \text{mdc}(m'a^2, A) \mid 2m'$ e $n \mid \text{mdc}(x_k - 1, A) \mid \text{mdc}(n'b^2, A) \mid 2n'$.

Se $e = 2$ e $A = m'n'$ é ímpar, temos m' e n' ímpares, e, como $m'a^2 - n'b^2 = 2$, temos a e b ímpares, pois, caso contrário, como eles têm a mesma paridade, seriam ambos pares, e teríamos $4 \mid 2$, absurdo. Assim, nesse caso, $x_1 \equiv x_k = m'a^2 - 1 \equiv 0 \pmod{2}$.

Se $m'a^2 - n'b^2 = 2$ e $\tilde{m}a^2 - \tilde{n}b^2 = 2$ com m' e \tilde{m} distintos de 2 e $m'n' = \tilde{m}\tilde{n} = A$, temos

$$m'a^2 - 1 + ab\sqrt{A} = (a\sqrt{m'} + b\sqrt{n'})^2/2 = (x_1 + y_1\sqrt{A})^k$$

e

$$\tilde{m}a^2 - 1 + ab\sqrt{A} = (a\sqrt{\tilde{m}} + b\sqrt{\tilde{n}})^2/2 = (x_1 + y_1\sqrt{A})^r,$$

com k e r ímpares. Assim, teremos $a\sqrt{\tilde{m}} + b\sqrt{\tilde{n}} = (a\sqrt{m'} + b\sqrt{n'})(x_1 + y_1\sqrt{A})^t$, onde $t = \frac{r-k}{2} \in \mathbb{Z}$, e portanto $\tilde{m} = m'$ e $\tilde{n} = n'$.

No caso em que A é par (e portanto x_1 é ímpar), os argumentos acima mostram que $m \mid 2m'$ e $n \mid 2n'$. Nesse caso, as soluções de $mx^2 - ny^2 = 1$ e $mx^2 - ny^2 = 2$ estão relacionadas da seguinte forma:

- se $mx^2 - ny^2 = 1$ e m é par, então $(m/2)(2x)^2 - 2ny^2 = 2$, e, se n é par, então $2mx^2 - (n/2)(2y)^2 = 2$;
- se $mx^2 - ny^2 = 2$ e m é par, então $(m/2)x^2 - 2n(y/2)^2 = 1$, e, se n é par, então $2m(x/2)^2 - (n/2)y^2 = 2$.

□

Corolário 4.37. *Dados inteiros positivos livres de quadrados m e n com $\text{mdc}(m, n) = 1$ e $m \neq 1$, a equação $mx^2 - ny^2 = 1$ possui uma solução se, e só se, dada a solução fundamental (x_1, y_1) de $x^2 - mny^2 = 1$, o sistema de equações*

$$\begin{aligned} 2mx^2 - 1 &= x_1 \\ 2xy &= y_1 \end{aligned}$$

tem solução inteira.

DEMONSTRAÇÃO: Vimos acima que, se a equação possui solução, x_1 deve ser ímpar e existem s, t primos relativos tais que $y_1 = 2st$ e $\frac{x_1+1}{2} = ms^2$, o que prova que o sistema do enunciado tem a solução inteira $(x, y) = (s, t)$. Reciprocamente, como $x_1^2 - 1 = Ay_1^2$, de $2mx^2 - 1 = x_1$ segue que $x_1 + 1 = 2mx^2$, donde $x_1 - 1 = \frac{x_1^2 - 1}{x_1 + 1} = 2\frac{A}{m}(\frac{y_1}{2x})^2 = 2n(\frac{y_1}{2x})^2 = 2ny^2$, e logo $mx^2 - ny^2 = \frac{1}{2}((x_1 + 1) - (x_1 - 1)) = 1$. □

Exemplo 4.38 (OIbM1989). *Demonstrar que existe uma infinidade de pares (x, y) de números naturais tais que*

$$2x^2 - 3x - 3y^2 - y + 1 = 0.$$

SOLUÇÃO: Completando quadrados e fatorando temos que a equação original é equivalente a

$$3(4x - 3)^2 - 2(6y + 1)^2 = 1.$$

Substituindo $z = 4x - 3$ e $w = 6y + 1$, o problema inicial se transforma em encontrar infinitas soluções da equação

$$3z^2 - 2w^2 = 1 \quad \text{com} \quad z \equiv 1 \pmod{4} \quad \text{e} \quad w \equiv 1 \pmod{6}.$$

Para isto, consideremos a equação de Pell auxiliar $s^2 - 6t^2 = 1$, que possui solução mínima $(5, 2)$, assim todas as soluções positivas são dadas por

$$s_n + \sqrt{6}t_n = (5 + 2\sqrt{6})^n = (5 + 2\sqrt{6})(s_{n-1} + \sqrt{6}t_{n-1}),$$

ou seja,

$$s_n = 5s_{n-1} + 12t_{n-1} \quad \text{e} \quad t_n = 2s_{n-1} + 5t_{n-1}.$$

A partir de uma solução de $s^2 - 6t^2 = 1$ obtemos uma solução de $3z^2 - 2w^2 = 1$ da seguinte forma

$$\sqrt{3}z_n + \sqrt{2}w_n = (\sqrt{3} + \sqrt{2})(s_n + \sqrt{6}t_n),$$

ou seja,

$$z_n = s_n + 2t_n \quad \text{e} \quad w_n = s_n + 3t_n.$$

Assim, só nos falta mostrar que existem infinitos pares (z_n, w_n) tais que $z_n \equiv 1 \pmod{4}$ e $w_n \equiv 1 \pmod{6}$. Vamos provar por indução que para todo n par

$$s_n \equiv 1 \pmod{12} \quad \text{e} \quad t_n \equiv 0 \pmod{2}$$

donde concluiremos que, para todo n par,

$$z_n \equiv 1 \pmod{4} \quad \text{e} \quad w_n \equiv 1 \pmod{6}$$

Temos que $s_2 = 49$ e $t_2 = 20$ cumprem as condições pedidas. Agora se $n \geq 2$ é par temos, por hipótese de indução,

$$s_{n+2} \equiv 5s_{n+1} \equiv 5^2s_n \equiv s_n \pmod{12}$$

$$t_{n+2} \equiv 5t_{n+1} \equiv 5^2t_n \equiv t_n \pmod{2}$$

o que encerra a prova. □

Problemas Propostos

4.32. Demonstrar que $\lfloor (1 + \sqrt{3})^{2n-1} \rfloor$ é divisível por 2^n .

4.33. Encontrar todos os triângulos retângulos com lados inteiros tais que a diferença entre os catetos é 1.

4.34. *Demonstrar que a equação $7x^2 - 13y^2 = 1$ não tem soluções inteiras.*

4.35. *Seja p um primo. Demonstrar que a equação $x(x+1) = p^2y(y+1)$ não tem soluções inteiras positivas. A equação pode ter soluções inteiras?*

4.36. *Demonstrar que $2x^2 - 219y^2 = -1$ não tem soluções inteiras, mas $2x^2 - 219y^2 \equiv -1 \pmod{m}$ tem soluções para todo inteiro positivo m .*

Dica: Considere a “nova solução” $x_1 = |293x - 3066y|$, $y_1 = -28x + 293y$.

4.37. *(OBM2010) Encontre todos os pares (a, b) de inteiros positivos tais que*

$$3^a = 2b^2 + 1.$$

Capítulo 5

Funções Aritméticas

Neste capítulo estudaremos o comportamento assintótico de algumas das mais importantes funções aritméticas, muitas delas já introduzidas em capítulos anteriores. Frequentemente resultados mais precisos sobre o crescimento dessas funções dependem de estimativas precisas sobre números primos, algumas das quais desenvolveremos neste capítulo, que é fortemente inspirado nos capítulos XVIII e XXII de [67].

Notação: dadas duas funções $f: \mathbb{N} \rightarrow \mathbb{R}$ e $g: \mathbb{N} \rightarrow (0, +\infty)$, escrevemos

$$f = o(g) \text{ se } \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0 \text{ e}$$

$$f = O(g) \text{ se existe } C > 0 \text{ com } |f(n)| < Cg(n) \text{ para } n \gg 0.$$

Em todo o livro, a menos que se afirme o contrário, \log denota o logaritmo natural. Neste capítulo, divisor de um número natural significará divisor positivo.

5.1 Funções Multiplicativas

Uma função f definida sobre $\mathbb{N}_{>0}$ é dita *multiplicativa* se dados dois números naturais a e b tais que $\text{mdc}(a, b) = 1$ então $f(ab) = f(a)f(b)$, e *totalmente multiplicativa* se $f(ab) = f(a)f(b)$ para todo a e b . Vejamos algumas funções multiplicativas importantes.

Proposição 5.1. *Seja n um número inteiro positivo e k um real qualquer. As funções*

$$\sigma_k(n) \stackrel{\text{def}}{=} \sum_{d|n} d^k \quad e \quad \varphi(n) = \text{função } \varphi \text{ de Euler}$$

são multiplicativas. Em particular, as funções

$$\begin{aligned} d(n) &\stackrel{\text{def}}{=} \sigma_0(n) = \text{número de divisores de } n \\ \sigma(n) &\stackrel{\text{def}}{=} \sigma_1(n) = \text{soma dos divisores de } n \end{aligned}$$

são multiplicativas.

DEMONSTRAÇÃO: Já vimos na seção 1.7 que φ é multiplicativa. Por outro lado, pela proposição 1.21, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ é a fatoração canônica de n em primos então temos uma fórmula explícita

$$\sigma_k(n) = \frac{p_1^{(\alpha_1+1)k} - 1}{p_1^k - 1} \cdot \dots \cdot \frac{p_m^{(\alpha_m+1)k} - 1}{p_m^k - 1},$$

donde é fácil provar que σ_k é multiplicativa. □

Uma função totalmente multiplicativa f fica completamente determinada por seus valores nos números primos. Impondo algumas restrições adicionais, temos o seguinte resultado

Teorema 5.2. *Seja $f: \mathbb{N}_{>0} \rightarrow \mathbb{R}_{>0}$ uma função totalmente multiplicativa e monótona, então existe $\alpha \in \mathbb{R}$ tal que $f(n) = n^\alpha$.*

DEMONSTRAÇÃO: Trocando f por $1/f$, podemos supor sem perda de generalidade que f é crescente, e definamos $\alpha = \log_2 f(2)$. Vejamos que $f(n) = n^\alpha$. Para isto observemos que, aplicando f , para todo $m \in \mathbb{N}_{>0}$ temos

$$\begin{aligned} 2^{\lfloor m \log_2 n \rfloor} &\leq n^m < 2^{\lfloor m \log_2 n \rfloor + 1} \\ \implies 2^{\alpha \lfloor m \log_2 n \rfloor} &\leq (f(n))^m \leq 2^{\alpha (\lfloor m \log_2 n \rfloor + 1)} \end{aligned}$$

Assim,

$$2^{\frac{\alpha \lfloor m \log_2 n \rfloor}{m}} \leq f(n) \leq 2^{\frac{\alpha (\lfloor m \log_2 n \rfloor + 1)}{m}} \quad \text{para todo } m \in \mathbb{N}_{>0}.$$

Mas

$$\lim_{m \rightarrow \infty} \frac{\alpha \lfloor m \log_2 n \rfloor}{m} = \lim_{m \rightarrow \infty} \frac{\alpha (\lfloor m \log_2 n \rfloor + 1)}{m} = \alpha \log_2 n,$$

donde concluimos que $f(n) = 2^{\alpha \log_2 n} = n^\alpha$. □

Para uma extensão desse resultado para funções multiplicativas, veja o exercício 5.19.

Exemplo 5.3. *Encontrar condições necessárias e suficientes sobre m e n para que $n\varphi(m) = m\varphi(n)$.*

SOLUÇÃO: Se $n\varphi(m) = m\varphi(n)$ então

$$n\varphi(m) = mn \prod_{\substack{p|m \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right) = mn \prod_{\substack{q|n \\ q \text{ primo}}} \left(1 - \frac{1}{q}\right) = m\varphi(n).$$

Daí temos que n e m devem ter os mesmos divisores primos; caso contrário, consideremos $\{p_i\}$ e $\{q_j\}$ os fatores primos de n e m respectivamente que não são comuns aos dois números, então

$$\prod (p_i - 1) \prod q_j = \prod (q_j - 1) \prod p_i.$$

Mas, como $p_i \nmid q_j$ e $q_j \nmid p_i$ para todos os fatores primos, concluimos que

$$\prod p_i \mid \prod (p_i - 1) \quad \text{e} \quad \prod q_j \mid \prod (q_j - 1),$$

o que é impossível. Agora, se n e m tem os mesmos fatores primos prova-se diretamente da fórmula acima que $n\varphi(m) = m\varphi(n)$. □

O seguinte teorema nos mostra uma forma de construir funções multiplicativas.

Teorema 5.4. *Se f é uma função multiplicativa então a função*

$$F(n) = \sum_{d|n} f(d)$$

é também multiplicativa.

DEMONSTRAÇÃO: Sejam a e b inteiros tais que $\text{mdc}(a, b) = 1$ então

$$\begin{aligned} F(ab) &= \sum_{d|ab} f(d) = \sum_{d_1|a, d_2|b} f(d_1 d_2) = \sum_{d_1|a, d_2|b} f(d_1) f(d_2) \\ &= \sum_{d_1|a} \sum_{d_2|b} f(d_1) f(d_2) = \sum_{d_1|a} f(d_1) \sum_{d_2|b} f(d_2) \\ &= F(a)F(b). \end{aligned}$$

Segue que F também é multiplicativa. \square

Com o resultado anterior obtemos outro método para demonstrar que $\sigma_k(n)$ é multiplicativa, já que $f(n) = n^k$ é claramente uma função multiplicativa.

Exemplo 5.5. *Demonstrar que $\varphi(n)d(n) \geq n$.*

SOLUÇÃO: Se $\alpha \geq \beta \geq 0$ então para qualquer primo p temos $\varphi(p^\alpha) \geq \varphi(p^\beta)$, logo como φ é multiplicativa temos que $\varphi(n) \geq \varphi(d)$ para todo divisor d de n . Então, pelo lema 1.77,

$$\varphi(n)d(n) = \sum_{d|n} \varphi(n) \geq \sum_{d|n} \varphi(d) = n,$$

como queríamos demonstrar. Note que a igualdade só se obtém quando $n = 1$ ou $n = 2$. \square

Exemplo 5.6. *Encontrar todos os inteiros n para os quais $\varphi(n) = d(n)$.*

SOLUÇÃO: Se $p \geq 3$ é um primo, temos que

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1} \geq 2(1+2)^{\alpha-1} \geq 2(1+2(\alpha-1)) \geq \alpha+1 = d(p^\alpha),$$

onde a igualdade só se dá quando $p = 3$ e $\alpha = 1$. Portanto, pela multiplicatividade das funções $\varphi(n)$ e $d(n)$, os únicos ímpares que satisfazem $\varphi(n) = d(n)$ são $n = 1$ e $n = 3$. Por outro lado, se $\alpha > 3$ temos $\varphi(2^\alpha) = 2^{\alpha-1} > \alpha+1 = d(2^\alpha)$; para $\alpha = 3$ obtemos as soluções $n = 1 \cdot 8 = 8$ e $n = 3 \cdot 8 = 24$.

Assim, só nos falta resolver os casos $\varphi(2n) = d(2n) \iff \varphi(n) = 2d(n)$ e $\varphi(4n) = d(4n) \iff 2\varphi(n) = 3d(n)$ onde n é ímpar. Temos

$\varphi(5) = 4 = 2d(5)$, $\varphi(15) = 8 = 2d(15)$ e $\varphi(9) = 6 = 2d(9)$, donde $2 \cdot 5 = 10$, $2 \cdot 9 = 18$ e $2 \cdot 15 = 30$ também são soluções da equação inicial. Demonstremos agora que não existem mais soluções. Se $n = p^\alpha$ é potência de um primo ímpar p então para $p = 3$ e $\alpha \geq 3$, ou para $p = 5$ e $\alpha \geq 2$, ou para $p \geq 7$, temos como acima que

$$\varphi(n) = p^{\alpha-1}(p-1) > 2\alpha + 2 = 2d(n) > \frac{3}{2}d(n).$$

Por outro lado, já sabemos que $\varphi(n) \geq d(n)$ para todo n ímpar. Assim, da multiplicatividade das funções $\varphi(n)$ e $d(n)$, obtemos que se n é divisível por 3^3 , 5^2 ou por algum primo $p \geq 7$, então $\varphi(n) > 2d(n) > \frac{3}{2}d(n)$ e analisando os casos restantes obtemos apenas as soluções apresentadas anteriormente.

Em conclusão, as únicas soluções de $\varphi(n) = d(n)$ são 1, 3, 8, 10, 18, 24, 30. \square

O seguinte teorema relaciona a função $d(n)$ com a função $[x]$.

Teorema 5.7. *Seja n um inteiro positivo, então*

$$\sum_{k=1}^{2n} d(k) - \sum_{k=1}^n \left\lfloor \frac{2n}{k} \right\rfloor = n.$$

DEMONSTRAÇÃO: Seja

$$f(i) \stackrel{\text{def}}{=} \sum_{1 \leq k \leq i} \left\lfloor \frac{2i}{k} \right\rfloor.$$

Observemos que para $i, k > 1$

$$\left\lfloor \frac{2i}{k} \right\rfloor - \left\lfloor \frac{2i-2}{k} \right\rfloor = \begin{cases} 1 & \text{se } k \mid 2i \text{ ou } k \mid 2i-1 \\ 0 & \text{caso contrário.} \end{cases}$$

Portanto para $i \geq 2$ temos

$$\begin{aligned} f(i) - f(i-1) &= [2i] - [2i-2] + \sum_{2 \leq k \leq i} \left(\left\lfloor \frac{2i}{k} \right\rfloor - \left\lfloor \frac{2i-2}{k} \right\rfloor \right) + \left\lfloor \frac{2i-2}{i} \right\rfloor \\ &= 2 + (d(2i) - 2) + (d(2i-1) - 2) + 1 \\ &= d(2i) + d(2i-1) - 1, \end{aligned}$$

donde

$$\begin{aligned}\sum_{k=1}^{2n} d(k) &= d(2) + d(1) + \sum_{i=2}^n (f(i) - f(i-1) + 1) \\ &= 3 + f(n) - f(1) + n - 1 \\ &= f(n) + n\end{aligned}$$

que era o que queríamos demonstrar. \square

5.2 Função de Möbius e Fórmula de Inversão

Definimos a *função de Möbius* $\mu: \mathbb{N}_{>0} \rightarrow \mathbb{Z}$ por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } a^2 \mid n \text{ para algum } a > 1 \\ (-1)^k & \text{se } n \text{ é produto de } k \text{ primos distintos.} \end{cases}$$

Facilmente se comprova que a função de Möbius é multiplicativa. Além disso

Lema 5.8. *Para todo inteiro positivo n temos*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1. \end{cases}$$

DEMONSTRAÇÃO: No caso $n = 1$ não temos nada para provar. Como a função $\sum_{d|n} \mu(d)$ é multiplicativa pelo teorema 5.4, basta mostra o lema para $n = p^k$ onde p é um número primo. De fato,

$$\sum_{d|p^k} \mu(d) = \sum_{j=0}^k \mu(p^j) = 1 - 1 = 0$$

como queríamos demonstrar. \square

Teorema 5.9 (Fórmula de inversão de Möbius). *Seja $f(n)$ uma função sobre os inteiros positivos e $F(n) = \sum_{d|n} f(d)$, então para todo n inteiro positivo,*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

DEMONSTRAÇÃO: Vejamos que

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d_1|\frac{n}{d}} f(d_1) \\ &= \sum_{d|n} \sum_{d_1|\frac{n}{d}} \mu(d) f(d_1) \\ &= \sum_{d_1|n} \sum_{d|\frac{n}{d_1}} \mu(d) f(d_1) \\ &= \sum_{d_1|n} f(d_1) \sum_{d|\frac{n}{d_1}} \mu(d) = f(n) \mu(1) = f(n), \end{aligned}$$

como queríamos demonstrar. \square

Agora, observemos que para todo número natural m , f e F definidas como antes,

$$\sum_{n=1}^m F(n) = \sum_{n=1}^m \sum_{d|n} f(d) = \sum_{d=1}^m \sum_{\substack{d|n \\ 1 \leq n \leq m}} f(d)$$

Como $f(d)$ é somado $\left\lfloor \frac{m}{d} \right\rfloor$ vezes, então

$$\sum_{n=1}^m F(n) = \sum_{d=1}^m f(d) \left\lfloor \frac{m}{d} \right\rfloor.$$

No caso particular em que $f(n) = \varphi(n)$ temos que $F(n) = n$ pelo lema 1.77 e assim

$$\frac{m(m+1)}{2} = \sum_{n=1}^m \varphi(n) \left\lfloor \frac{m}{n} \right\rfloor.$$

Se $f(n) = \mu(n)$, então $F(n) = 0$ se $n > 1$ e $F(1) = 1$ pelo lema 5.8, portanto

$$1 = \sum_{n=1}^m \mu(n) \left\lfloor \frac{m}{n} \right\rfloor.$$

A igualdade anterior nos permite resolver o seguinte

Exemplo 5.10. *Demonstrar que, para todo inteiro $m > 1$,*

$$\left| \sum_{k=1}^m \frac{\mu(k)}{k} \right| < 1.$$

SOLUÇÃO: Como $-1 < \mu(k) \left(\left\lfloor \frac{m}{k} \right\rfloor - \frac{m}{k} \right) < 1$ e $\left\lfloor \frac{m}{k} \right\rfloor - \frac{m}{k} = 0$ quando $k = 1, m$, então

$$\left| \sum_{k=1}^m \mu(k) \left\lfloor \frac{m}{k} \right\rfloor - m \sum_{k=1}^m \frac{\mu(k)}{k} \right| < m - 1$$

Usando a identidade acima provada temos que

$$\left| 1 - m \sum_{k=1}^m \frac{\mu(k)}{k} \right| < m - 1,$$

logo $\left| m \sum_{k=1}^m \frac{\mu(k)}{k} \right| < m$ e simplificando m obtemos o que queríamos demonstrar. É conhecido (Mangoldt 1897) que se m tende para infinito, então a soma anterior converge para 0. \square

Teorema 5.11 (Segunda fórmula de inversão de Möbius). *Sejam f, g funções reais com domínio $(0, +\infty)$ tais que*

$$g(x) = \sum_{k=1}^{\infty} f\left(\frac{x}{k}\right)$$

para todo x , então

$$f(x) = \sum_{k=1}^{\infty} \mu(k) g\left(\frac{x}{k}\right).$$

DEMONSTRAÇÃO: Observemos que

$$f(x) = \sum_{k=1}^{\infty} \mu(k) \left(\sum_{r=1}^{\infty} f\left(\frac{x}{kr}\right) \right) = \sum_{m=1}^{\infty} \left(\sum_{k|m} \mu(k) \right) f\left(\frac{x}{m}\right) = f(x),$$

como queríamos demonstrar. \square

A seguinte é uma das formulações da famosa hipótese de Riemann, um dos problemas em aberto mais importantes da Matemática. O Clay Mathematics Institute oferece um prêmio de 1 milhão de dólares para a primeira demonstração da Hipótese de Riemann (ver a página web <http://www.claymath.org/millennium/>).

Conjetura 5.12 (Hipótese de Riemann). *Se $\alpha > 1/2$, então*

$$\lim_{n \rightarrow \infty} \frac{1}{n^\alpha} \sum_{m=1}^n \mu(m) = 0.$$

Podemos reenunciar esta conjectura assim: seja $f: (0, +\infty) \rightarrow \mathbb{R}$ definida por

$$\begin{cases} f(t) = 0 & \text{se } t < 1 \\ \sum_{k=1}^{\infty} f(t/k) = 1 & \text{se } t \geq 1. \end{cases}$$

Então, para todo $\alpha > 1/2$,

$$\lim_{t \rightarrow \infty} \frac{f(t)}{t^\alpha} = 0.$$

De fato, pela segunda fórmula de inversão de Möbius, temos

$$f(t) = \sum_{m=1}^{\lfloor t \rfloor} \mu(m).$$

Problemas Propostos

5.1. *Encontrar todos os inteiros positivos n tais que*

$$n = d_6^2 + d_7^2 - 1,$$

onde $1 = d_1 < d_2 < \dots < d_k = n$ são todos os divisores positivos do número n .

5.2. *Seja r o número de fatores primos diferentes de n , demonstrar que*

$$\sum_{d|n} |\mu(d)| = 2^r.$$

5.3. *Seja n um inteiro positivo que não é primo e tal que $\varphi(n) \mid n - 1$. Demonstrar que n possui ao menos quatro fatores primos distintos.*

5.4. *Dados dois números reais α e β tais que $0 \leq \alpha < \beta \leq 1$, demonstrar que existe um número natural m tal que*

$$\alpha < \frac{\varphi(m)}{m} < \beta.$$

5.5. *Seja m um inteiro positivo. Dizemos que um inteiro $m \geq 1$ é “superabundante” se*

$$\forall k \in \{1, 2, \dots, m-1\} \quad \frac{\sigma(m)}{m} > \frac{\sigma(k)}{k}.$$

Demonstrar que existe um número infinito de números superabundantes.

5.6. *Demonstrar que $d(n) < 2\sqrt{n}$. Poderia melhorar esta cota?*

5.7. *Demonstrar que*

$$\frac{\sigma(n)}{d(n)} \geq \sqrt{n}.$$

5.8. *Encontrar todos os valores de n para os quais $\varphi(n) \mid n$.*

5.9. *Dois números a e b são amigos se $\sigma(a) = b$ e $\sigma(b) = a$. Por exemplo 1184 e 1210 são amigos (verificar!). Encontrar outra dupla de números amigos.*

5.10. *Demonstrar que $m \mid \sigma(mn - 1)$ para todo n se, e só se, $m = 2, 3, 4, 6, 8, 12$ ou 24 .*

5.11. *Demonstrar que*

$$\frac{\sigma(n!)}{n!} > 1 + \frac{1}{2} + \dots + \frac{1}{n}.$$

5.12. *Demonstrar que existem infinitos números naturais n para os quais $\sigma(x) = n$ não tem solução.*

5.13. *Demonstrar que para todo $m > 1$*

$$\left| \sum_{k=1}^m \frac{\mu(k)}{k} \right| < \frac{2}{3}.$$

5.14 (IMO1998). *Para cada inteiro positivo n , $d(n)$ denota o número de divisores de n . Determine todos os inteiros positivos k tais que $d(n^2) = kd(n)$ para algum n .*

5.15. *Se n é composto, mostre que $\varphi(n) \leq n - \sqrt{n}$.*

5.16. *Determinar todos os números inteiros positivos n tais que $n = d(n)^2$.*

5.17. *Uma pulseira é formada por pedras coloridas, de mesmo tamanho, pregadas em volta de um círculo de modo a ficarem igualmente espaçadas. Duas pulseiras são consideradas iguais se, e somente se, suas configurações de pedras coincidem por uma rotação. Se há pedras disponíveis de $k \geq 1$ cores distintas, mostre que o número de pulseiras diferentes possíveis com n pedras é dado pela expressão*

$$\frac{1}{n} \sum_{d|n} \varphi(d) \cdot k^{n/d}.$$

5.18. *Seja f uma função multiplicativa tal que para todo número primo p ,*

$$f(p^k) = \begin{cases} 1 & \text{se } k = 2^s \text{ para algum } s \in \mathbb{N} \\ 0 & \text{caso contrário.} \end{cases}$$

Mostre que f é uma função tal que $f(n^2) = f(n)^2$ para todo $n \in \mathbb{N}$, mas não é totalmente multiplicativa.

5.19. *Seja $f : \mathbb{N}^+ \rightarrow \mathbb{R}^+$ uma função multiplicativa e crescente.*

(a) Prove que, para todo inteiro $M > 1$ e todo inteiro positivo n ,

$$f(M^{n+1} - 1) \geq f(M^n - 1)f(M) \text{ e } f(M^{n+1} + 1) \leq f(M^n + 1)f(M).$$

Conclua que

$$\lim_{n \rightarrow \infty} \sqrt[n]{f(M^n)} = f(M).$$

- (b) Utilize o item anterior para M potência de primo para concluir que $f(p^k) = f(p)^k$ para todo primo p .
- (c) Conclua que f é totalmente multiplicativa, e portanto existe $\alpha > 0$ tal que $f(n) = n^\alpha$ para todo inteiro positivo n .

5.20. Mostrar que $\varphi(n) + \sigma(n) \geq 2n$ para todo inteiro positivo n .

5.21. Dadas duas funções $f, g : \mathbb{N}_{>0} \rightarrow \mathbb{C}$, definimos o produto de Dirichlet (ou convolução de Dirichlet) $f * g : \mathbb{N}_{>0} \rightarrow \mathbb{C}$ de f e g por

$$f * g(n) \stackrel{\text{def}}{=} \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1)g(d_2).$$

- (a) Prove que, se $s \in \mathbb{R}$ (ou $s \in \mathbb{C}$) e as séries $\sum_{n \geq 1} \frac{f(n)}{n^s}$ e $\sum_{n \geq 1} \frac{g(n)}{n^s}$ convergem absolutamente então

$$\sum_{n \geq 1} \frac{f(n)}{n^s} \cdot \sum_{n \geq 1} \frac{g(n)}{n^s} = \sum_{n \geq 1} \frac{f * g(n)}{n^s}.$$

- (b) Prove que, para quaisquer funções $f, g, h : \mathbb{N}_{>0} \rightarrow \mathbb{C}$, temos $f * g = g * f$ e $f * (g * h) = (f * g) * h$ (isto é, o produto de Dirichlet é comutativo e associativo), e que a função $I : \mathbb{N}_{>0} \rightarrow \mathbb{C}$ dada por $I(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}$ é o elemento neutro do produto $*$, i.e., $I * f = f * I = f$, $\forall f : \mathbb{N}_{>0} \rightarrow \mathbb{C}$.

- (c) Prove que se f e g são multiplicativas então $f * g$ é multiplicativa.

- (d) Prove que, se $f : \mathbb{N}_{>0} \rightarrow \mathbb{C}$ é tal que $f(1) \neq 0$, então existe uma única função $f^{(-1)} : \mathbb{N}_{>0} \rightarrow \mathbb{C}$ tal que $f * f^{(-1)} = f^{(-1)} * f = I$, a qual é dada recursivamente por $f^{(-1)}(1) = 1/f(1)$ e, para $n > 1$,

$$f^{(-1)}(n) = -\frac{1}{f(1)} \sum_{d|n, d < n} f\left(\frac{n}{d}\right) f^{(-1)}(d).$$

- (e) Prove que, se f é multiplicativa, então a função $f^{(-1)}$ definida no item anterior também é multiplicativa.

5.3 Algumas Estimativas sobre Primos

Para estudar o comportamento assintótico das funções aritméticas da seção anterior, precisaremos de algumas estimativas sobre o crescimento dos primos.

5.3.1 O Teorema de Chebyshev

Começamos com um

Lema 5.13. *Sejam n um número natural e p um número primo. Seja θ_p o inteiro tal que $p^{\theta_p} \leq 2n < p^{\theta_p+1}$. Então o expoente da maior potência de p que divide $\binom{2n}{n}$ é menor ou igual a θ_p . Em particular, se $p > \sqrt{2n}$ então o expoente desta máxima potência de p é menor do que ou igual a 1. Além disso, se $\frac{2}{3}n < p < n$ então p não divide $\binom{2n}{n}$.*

DEMONSTRAÇÃO: Sejam α e β os expoentes das maiores potências de p que dividem $(2n)!$ e $n!$ respectivamente. Sabemos da proposição 1.22 que

$$\alpha = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \cdots \quad \text{e} \quad \beta = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots.$$

Portanto o expoente da máxima potência de p que divide $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é

$$\alpha - 2\beta = \sum_{i=1}^{\theta_p} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Mas como

$$\frac{2n}{p^i} \geq \left\lfloor \frac{2n}{p^i} \right\rfloor > \frac{2n}{p^i} - 1 \quad \text{e} \quad -2 \left(\frac{n}{p^i} - 1 \right) > -2 \left\lfloor \frac{n}{p^i} \right\rfloor \geq -2 \frac{n}{p^i},$$

somando teremos que

$$2 > \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor > -1.$$

Portanto esta última expressão só pode tomar os valores 1 e 0. Concluímos que

$$\alpha - 2\beta \leq \sum_{i=1}^{\theta_p} 1 = \theta_p.$$

Além disso, se $\frac{2n}{3} < p < n$ então $\alpha = 2$ e $\beta = 1$, logo $\alpha - 2\beta = 0$. □

Corolário 5.14. *Para todo inteiro positivo n , o mínimo múltiplo comum dos números $1, 2, \dots, 2n$ é maior ou igual a $\binom{2n}{n}$.*

Podemos agora mostrar a seguinte

Proposição 5.15 (Chebyshev). *Seja $\pi(x)$ a quantidade de primos menores do que ou iguais a x . Existem constantes positivas $c < C$ tais que*

$$c \frac{x}{\log x} < \pi(x) < C \frac{x}{\log x}$$

para todo $x \geq 2$.

DEMONSTRAÇÃO: Observemos inicialmente que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é múltiplo de todos os primos p que satisfazem $n < p \leq 2n$. Como

$$\binom{2n}{n} < \sum_{0 \leq k \leq 2n} \binom{2n}{k} = 2^{2n},$$

segue que o produto dos primos entre n e $2n$ é menor do que 2^{2n} . Como há $\pi(2n) - \pi(n)$ primos como esses segue que $n^{\pi(2n) - \pi(n)} < 2^{2n}$ (pois todos esses primos são maiores que n), donde $(\pi(2n) - \pi(n)) \log n < 2n \log 2$ e

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}.$$

Isso implica facilmente, por indução, que

$$\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k}$$

(começando com $k = 5$; até $k = 5$ segue de $\pi(n) \leq n/2$ para $n \geq 4$). Daí segue que se $2^k < x \leq 2^{k+1}$ então

$$\pi(x) \leq \frac{5 \cdot 2^k}{k} \leq \frac{5x \log 2}{\log x}$$

pois $f(x) = x \log 2 / \log x$ é uma função crescente para $x \geq 3$.

Vamos agora provar a outra desigualdade. Se $\binom{2n}{n} = \prod_{p < 2n} p^{\alpha_p}$ é a fatoração canônica de $\binom{2n}{n}$ então pelo lema 5.13 temos $p^{\alpha_p} \leq 2n \iff \alpha_p \log p \leq \log 2n$ e portanto

$$\log \binom{2n}{n} = \sum_{p < 2n} \alpha_p \log p \leq \pi(2n) \log(2n),$$

donde

$$\pi(2n) \geq \frac{\log \binom{2n}{n}}{\log(2n)} \geq \frac{n \log 2}{\log(2n)}$$

pois

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} \geq 2^n,$$

assim,

$$\pi(x) \geq \frac{x \log 2}{2 \log x}$$

para todo x par, o que implica na mesma estimativa para todo x inteiro, pois $\pi(2k-1) = \pi(2k)$. \square

Corolário 5.16. *Seja p_n o n -ésimo número primo. Existem constantes $C' > c' > 0$ tais que*

$$c' n \log n < p_n < C' n \log n$$

para todo $n \geq 2$.

DEMONSTRAÇÃO: Se $\limsup_{n \rightarrow \infty} \frac{p_n}{n \log n} > C'$, então

$$\begin{aligned} \liminf_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} &\leq \liminf_{n \rightarrow \infty} \frac{\pi(p_n)}{p_n/\log p_n} \\ &\leq \liminf_{n \rightarrow \infty} \frac{n(\log C' + \log n + \log \log n)}{C' n \log n} = \frac{1}{C'} \end{aligned}$$

já que $x/\log x$ é crescente para $x \geq 3$. Assim, como $\liminf_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} > 0$ pelo teorema anterior, temos que existe C' tal que $p_n < C' n \log n$ para todo $n \geq 2$. Analogamente se prova a existência de c' . \square

Temos ainda o seguinte corolário do teorema de Chebyshev, que deixamos como exercício para o leitor.

Corolário 5.17. *Seja $f: \mathbb{N} \rightarrow [0, +\infty)$ uma função decrescente. A série*

$$\sum_{p \text{ primo}} f(p)$$

converge se, e somente se, a série

$$\sum_{n=2}^{\infty} \frac{f(n)}{\log n}$$

converge. Em particular,

$$\sum_{p \text{ primo}} \frac{1}{p} = +\infty.$$

Observação 5.18. Um interessante argumento devido a Erdős dá uma outra prova da divergência da série dos inversos dos primos: supondo que $\sum_{p \text{ primo}} \frac{1}{p} < +\infty$, existe $N \in \mathbb{N}$ tal que

$$\sum_{\substack{p \text{ primo} \\ p \geq N}} \frac{1}{p} < \frac{1}{2}.$$

Vamos considerar a decomposição $\mathbb{N} = A \cup B$ em que

$A = \{n \in \mathbb{N} \mid \text{todos os fatores primos de } n \text{ são menores que } N\}$ e $B = \mathbb{N} \setminus A$. Sejam p_1, p_2, \dots, p_k todos os primos menores que N . Fixemos $M \in \mathbb{N}$. Se $n \in A$ e $n \leq M$, então n se fatora como $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, onde $\alpha_j \leq \frac{\log M}{\log p_j}$, $\forall j \leq k$. Assim, $|A \cap [1, M]| \leq (1 + \frac{\log M}{\log 2})^k$. Por outro lado, todo elemento de B tem um fator primo maior ou igual a N , donde

$$|B \cap [1, M]| \leq \sum_{\substack{p \text{ primo} \\ p \geq N}} \left\lfloor \frac{M}{p} \right\rfloor \leq M \sum_{\substack{p \text{ primo} \\ p \geq N}} \frac{1}{p} < \frac{M}{2}.$$

Como $M = |\mathbb{N} \cap [1, M]| = |A \cap [1, M]| + |B \cap [1, M]| < (1 + \frac{\log M}{\log 2})^k + \frac{M}{2}$, temos $\frac{M}{2} < (1 + \frac{\log M}{\log 2})^k$ para todo $M \in \mathbb{N}$, o que é absurdo, pois

$$\lim_{M \rightarrow +\infty} \frac{1}{M} \left(1 + \frac{\log M}{\log 2}\right)^k = 0.$$

□

5.3.2 O Postulado de Bertrand

Sabemos que há sequências arbitrariamente grandes de números consecutivos que não contém primos, por exemplo

$$k! + 2, k! + 3, k! + 4, \dots, k! + k$$

Nosso próximo resultado é o seguinte teorema, também devido a Chebyshev, que afirma que os primos não são tão “esparços” assim. Ele é chamado de “postulado” por razões históricas.

Teorema 5.19 (Postulado de Bertrand). *Seja n um inteiro positivo. Então sempre existe um primo p tal que $n \leq p \leq 2n$.*

Lema 5.20. *Para todo $n \geq 2$, temos*

$$\prod_{\substack{p \leq n \\ p \text{ primo}}} p < 4^n.$$

DEMONSTRAÇÃO: A prova é por indução em n . Para isso, vemos que para n pequeno tal desigualdade é válida. Além disso, se o resultado vale para $n = 2m + 1$ então também vale para $n = 2m + 2$ pois não agregamos novos primos ao produto quando passamos de $2m + 1$ para $2m + 2$. Logo basta provar a desigualdade para um valor ímpar $n = 2m + 1$.

Dado que para todo primo p tal que $m + 1 < p \leq 2m + 1$ tem-se que p divide $(2m + 1)!$ mas não divide $(m + 1)!$ nem $m!$ então

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m+1} = \binom{2m}{m+1} + \binom{2m}{m} < (1+1)^{2m} = 4^m.$$

Portanto da hipótese de indução temos que

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \prod_{m+1 < p \leq 2m+1} p < 4^{m+1} 4^m = 4^{2m+1},$$

como queríamos demonstrar. □

DEMONSTRAÇÃO: (DO POSTULADO DE BERTRAND) Suponhamos que esta afirmação é falsa para algum valor de n e mostraremos que n não pode ser muito grande.

Seja p_i o i -ésimo primo e α_i máximo tal que $p_i^{\alpha_i} \mid \binom{2n}{n}$. Como estamos supondo que não há primos entre n e $2n$ e como nenhum primo entre $\frac{2}{3}n$ e n divide $\binom{2n}{n}$ pelo lema 5.13, temos $\binom{2n}{n} = \prod_{p_i \leq \frac{2n}{3}} p_i^{\alpha_i}$. Ainda pelo lema 5.13, $p_i^{\alpha_i} \leq 2n$ e $\alpha_j \leq 1$ para $p_j > \sqrt{2n}$, logo

$$\binom{2n}{n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{\alpha_i} \prod_{\sqrt{2n} < p_j \leq \frac{2n}{3}} p_j \leq \prod_{p_i \leq \sqrt{2n}} 2n \prod_{p_j \leq \frac{2n}{3}} p_j.$$

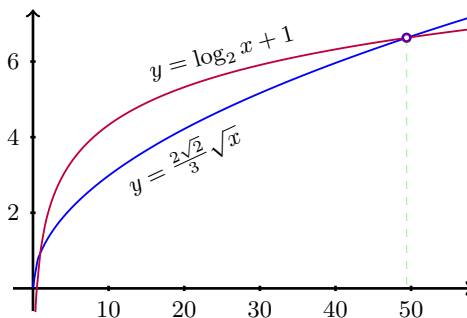
Utilizando o lema anterior, e supondo que n é suficientemente grande de modo que o número de primos entre 1 e $\sqrt{2n}$ é menor que $\sqrt{n/2} - 1$ ($n = 100$ é suficiente e a partir deste valor esta hipótese se cumpre já que metade dos números neste intervalo são pares), temos

$$\binom{2n}{n} < (2n)^{\sqrt{n/2}-1} 4^{2n/3}.$$

Por outra parte, $n \binom{2n}{n} = n \binom{2n-1}{n} + n \binom{2n-1}{n-1} > (1+1)^{2n-1} = 2^{2n-1}$ e assim a desigualdade anterior implica

$$\frac{2^{2n-1}}{n} < (2n)^{\sqrt{n/2}-1} 4^{2n/3} \implies 2^{2n/3} < (2n)^{\sqrt{n/2}}.$$

Tomando logaritmo na base 2, obtemos a desigualdade $\frac{2\sqrt{2}}{3}\sqrt{n} < \log_2 n + 1$, que é falsa para todo $n \geq 50$.



Portanto, se existe um contra-exemplo do postulado de Bertrand, este deve ser menor do que 100. Para terminar a demonstração só falta mostrar um primo que cumpra as condições do teorema para todo inteiro menor que 100: tome

$p = 2$	para	$1 \leq n \leq 2$
$p = 5$	para	$3 \leq n \leq 5$
$p = 11$	para	$6 \leq n \leq 11$
$p = 23$	para	$12 \leq n \leq 23$
$p = 47$	para	$24 \leq n \leq 47$
$p = 79$	para	$48 \leq n \leq 79$
$p = 101$	para	$80 \leq n \leq 100$

□

Exemplo 5.21. *Seja $n > 2^k$. Demonstrar que os k primeiros números que são maiores do que n e primos relativos com $n!$ são primos.*

SOLUÇÃO: Como $n > 2^k$ então $n^2 > 2^k n$. Então entre dois termos consecutivos da sequência $n, 2n, 4n, \dots, 2^k n$ existe ao menos um primo. Portanto, entre n e n^2 existem ao menos k primos. Em particular, os k primeiros números maiores que n que são primos relativos com $n!$ estarão entre n e n^2 . Se um de tais números não fora primo, digamos $l = ab$, supondo $a \leq b$, teremos que $a^2 \leq l \leq n^2$, logo $a \leq n$, o que contradiz o fato de que $n!$ e l são primos relativos. □

5.3.3 Outras estimativas

Precisaremos também das seguintes estimativas:

Lema 5.22. 1. $\sum_{1 \leq j \leq n} \frac{1}{j} = \log n + \gamma + O\left(\frac{1}{n}\right) = \log n + O(1)$, onde

$$\gamma = \lim_{n \rightarrow \infty} \left(\left(\sum_{1 \leq j \leq n} \frac{1}{j} \right) - \log n \right) = 0,577215664901532860606512\dots$$

é a constante de Euler-Mascheroni (ver [38] por exemplo).

2. $\sum_{j=1}^n \log j = \left(n + \frac{1}{2}\right) \log n - n + O(1).$

3. $\sum_{j=2}^n \frac{1}{j \log j} = \log \log n + O(1).$

DEMONSTRAÇÃO: Para estimativa mais precisa da primeira soma, veja por exemplo [60]. Aqui provaremos apenas a segunda estimativa, que nos será suficiente na maioria das aplicações. Para isto, observemos que a função $g(x) = \frac{1}{x}$ é estritamente decrescente e côncava para cima, assim para todo inteiro $j > 1$, no intervalo $[j-1, j]$ a reta $y = \frac{1}{j}$ fica embaixo de $y = g(x)$, que por sua vez fica embaixo da reta que passa pelos pontos $(j-1, \frac{1}{j-1})$ e $(j, \frac{1}{j})$. Portanto calculando as áreas sob as curvas temos que

$$\frac{1}{j} < \int_{j-1}^j \frac{1}{x} dx < \frac{1}{2} \left(\frac{1}{j-1} + \frac{1}{j} \right),$$

Somando todas estas desigualdades desde 2 até n temos que

$$\sum_{j=2}^n \frac{1}{j} < \int_1^n \frac{1}{x} dx < \sum_{j=2}^n \frac{1}{2} \left(\frac{1}{j-1} + \frac{1}{j} \right) = \frac{1}{2} - \frac{1}{2n} + \sum_{j=2}^n \frac{1}{j}$$

e assim

$$\frac{1}{2} + \frac{1}{2n} + \log n < \sum_{j=1}^n \frac{1}{j} < 1 + \log n.$$

Para estimar o segundo somatório, observemos que a função $h(x) = \log x$ é estritamente crescente e côncava para baixo. Como antes, temos que para todo inteiro $j > 1$, no intervalo $[j-1, j]$ a reta que contém o ponto $(j, \log j)$ e tem inclinação $m_j = h'(j) = \frac{1}{j}$ fica por cima de $y = h(x)$, que por sua vez fica acima da reta que passa pelos pontos $(j-1, \log(j-1))$, $(j, \log j)$. Logo

$$\log j - \frac{1}{2j} > \int_{j-1}^j \log x dx > \frac{1}{2}(\log(j-1) + \log j).$$

Somando estas desigualdades desde 2 até n temos que

$$\begin{aligned} \sum_{j=2}^n \log j - \sum_{j=2}^n \frac{1}{2j} &> \int_1^n \log x dx \\ &> \sum_{j=2}^n \frac{1}{2}(\log(j-1) + \log j) = \sum_{j=2}^n \log j - \frac{1}{2} \log n. \end{aligned}$$

Ou seja,

$$\left(n + \frac{1}{2} \right) \log n - n + 1 > \sum_{j=1}^n \log j > n \log n - n + \frac{1}{2} + \frac{1}{2} \sum_{j=1}^n \frac{1}{j}.$$

Assim, concluímos que

$$\left(n + \frac{1}{2}\right) \log n - n + 1 > \sum_{j=1}^n \log j > \left(n + \frac{1}{2}\right) \log n - n + \frac{1}{4n} + \frac{3}{4}$$

e o resultado segue.

A terceira soma é estimada comparando-a com a integral $\int_2^n \frac{dx}{x \log x} = \log \log n - \log \log 2$, e é deixada como exercício para o leitor. \square

Agora, mostremos algumas estimativas sobre números primos.

Proposição 5.23. $\sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{\log p}{p} = \log n + O(1).$

DEMONSTRAÇÃO: Pela proposição 1.22, temos

$$n! = \prod_{\substack{p \text{ primo} \\ p \leq n}} p^{v_p} \quad \text{onde} \quad v_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Tomando logaritmos, temos $\sum_{k=1}^n \log k = \sum_{\substack{p \text{ primo} \\ p \leq n}} v_p \log p$, e como $\frac{n}{p} - 1 <$

$$\left\lfloor \frac{n}{p} \right\rfloor \leq v_p < \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1},$$

$$\sum_{\substack{p \text{ primo} \\ p \leq n}} \left(\frac{n}{p} - 1 \right) \log p \leq \sum_{k=1}^n \log k \leq \sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{n}{p-1} \log p.$$

Ou seja,

$$-\frac{1}{n} \sum_{\substack{p \text{ primo} \\ p \leq n}} \log p \leq \frac{1}{n} \sum_{k=1}^n \log k - \sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{\log p}{p} \leq \sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{\log p}{p(p-1)}.$$

Pelo teorema de Chebyshev 5.15, temos $\sum_{\substack{p \text{ primo} \\ p \leq n}} \log p \leq \pi(n) \log n = O(n).$

Por outro lado, $\sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{\log p}{p(p-1)} \leq \sum_{n \geq 1} \frac{1}{n^{3/2}} = O(1).$ O resultado segue,

pois $\frac{1}{n} \sum_{k=1}^n \log k = \log n + O(1)$ pelo lema anterior. \square

A proposição anterior nos permite estimar a ordem de crescimento da soma dos inversos dos primos.

Teorema 5.24. $\sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{1}{p} = \log \log n + O(1).$

DEMONSTRAÇÃO: Defina

$$a_k = \begin{cases} \frac{\log k}{k} & \text{se } k \text{ é primo} \\ 0 & \text{caso contrário} \end{cases} \quad \text{e} \quad S_n = \sum_{k=1}^n a_k.$$

Pela proposição anterior, temos que $S_k = \sum_{\substack{p \text{ primo} \\ p \leq k}} \frac{\log p}{p} = \log k + O(1).$

Assim, temos por “integração por partes” discreta

$$\begin{aligned} \sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{1}{p} &= \sum_{k=2}^n \frac{a_k}{\log k} = \sum_{k=2}^n \frac{S_k - S_{k-1}}{\log k} \\ &= \sum_{k=2}^n S_k \left(\frac{1}{\log k} - \frac{1}{\log(k+1)} \right) + \frac{S_n}{\log(n+1)} \\ &= \sum_{k=2}^n \log k \left(\frac{1}{\log k} - \frac{1}{\log(k+1)} \right) + O(1) \\ &= \sum_{k=2}^n \frac{\log(k+1) - \log k}{\log(k+1)} + O(1) \\ &= \sum_{k=2}^n \frac{1}{(k+1) \log(k+1)} + O(1) \end{aligned}$$

onde a última igualdade segue de

$$\begin{aligned} \frac{1}{k+1} &\leq \int_k^{k+1} \frac{dx}{x} \leq \frac{1}{k} \\ \Rightarrow \frac{1}{(k+1) \log(k+1)} &\leq \frac{\log(k+1) - \log k}{\log(k+1)} \leq \frac{1}{k \log(k+1)} \end{aligned}$$

e

$$\left| \sum_{k=2}^n \frac{1}{k \log(k+1)} - \sum_{k=2}^n \frac{1}{(k+1) \log(k+1)} \right| \leq \sum_{k=2}^n \left(\frac{1}{k} - \frac{1}{k+1} \right) = O(1),$$

O resultado segue do lema anterior, já que $\sum_{k=2}^n \frac{1}{(k+1)\log(k+1)} = \log \log n + O(1)$. \square

Observação 5.25. Não é difícil mostrar que a prova acima fornece um termo de erro do tipo $c + O(\frac{1}{\log n})$ (em lugar de $O(1)$) para uma certa constante c (a constante de Mertens), que vale aproximadamente

$$0,2614972128476427837554268386 \dots$$

Deixamos os detalhes como exercício para o leitor. É possível provar que a constante de Mertens c é igual a $\gamma + \sum_{p \text{ primo}} (\log(1 - \frac{1}{p}) + \frac{1}{p})$, onde γ é a constante de Euler-Mascheroni.

É possível obter estimativas mais precisas para o termo de erro. Landau, por exemplo, provou em [84] que é possível trocar o termo de erro $O(\frac{1}{\log n})$ por $O(\exp(-(\log n)^{1/14}))$, e Vinogradov ([149]) provou que é possível trocar o termo de erro por $O(\exp(-a(\log n)^{3/5}(\log \log n)^{-1/5}))$, para alguma constante positiva a .

Mais recentemente, Diamond e Pintz ([50]) provaram que o erro $\sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{1}{p} - \log \log n - c$ troca de sinal infinitas vezes. Mais precisamente, $n^{1/2} \log n (\sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{1}{p} - \log \log n - c)$ atinge valores positivos e negativos de módulos arbitrariamente grandes.

Um outro resultado importante, que será usado nas seções seguintes, é

Proposição 5.26. $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$

DEMONSTRAÇÃO: No plano complexo, temos

$$\operatorname{sen} z = z \prod_{k=1}^{\infty} \left(1 - \frac{z^2}{\pi^2 k^2}\right).$$

Assumindo esta fórmula, vejamos como terminar a prova. O coeficiente de z^3 neste produto é $-\sum_{k=1}^{\infty} \frac{1}{\pi^2 k^2}$, mas como

$$\operatorname{sen} z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \dots$$

concluimos que $\sum_{k=1}^{\infty} \frac{1}{\pi^2 k^2} = \frac{1}{3!}$, donde o resultado segue.

Para provar a fórmula acima, basta fazê-lo para z real, uma vez que o resultado geral segue por continuação analítica. Note que para todo $k \geq 1$, $\sin((2k+1)y)$ pode ser escrito como $P_k(\sin y)$, onde P_k é um polinômio de grau $2k+1$ (e coeficiente líder $(-4)^k$). De fato, $\sin y = \sin y$, $\sin(3y) = 3\sin y - 4\sin^3(y)$ e, para todo $k \geq 1$,

$$\begin{aligned} P_{k+1}(\sin y) + P_{k-1}(\sin y) &= \sin((2k+3)y) + \sin((2k-1)y) \\ &= \sin((2k+1)y + 2y) + \sin((2k+1)y - 2y) \\ &= 2\sin((2k+1)y) \cos(2y) \\ &= 2P_k(\sin y)(1 - 2\sin^2(y)), \end{aligned}$$

o que implica o resultado por indução, com $P_{k+1}(t) = 2(1 - 2t^2)P_k(t) - P_{k-1}(t)$. As raízes de $P_k(t)$ são os $2k+1$ números $\sin(\pi r/(2k+1))$, onde r é inteiro com $-k \leq r \leq k$. Assim, temos

$$\begin{aligned} \sin((2k+1)y) &= (-4)^k \sin y \prod_{1 \leq r \leq k} \left(\sin^2 y - \sin^2 \left(\frac{\pi r}{2k+1} \right) \right) \\ &= c_k \sin y \prod_{1 \leq r \leq k} \left(1 - \frac{\sin^2 y}{\sin^2 \left(\frac{\pi r}{2k+1} \right)} \right) \end{aligned}$$

para alguma constante c_k . Como $\lim_{y \rightarrow 0} \frac{\sin((2k+1)y)}{\sin y} = 2k+1$, temos que $c_k = 2k+1$. Fazendo agora $y = x/(2k+1)$, temos

$$\sin x = (2k+1) \sin \left(\frac{x}{2k+1} \right) \prod_{1 \leq r \leq k} \left(1 - \frac{\sin^2 \left(\frac{x}{2k+1} \right)}{\sin^2 \left(\frac{\pi r}{2k+1} \right)} \right).$$

Como $2t/\pi \leq \sin t \leq t$ para todo t entre 0 e $\pi/2$, temos, para todo x real e $1 \leq r \leq k$,

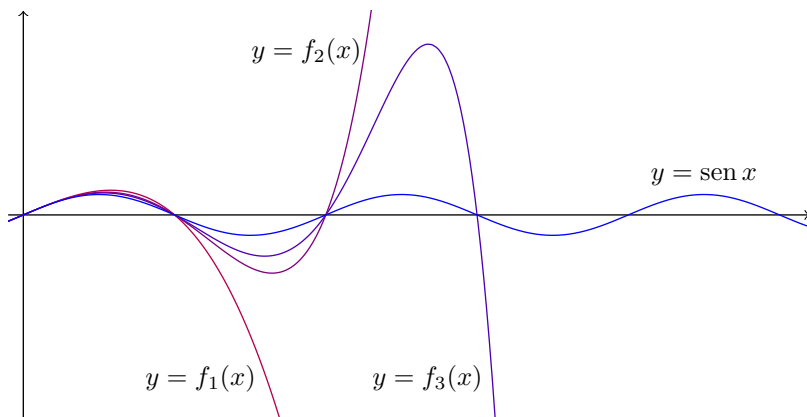
$$\frac{2r}{2k+1} \leq \sin \left(\frac{\pi r}{2k+1} \right) \leq \frac{\pi r}{2k+1} \implies 1 - \frac{x^2}{4r^2} \leq 1 - \frac{\sin^2 \left(\frac{x}{2k+1} \right)}{\sin^2 \left(\frac{\pi r}{2k+1} \right)} \leq 1.$$

Assim, o produto converge uniformemente em compactos, e podemos passar ao limite $k \rightarrow \infty$ termo a termo, obtendo a fórmula

$$\sin x = x \prod_{r \geq 1} \left(1 - \frac{x^2}{\pi^2 r^2} \right).$$

□

No seguinte desenho se ilustram os gráficos $y = f_k(x)$, dos primeiros três termos da sequência $f_k(x) := x \prod_{1 \leq r \leq k} \left(1 - \frac{x^2}{\pi^2 r^2}\right)$ que converge em compactos à função $\sin x$.



Problemas Propostos

5.22. Seja $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ a função zeta de Riemann. Mostrar usando a proposição anterior que $\zeta(4) = \frac{\pi^4}{90}$.

5.23. Mostrar indutivamente que $\frac{\zeta(2k)}{\pi^{2k}}$ é sempre racional.

5.24 (Frações egípcias). Uma fração egípcia é uma fração da forma $\frac{1}{n}$, onde n é um inteiro positivo (parece que os egípcios não gostavam de frações com numerador maior que 1). Prove que todo racional positivo pode ser escrito como soma de frações egípcias distintas.

5.25. (a) Dados inteiros $b \geq 2$ e a , com $0 \leq a \leq b-1$, seja $X_{a,b}$ o conjunto dos inteiros positivos n em cuja representação na base b o dígito a não aparece. Prove que $\sum_{n \in X_{a,b}} \frac{1}{n}$ converge.

(b) Prove que qualquer sequência finita de dígitos aparece como uma sequência de dígitos consecutivos na representação decimal de infinitos números primos.

5.4 A Função φ de Euler

As seguintes proposições mostram algumas estimativas da função φ de Euler.

Proposição 5.27. $\sum_{k=1}^n \varphi(k) = \frac{3n^2}{\pi^2} + O(n \log n)$.

DEMONSTRAÇÃO: Observemos que pela fórmula de inversão de Möbius (teorema 5.9) e o lema 1.77 temos $\varphi(k) = \sum_{d|k} \mu(d) \frac{k}{d}$, logo

$$\begin{aligned} \sum_{k=1}^n \varphi(k) &= \sum_{k=1}^n \sum_{d|k} \mu(d) \cdot \frac{k}{d} = \sum_{d=1}^n \sum_{\substack{d|k \\ 1 \leq k \leq n}} \mu(d) \cdot \frac{k}{d} \\ &= \sum_{d=1}^n \mu(d) \sum_{r=1}^{\lfloor \frac{n}{d} \rfloor} r = \sum_{d=1}^n \mu(d) \frac{\lfloor \frac{n}{d} \rfloor (\lfloor \frac{n}{d} \rfloor + 1)}{2} \end{aligned}$$

onde fizemos a substituição $r = \frac{k}{d} \leq \frac{n}{d}$. Por outro lado,

$$\left\lfloor \frac{n}{d} \right\rfloor \left(\left\lfloor \frac{n}{d} \right\rfloor + 1 \right) = \left(\frac{n}{d} \right)^2 + O\left(\frac{n}{d}\right)$$

e $\sum_{k>n} \frac{1}{k^2} = O\left(\int_n^\infty \frac{dx}{x^2}\right) = O\left(\frac{1}{n}\right)$, logo $\sum_{d>n} \frac{\mu(d)}{d^2} = O\left(\frac{1}{n}\right)$ e assim

$$\sum_{k=1}^n \varphi(k) = \frac{n^2}{2} \sum_{d=1}^n \frac{\mu(d)}{d^2} + O\left(n \sum_{d=1}^n \frac{1}{d}\right) = \frac{n^2}{2} \sum_{d=1}^\infty \frac{\mu(d)}{d^2} + O(n \log n).$$

Além disso, note que para todo $\alpha > 1$ temos que

$$\sum_{m=1}^\infty \frac{1}{m^\alpha} \sum_{n=1}^\infty \frac{\mu(n)}{n^\alpha} = \sum_{k=1}^\infty \frac{\sum_{d|k} \mu(d)}{k^\alpha} = 1.$$

Em particular $\sum_{d=1}^\infty \frac{\mu(d)}{d^2} = \left(\sum_{d=1}^\infty \frac{1}{d^2}\right)^{-1} = \frac{6}{\pi^2}$ pela proposição 5.26, assim substituindo este valor na expressão acima temos o resultado desejado. □

Observemos que a proposição anterior mostra que a “probabilidade” de que dois números naturais sejam primos entre si, ou seja,

$$\lim_{N \rightarrow \infty} \frac{1}{N^2} \#\{(m, n) \in \mathbb{N}^2 \mid 1 \leq n, m \leq N \text{ e } \text{mdc}(m, n) = 1\}$$

é igual a $\frac{6}{\pi^2} \approx 60,79\%$. Este resultado pode ser generalizado da seguinte forma:

Proposição 5.28. *Dados $k \geq 2$ um inteiro e $x \in (0, +\infty)$, sejam*

$$X = \{(m_1, m_2, \dots, m_k) \in \mathbb{N}^k \mid \text{mdc}(m_1, m_2, \dots, m_k) = 1\} \text{ e}$$

$$f(x) = \#\{(m_1, m_2, \dots, m_k) \in X \mid 1 \leq m_1, m_2, \dots, m_k \leq x\}.$$

Seja ainda ζ a função zeta de Riemann dada por $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$.

Então, para $k = 2$, $f(x) = \frac{x^2}{\zeta(2)} + O(x \log x)$ e, para $k > 2$, $f(x) = \frac{x^k}{\zeta(k)} + O(x^{k-1})$.

Em particular, $\lim_{x \rightarrow +\infty} \frac{f(x)}{x^k} = \frac{1}{\zeta(k)}$. Em outras palavras, a “probabilidade” de termos $\text{mdc}(m_1, m_2, \dots, m_k) = 1$, para $m_1, m_2, \dots, m_k \in \mathbb{N}$ é $\frac{1}{\zeta(k)}$.

DEMONSTRAÇÃO: Temos $f(x) = 0$ para todo $x \in (0, 1)$, e, para todo $x \in (0, +\infty)$, $\sum_{d \geq 1} f(x/d) = [x]^k$, pois cada um dos $[x]^k$ pontos inteiros $(m_1, m_2, \dots, m_k) \in [1, [x]]^k$ se escreve de maneira única como $d.(r_1, r_2, \dots, r_k)$, onde d (que é igual a $\text{mdc}(m_1, m_2, \dots, m_k)$) é um inteiro positivo e $\text{mdc}(r_1, r_2, \dots, r_k) = 1$, com $(r_1, r_2, \dots, r_k) \in [1, [x/d]]^k$.

Portanto, pela segunda fórmula de inversão de Möbius, temos

$$f(x) = \sum_{d \geq 1} \mu(d) [x/d]^k = \sum_{d=1}^{\lfloor x \rfloor} \mu(d) [x/d]^k.$$

Como $[x/d]^k = x^k/d^k + O(x^{k-1}/d^{k-1})$, temos

$$\begin{aligned} f(x) &= \sum_{d=1}^{\lfloor x \rfloor} \mu(d) \left(\frac{x}{d}\right)^k + O\left(\sum_{d=1}^{\lfloor x \rfloor} \frac{x^{k-1}}{d^{k-1}}\right) = \sum_{d=1}^{\lfloor x \rfloor} \mu(d) \left(\frac{x}{d}\right)^k + O\left(\sum_{d=1}^{\lfloor x \rfloor} \frac{x^{k-1}}{d^{k-1}}\right) = \\ &= x^k \sum_{d=1}^{\infty} \frac{\mu(d)}{d^k} + O\left(x^{k-1} \cdot \sum_{d=1}^{\lfloor x \rfloor} \frac{1}{d^{k-1}}\right) = \frac{x^k}{\zeta(k)} + O\left(x^{k-1} \cdot \sum_{d=1}^{\lfloor x \rfloor} \frac{1}{d^{k-1}}\right), \end{aligned}$$

o que implica o resultado desejado. \square

Proposição 5.29. $\sum_{k=1}^n \frac{\varphi(k)}{k} = \frac{6n}{\pi^2} + O(\log n).$

DEMONSTRAÇÃO: Como na proposição anterior, $\varphi(k) = \sum_{d|k} \mu(d) \frac{k}{d}$ e portanto

$$\begin{aligned} \sum_{k=1}^n \frac{\varphi(k)}{k} &= \sum_{k=1}^n \sum_{d|k} \frac{\mu(d)}{d} = \sum_{d=1}^n \left\lfloor \frac{n}{d} \right\rfloor \cdot \frac{\mu(d)}{d} \\ &= n \sum_{d=1}^n \frac{\mu(d)}{d^2} + O\left(\sum_{d=1}^n \frac{1}{d}\right) = \frac{6}{\pi^2} n + O(\log n). \end{aligned}$$

□

Proposição 5.30. $0 < \liminf_{n \rightarrow \infty} \frac{\varphi(n) \log \log n}{n} < +\infty$.

DEMONSTRAÇÃO: Seja p_i o i -ésimo número primo. Se n tem k fatores distintos, então $n > n_k$ onde $n_k = p_1 \cdot p_2 \cdots p_k$ é o produto dos k primeiros números primos. Assim,

$$\frac{\varphi(n)}{n} = \prod_{\substack{p \text{ primo} \\ p|n}} \left(1 - \frac{1}{p}\right) \geq \prod_{1 \leq i \leq k} \left(1 - \frac{1}{p_i}\right) = \frac{\varphi(n_k)}{n_k},$$

logo $\frac{\varphi(n) \log \log n}{n} \geq \frac{\varphi(n_k) \log \log n_k}{n_k}$. Basta mostrar que $\liminf_{k \rightarrow \infty} \frac{\varphi(n_k) \log \log n_k}{n_k} \in (0, \infty)$, mas

$$\log \frac{\varphi(n_k) \log \log n_k}{n_k} = \sum_{j=1}^k \log \left(1 - \frac{1}{p_j}\right) + \log \log \log n_k.$$

Como $\log\left(1 - \frac{1}{p_j}\right) = -\frac{1}{p_j} + O\left(\frac{1}{p_j^2}\right)$, pela proposição 5.24 obtemos

$$\sum_{j=1}^k \log \left(1 - \frac{1}{p_j}\right) = -\sum_{j=1}^k \frac{1}{p_j} + O(1) = -\log \log p_k + O(1).$$

Mas pelo corolário 5.16, temos que $k \leq p_k \leq Ck \log k$ para algum C , o que implica $\log \log p_k = \log \log k + O(1)$. Desta maneira, para mostrar que $\liminf_{k \rightarrow \infty} \frac{\varphi(n_k) \log \log n_k}{n_k} \in (0, \infty)$, basta verificar que

$$\limsup_{k \rightarrow \infty} (\log \log k - \log \log \log n_k) = 0.$$

Temos que $n_k = \prod_{j=1}^k p_k \leq (Ck \log k)^k$, donde

$$\log n_k \leq k(\log k + \log(C \log k)) < 2k \log k \quad \text{para } k \text{ grande,}$$

e assim $\log \log n_k < \log k + \log \log k + \log 2$. Portanto

$$\limsup_{k \rightarrow \infty} (\log \log k - \log \log \log n_k) \geq 0.$$

Por outro lado, certamente temos $n_k > 2^k$, logo $\log n_k > k \log 2$, $\log \log n_k > \log k + \log \log 2$, e assim

$$\limsup_{k \rightarrow \infty} (\log \log k - \log \log \log n_k) \leq 0.$$

Logo este \limsup é zero, completando a prova. \square

Observação 5.31. *É possível provar que $\liminf_{n \rightarrow \infty} \frac{\varphi(n) \log \log n}{n} = e^{-\gamma}$.*

Observe que outro tipo de estimativa trivial pode ser obtida do fato que $\varphi(p) = p-1$, para todo p primo, assim fica claro que $\limsup_{n \rightarrow \infty} \frac{\varphi(n)}{n} = 1$.

Resumindo os vários tipos de resultados que obtivemos sobre $\varphi(n)$ dizemos que a ordem média de $\varphi(n)$ é $\frac{6n}{\pi^2}$, a ordem máxima de $\varphi(n)$ é n e a ordem mínima de $\varphi(n)$ é $\frac{e^{-\gamma}n}{\log \log n}$.

Problemas Propostos

5.26. *Prove que se a parte real de α é maior ou igual a 2 então*

$$\sum_{m=1}^{\infty} \frac{\varphi(m)}{m^{\alpha}} = \sum_{m=1}^{\infty} \frac{1}{m^{\alpha-1}} \bigg/ \sum_{m=1}^{\infty} \frac{1}{m^{\alpha}}.$$

5.27 (Sierpiński). *Mostrar que o conjunto*

$$\left\{ \frac{\varphi(n+1)}{n} \mid n \in \mathbb{N} \right\}$$

é denso em $[0, 1]$, isto é, que, para todo $a \in [0, 1]$ e todo $\epsilon > 0$, existe um inteiro positivo n tal que $\left| \frac{\varphi(n)}{n} - a \right| < \epsilon$.

5.28 (Schinzel). *Mostrar que o conjunto*

$$\left\{ \frac{\varphi(n+1)}{\varphi(n)} \mid n \in \mathbb{N} \right\}$$

é denso no conjunto dos números reais positivos.

5.29. *Mostar que para todo $\alpha \leq 1$ e $n \gg 0$*

$$\sum_{k=1}^n \frac{\varphi(k)}{k^\alpha} = \frac{6}{\pi^2(2-\alpha)} n^{2-\alpha} + O(n^{1-\alpha} \log n).$$

5.30. *Mostrar que*

$$\sum_{k=1}^n \frac{\varphi(k)}{k^2} = \frac{6}{\pi^2} \log n + C + O\left(\frac{\log n}{n}\right),$$

onde $C = \frac{6\gamma}{\pi^2} - \sum_{d \geq 1} \frac{\mu(d) \log d}{d^2}$.

5.5 A Função σ

Lembramos que $\sigma(n) = \sum_{d|n} d$ é uma função multiplicativa. Assim, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ é a fatoração canônica de n , então

$$\sigma(n) = \prod_{j=1}^k (1 + p_j + \cdots + p_j^{\alpha_j}) = \prod_{j=1}^k \frac{p_j^{\alpha_j+1} - 1}{p_j - 1} = \prod_{j=1}^k p_j^{\alpha_j} \left(1 + \frac{1 - p_j^{-\alpha_j}}{p_j - 1} \right)$$

donde $n \prod_{j=1}^k (1 + \frac{1}{p_j}) \leq \sigma(n) < n \prod_{j=1}^k \frac{p_j}{p_j - 1}$. Usando a fórmula de $\varphi(n)$ temos que

$$\prod_{j=1}^k \left(1 - \frac{1}{p_j^2} \right) \leq \frac{\varphi(n)\sigma(n)}{n^2} < 1,$$

mas

$$\prod_{p \text{ primo}} \frac{1}{1 - \frac{1}{p^2}} = \prod_{p \text{ primo}} \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \cdots \right) = \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$$

já que expandindo o produto, cada natural k aparece exatamente uma vez pelo teorema fundamental da aritmética. Logo temos que $\frac{6}{\pi^2} < \frac{\varphi(n)\sigma(n)}{n^2} < 1$ para todo $n > 1$. Juntamente com a proposição 5.30 isso implica a

Proposição 5.32. $\limsup_{n \rightarrow \infty} \frac{\sigma(n)}{n \log \log n} \in (0, \infty)$. Naturalmente, se n é primo, $\sigma(n) = n + 1$, donde $\liminf_{n \rightarrow \infty} \frac{\sigma(n)}{n} = 1$.

Observação 5.33. É possível provar que $\limsup_{n \rightarrow \infty} \frac{\sigma(n)}{n \log \log n} = e^\gamma$.

Temos também a

Proposição 5.34. $\sum_{k=1}^n \sigma(k) = \frac{\pi^2}{12} n^2 + O(n \log n)$

DEMONSTRAÇÃO: Da definição de σ temos que

$$\begin{aligned} \sum_{k=1}^n \sigma(k) &= \sum_{k=1}^n \sum_{d|k} d = \sum_{d=1}^n d \left\lfloor \frac{n}{d} \right\rfloor \\ &= \sum_{d \geq 1} \sum_{\substack{k \geq 1 \\ kd \leq n}} d = \sum_{k \geq 1} \sum_{\substack{d \geq 1 \\ kd \leq n}} d = \sum_{k=1}^n \frac{\left\lfloor \frac{n}{k} \right\rfloor (\left\lfloor \frac{n}{k} \right\rfloor + 1)}{2} \\ &= \frac{n^2}{2} \sum_{k=1}^n \frac{1}{k^2} + O(n \log n) \\ &= \frac{\pi^2}{12} n^2 + O(n \log n), \end{aligned}$$

pois $\sum_{k > n} \frac{1}{k^2} = O\left(\int_n^\infty \frac{dx}{x^2}\right) = O\left(\frac{1}{n}\right)$ e $\sum_{k \geq 1} \frac{1}{k^2} = \frac{\pi^2}{6}$. □

Proposição 5.35. $\sum_{k=1}^n \frac{\sigma(k)}{k} = \frac{\pi^2}{6} n + O(\log n)$.

DEMONSTRAÇÃO: Observemos que $\frac{\sigma(k)}{k} = \sum_{d|k} \frac{d}{k} = \sum_{d'|k} \frac{1}{d'}$, assim por um procedimento similar ao anterior temos

$$\begin{aligned} \sum_{k=1}^n \frac{\sigma(k)}{k} &= \sum_{k=1}^n \sum_{d'|k} \frac{1}{d'} = \sum_{d'=1}^n \frac{1}{d'} \left\lfloor \frac{n}{d'} \right\rfloor \\ &= n \sum_{d'=1}^n \frac{1}{d'^2} + O(\log n) = \frac{\pi^2}{6} n + O(\log n). \end{aligned}$$

□

5.6 Números Livres de Quadrados

Vamos nesta seção a estimar a “probabilidade” de um número natural dado ser livre de quadrados, ou seja, vamos calcular o limite

$$\lim_{n \rightarrow \infty} \frac{1}{n} \# \{1 \leq k \leq n \mid k \text{ é livre de quadrados}\} = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n |\mu(k)|.$$

Proposição 5.36. $\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n |\mu(k)| = \frac{6}{\pi^2}.$

DEMONSTRAÇÃO: Seja $g(x) = \lfloor x^2 \rfloor$ e $f(x) = \sum_{k \leq x} |\mu(k)|$. Observemos que como um natural n se escreve unicamente como $n = r^2 l$ com l livre de quadrados, temos que $\sum_{r \geq 1} f(\frac{x^2}{r^2}) = g(x)$. Assim, pela segunda fórmula de inversão de Möbius (teorema 5.11), temos

$$\begin{aligned} f(x^2) &= \sum_{k \leq x} \mu(k) g\left(\frac{x}{k}\right) = \sum_{k \leq x} \mu(k) \left\lfloor \frac{x^2}{k^2} \right\rfloor \\ &= \sum_{k \leq x} \frac{\mu(k)x^2}{k^2} + O(x) = \frac{6}{\pi^2} x^2 + O(x), \end{aligned}$$

já que $\sum_{k \geq 1} \frac{\mu(k)}{k^2} = \frac{6}{\pi^2}$ (ver a demonstração da proposição 5.27). Se $y = x^2$, temos que $f(y) = \frac{6}{\pi^2} y + O(\sqrt{y})$, o que implica o resultado. \square

5.7 As Funções ω e Ω

Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ com $p_1 < p_2 < \cdots < p_k$ primos é a fatoraçaõ canônica de n , então $\omega(n) = k$ e $\Omega(n) = \sum_{j=1}^k \alpha_j$ são respectivamente o número de fatores primos distintos de n e o número de fatores primos de n com multiplicidade. Vamos provar que, para a “maioria” dos valores de n , $\omega(n)$ e $\Omega(n)$ são da ordem $\log \log n$.

Notemos inicialmente que $\omega(n) \leq \Omega(n)$ para todo n e que

$$\Omega(n) = \sum_{k \geq 1} \sum_{\substack{p \text{ primo} \\ p^k | n}} 1 \quad \text{e} \quad \omega(n) = \sum_{\substack{p \text{ primo} \\ p | n}} 1,$$

donde

$$\begin{aligned}
 \sum_{r=1}^n \Omega(r) - \omega(r) &= \sum_{r=1}^n \sum_{k \geq 2} \sum_{\substack{p \text{ primo} \\ p^k | r}} 1 = \sum_{k \geq 2} \sum_{p \text{ primo}} \left\lfloor \frac{n}{p^k} \right\rfloor \\
 &\leq \sum_{p \text{ primo}} \sum_{k \geq 2} \frac{n}{p^k} = \sum_{p \text{ primo}} \frac{n}{p(p-1)} \\
 &\leq n \sum_{k \geq 2} \left(\frac{1}{k-1} - \frac{1}{k} \right) = O(n).
 \end{aligned}$$

Para mostrar que $\omega(n)$ é da ordem de $\log \log n$ para a maioria dos n , vamos estimar a soma $\sum_{r=1}^n (\omega(r) - \log \log n)^2$. Começamos estimando $\sum_{r=1}^n \omega(r)$. Pelo teorema 5.24, temos

$$\sum_{r=1}^n \omega(r) = \sum_{\substack{p \text{ primo} \\ p \leq n}} \left\lfloor \frac{n}{p} \right\rfloor = n \sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{1}{p} + O(n) = n \log \log n + O(n),$$

Vamos agora estimar $\sum_{r=1}^n \omega(r)^2$, para isso observemos que

$$\begin{aligned}
 \sum_{r=1}^n \omega(r)^2 &= \sum_{r=1}^n \left(\sum_{\substack{p \text{ primo} \\ p | r}} 1 \right)^2 \\
 &= \sum_{r=1}^n \sum_{\substack{p_1, p_2 \text{ primos} \\ p_1 | r, p_2 | r}} 1 = \sum_{\substack{p \text{ primo} \\ p \leq n}} \sum_{\substack{q \text{ primo} \\ q \leq n}} \left\lfloor \frac{n}{\text{mmc}(p, q)} \right\rfloor \\
 &= \sum_{\substack{p \text{ primo} \\ p \leq n}} \left\lfloor \frac{n}{p} \right\rfloor + \sum_{\substack{p, q \text{ primos} \\ p \neq q}} \left\lfloor \frac{n}{pq} \right\rfloor = \sum_{r=1}^n \omega(r) + \sum_{\substack{p, q \text{ primos} \\ p \neq q}} \left\lfloor \frac{n}{pq} \right\rfloor.
 \end{aligned}$$

Note que $\sum_{\substack{p, q \text{ primos} \\ p \neq q}} \left\lfloor \frac{n}{pq} \right\rfloor \leq n \left(\sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{1}{p} \right)^2 = n(\log \log n)^2 + O(n \log \log n)$.

Por outro lado,

$$\begin{aligned}
 \sum_{\substack{p, q \text{ primos} \\ p \neq q}} \left\lfloor \frac{n}{pq} \right\rfloor &= \sum_{\substack{p, q \text{ primos} \\ p \neq q, pq \leq n}} \frac{n}{pq} + O(n) \\
 &\geq n \left(\sum_{\substack{p \text{ primo} \\ p \leq \sqrt{n}}} \frac{1}{p} \right)^2 + O(n) = n(\log \log \sqrt{n} + O(1))^2 + O(n) \\
 &= n(\log \log n)^2 + O(n \log \log n).
 \end{aligned}$$

Portanto $\sum_{r=1}^n \omega(r)^2 = n(\log \log n)^2 + O(n \log \log n)$.

Assim, temos que

$$\begin{aligned} \sum_{r=1}^n (\omega(r) - \log \log n)^2 &= \sum_{r=1}^n \omega(r)^2 - 2 \log \log n \sum_{r=1}^n \omega(r) + n(\log \log n)^2 \\ &= n(\log \log n)^2 + O(n \log \log n) \\ &\quad - 2 \log \log n \cdot (n \log \log n + O(n)) + n(\log \log n)^2 \\ &= O(n \log \log n). \end{aligned}$$

Definição 5.37. *Seja $f, g: \mathbb{N} \rightarrow \mathbb{R}$. Dizemos que a ordem normal de $f(n)$ é $g(n)$ se podemos decompor $\mathbb{N} = A \cup B$ de modo que*

$$\lim_{n \rightarrow \infty} \frac{\#\{k \in B \mid k \leq n\}}{n} = 0 \quad e \quad \lim_{\substack{n \rightarrow \infty \\ n \in A}} \frac{f(n)}{g(n)} = 1.$$

Observe que esta partição de \mathbb{N} implica que A contém quase todos os números naturais.

Em particular, dado $\alpha > 0$, $B(n) = \{r \leq n \mid |\omega(r) - \log \log n| \geq (\log \log n)^{\frac{1}{2} + \alpha}\}$ é tal que $\#B(n) = O(n/(\log \log n)^{2\alpha})$. Temos assim que a ordem normal de $\omega(n)$ (e de $\Omega(n)$ pois $\sum_{k \leq n} |\Omega(k) - \omega(k)| = O(n)$) é $\log \log n$.

Erdős e Kac provaram em [52] que a distribuição de probabilidade de $\frac{\omega(n) - \log \log n}{\sqrt{\log \log n}}$, $n \in \mathbb{N}$, é a distribuição normal usual. Mais precisamente, dados $a, b \in \mathbb{R}$ com $a < b$, temos

$$\lim_{n \rightarrow \infty} \frac{1}{n} \# \left\{ k \leq n \mid a \leq \frac{\omega(k) - \log \log k}{\sqrt{\log \log k}} \leq b \right\} = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt.$$

5.8 A Função Número de Divisores $d(n)$

A função $d(n) = \sum_{d|n} 1$ tem um comportamento bastante irregular. Temos que $d(p) = 2$ para todo primo p , donde $\liminf_{n \rightarrow \infty} d(n) = 2$. Por outro lado podemos estimar a ordem máxima de $d(n)$.

Proposição 5.38. *Se $\epsilon > 0$ então*

$$\lim_{n \rightarrow \infty} \frac{d(n)}{2^{(1+\epsilon) \log n / \log \log n}} = 0 \quad e \quad \limsup_{n \rightarrow \infty} \frac{d(n)}{2^{(1-\epsilon) \log n / \log \log n}} = +\infty.$$

DEMONSTRAÇÃO: Para a primeira afirmação, basta mostrar que

$$\log d(n) \leq (1 + \epsilon') \frac{\log 2 \log n}{\log \log n}$$

para algum ϵ' tal que $0 < \epsilon' < \epsilon$. Para isto, considere a fatoração canônica em primos $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, de modo que $d(n) = \prod_{i=1}^k (1 + \alpha_i)$. Temos

$$\log d(n) = \sum_{i=1}^k \log(1 + \alpha_i) \quad \text{e} \quad \log n = \sum_{i=1}^k \alpha_i \log p_i.$$

Seja $\delta > 0$. Dividimos em dois casos: primeiro, se $p_i \geq (\log n)^{1-\delta}$, temos $\log p_i \geq (1 - \delta) \log \log n$, e como $2^{\alpha_i} \geq 1 + \alpha_i \iff \alpha_i \log 2 \geq \log(1 + \alpha_i)$,

$$\log(1 + \alpha_i) \leq \alpha_i \log 2 \leq (1 - \delta)^{-1} \frac{\log 2 \cdot \alpha_i \log p_i}{\log \log n}.$$

Segundo, se $p_i < (\log n)^{1-\delta}$, como $2^{\alpha_i} \leq n \implies \alpha_i \leq \log n / \log 2 \implies \log(1 + \alpha_i) \leq 2 \log \log n$ para $n \gg 0$, temos

$$\sum_{p_i < (\log n)^{1-\delta}} \log(1 + \alpha_i) \leq 2(\log n)^{1-\delta} \log \log n = o\left(\frac{\log n}{\log \log n}\right).$$

Somando sobre todos os primos, temos portanto

$$\begin{aligned} \log d(n) &= \sum_{1 \leq i \leq k} \log(1 + \alpha_i) \\ &\leq (1 - \delta)^{-1} \frac{\log 2 \cdot \sum_{1 \leq i \leq k} \alpha_i \log p_i}{\log \log n} + o\left(\frac{\log n}{\log \log n}\right) \\ &\leq ((1 - \delta)^{-1} + \delta) \frac{\log 2 \cdot \log n}{\log \log n}, \end{aligned}$$

o que implica nossa afirmação para $n \gg 0$ e δ suficientemente pequeno.

Para a segunda afirmação, considere o produto $n_k = p_1 p_2 \cdots p_k$ dos k primeiros primos. Basta mostrar que

$$\log d(n_k) - (1 - \epsilon) \frac{\log 2 \log n_k}{\log \log n_k} \rightarrow \infty$$

quando $k \rightarrow \infty$. Temos $d(n_k) = 2^k$ donde $\log d(n_k) = k \log 2$. Por outro lado, pelo corolário 5.16, temos

$$\log n_k = \sum_{j=1}^k \log p_j = \sum_{j=1}^k \log O(j \log j) = k \log k + O(k \log \log k)$$

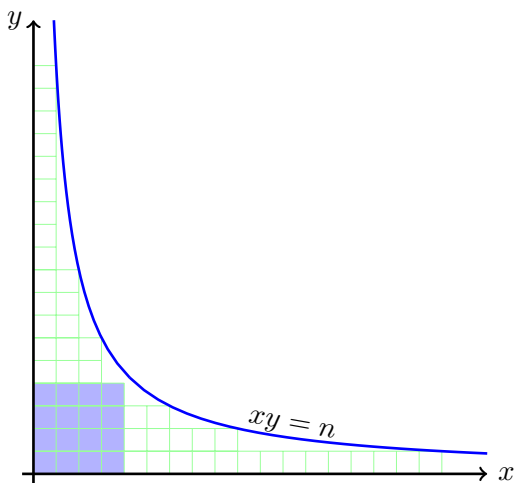
de modo que $\log n_k = (1 + o(1))k \log k$, $\log \log n_k = (1 + o(1)) \log k$ e assim $\frac{\log n_k}{\log \log n_k} = (1 + o(1))k$, o que implica o resultado. \square

Vamos agora calcular a ordem média de $d(n)$.

Proposição 5.39. $\frac{1}{n} \sum_{k=1}^n d(k) = \log n + 2\gamma - 1 + O\left(\frac{1}{\sqrt{n}}\right)$ onde γ é a constante de Euler-Mascheroni

DEMONSTRAÇÃO: Temos

$$\sum_{k=1}^n d(k) = \sum_{k=1}^n \sum_{d|k} 1 = \sum_{d=1}^n \left\lfloor \frac{n}{d} \right\rfloor = n \sum_{d=1}^n \frac{1}{d} + O(n) = n \log n + O(n).$$



Podemos estimar o termo de erro de forma mais precisa, contando os pontos de coordenadas inteiras sob o gráfico de $y = n/x$, conforme a

figura:

$$\begin{aligned}
 \sum_{d=1}^n \left\lfloor \frac{n}{d} \right\rfloor &= \#\{(x, y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid xy \leq n\} \\
 &= \#\{(x, y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid x \leq \sqrt{n}, xy \leq n\} \\
 &\quad + \#\{(x, y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid y \leq \sqrt{n}, xy \leq n\} \\
 &\quad - \#\{(x, y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid x \leq \sqrt{n}, y \leq \sqrt{n}\} \\
 &= 2 \sum_{d=1}^{\lfloor \sqrt{n} \rfloor} \left\lfloor \frac{n}{d} \right\rfloor - \lfloor \sqrt{n} \rfloor^2 = 2 \left(n \sum_{d=1}^{\lfloor \sqrt{n} \rfloor} \frac{1}{d} + O(\sqrt{n}) \right) - \left(\sqrt{n} + O(1) \right)^2 \\
 &= 2n \left(\log \sqrt{n} + \gamma + O\left(\frac{1}{\sqrt{n}}\right) \right) - n + O(\sqrt{n}) \\
 &= n \log n + (2\gamma - 1)n + O(\sqrt{n})
 \end{aligned}$$

utilizando a estimativa mais precisa $\sum_{1 \leq j \leq n} \frac{1}{j} = \log n + \gamma + O\left(\frac{1}{n}\right)$. \square

Observação 5.40. *É possível dar estimativas mais precisas para o termo de erro nesta proposição. Seja $\Delta(n) := \sum_{k=1}^n d(k) - n(\log n + 2\gamma - 1)$. A proposição anterior (que é devida a Dirichlet) diz que $\Delta(n) = O(n^{1/2})$. O problema dos divisores de Dirichlet consiste em determinar o menor $\theta \in \mathbb{R}$ tal que $\Delta(n) = O(n^{\theta+\varepsilon})$, $\forall \varepsilon > 0$. Hardy provou em [66] que $\theta \geq \frac{1}{4}$: de fato, ele mostrou que existe $c > 0$ tal que, para certos valores arbitrariamente grandes de n , $\Delta(n) > cn^{1/4}$, e, para outros valores arbitrariamente grandes de n , $\Delta(n) < -cn^{1/4}$. Por outro lado, Huxley provou em [75] que $\theta \leq \frac{131}{416} = 0,31490384615384615384615384615384615 \dots$. Conjetura-se que $\theta = 1/4$.*

Finalmente, para quase todo $n \in \mathbb{N}$, $\omega(n)$ e $\Omega(n)$ são da ordem de $\log \log n$ pela seção anterior, donde, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ é a fatoração canônica de n ,

$$2^{\omega(n)} = 2^k \leq \prod_{j=1}^k (1 + \alpha_j) = d(n) \leq \prod_{j=1}^k 2^{\alpha_j} = 2^{\Omega(n)}.$$

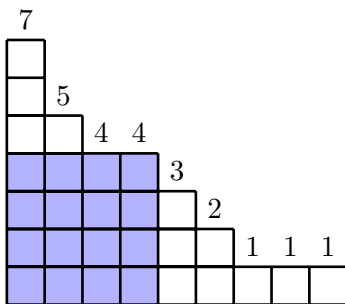
Assim, $\log d(n)$ é da ordem de $\log 2 \cdot \log \log n$ para quase todo n , ou seja, $d(n) = (\log n)^{\log 2} \ll \log n$ para quase todo n , apesar de a ordem média

de $d(n)$ ser $\log n$. Isso se deve ao fato de, para alguns poucos valores de n , $d(n)$ ser muito maior que $\log n$, lembrando que a ordem máxima de $d(n)$ é $2^{(1+o(1)) \log n / \log \log n} \gg \log n$, para todo $n \in \mathbb{N}$. De fato, Ramanujam mostrou que, para $r \geq 1$, esse efeito faz com que $\sum_{k=1}^n (d(k))^r$ seja da ordem $C(r)n(\log n)^{2^r-1}$ para uma certa constante $C(r) \in (0, \infty)$.

5.9 A Função Número de Partições $p(n)$

Uma *partição* de um inteiro positivo n é uma forma de escrever n como soma de inteiros positivos, não importando a ordem. Assim, podemos identificar uma partição de n com um vetor (a_1, a_2, \dots, a_k) , onde k, a_1, a_2, \dots, a_k são inteiros positivos, $a_1 \geq a_2 \geq \dots \geq a_k$ e $a_1 + a_2 + \dots + a_k = n$. Para cada inteiro positivo n , denotamos por $p(n)$ o número de partições distintas de n . Por exemplo, como as formas de escrever 6 como soma de inteiros positivos são $6 = 5 + 1 = 4 + 2 = 4 + 1 + 1 = 3 + 3 = 3 + 2 + 1 = 3 + 1 + 1 + 1 = 2 + 2 + 2 = 2 + 2 + 1 + 1 = 2 + 1 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1 + 1$, temos $p(6) = 11$.

Uma partição pode ser representada por uma pilha de quadradinhos onde a altura de cada coluna da pilha é monótona não crescente da esquerda para a direita. Uma convenção é de que as alturas das colunas são os inteiros $a_1 \geq a_2 \geq \dots \geq a_k$. Na figura mostramos a partição $7 + 5 + 4 + 4 + 3 + 2 + 1 + 1 + 1$ de 28.



Não é muito fácil estimar com precisão a ordem de magnitude da função $p(n)$. Começamos mostrando as seguintes estimativas elementares, análogas às estimativas mostradas em [73]:

Proposição 5.41. $2^{\lfloor \sqrt{2n} \rfloor - 2} \leq p(n) \leq \lfloor \sqrt{n} \rfloor n^{2\lfloor \sqrt{n} \rfloor}, \forall n \geq 1.$

DEMONSTRAÇÃO: Essas desigualdades são claramente válidas para $n = 1$. Vamos supor a partir de agora que $n > 1$. A primeira desigualdade pode ser mostrada considerando as partições obtidas da seguinte forma: Escolhemos k um número natural tal que $1 + 2 + \dots + k + (k + 1) \leq n$ (para isto basta tomar $k = \lfloor \sqrt{2n} \rfloor - 2$ para $n \geq 2$). Para cada conjunto $A = \{a_1, a_2, \dots, a_r\} \subset \{1, 2, \dots, k\}$, podemos associar a partição

$$n = a_1 + a_2 + \dots + a_r + (n - a_1 - a_2 - \dots - a_r).$$

Note que $n - (a_1 + a_2 + \dots + a_r) \geq n - (1 + 2 + \dots + k) \geq k + 1$ é o maior termo da partição, o que mostra que, para $n \geq 3$, a subconjuntos distintos de $\{1, 2, \dots, k\}$ correspondem partições distintas, e como há $2^k = 2^{\lfloor \sqrt{2n} \rfloor - 2}$ subconjuntos de $\{1, 2, \dots, k\}$, segue que $p(n) \geq 2^{\lfloor \sqrt{2n} \rfloor - 2}$ para $n \geq 2$, e a primeira desigualdade está provada.

Já para a segunda desigualdade, a cada partição $\pi = (a_1, a_2, \dots, a_k)$ de n , com $a_1 \geq a_2 \geq \dots \geq a_k$, associamos o maior inteiro positivo $q = q(\pi)$ tal que $a_q \geq q$. Em outras palavras, $q(\pi)$ é o lado do maior quadrado contido no diagrama da partição: no exemplo da figura anterior, $q(\pi) = 4$ (e o quadrado está sombreado). Note que $q(\pi)^2 \leq n$. Assim, há $\lfloor \sqrt{n} \rfloor$ possibilidades para $q(\pi)$.

Por outro lado, uma vez determinado $q(\pi)$, temos que $a_1, \dots, a_{q(\pi)} \geq q(\pi)$ satisfazem as desigualdades $0 \leq a_i < n, \forall i \leq q(\pi)$, que têm (esquecendo o fato de que os a_i estão em ordem decrescente) no máximo $n^{q(\pi)} \leq n^{\lfloor \sqrt{n} \rfloor}$ soluções (pois há no máximo n possibilidades para cada a_i). Além disso, como $a_j \leq q(\pi), \forall j > q(\pi)$, os a_j , para $j > q(\pi)$ estão unicamente determinados pelos números $b_i, 1 \leq i \leq q(\pi)$ dados por $b_i = |\{j > q(\pi); a_j \geq i\}|, 1 \leq i \leq q(\pi)$, os quais satisfazem $\sum_{i \leq q(\pi)} b_i = \sum_{j > q(\pi)} a_j < n$, e assim, como antes, há no máximo $n^{q(\pi)} \leq n^{\lfloor \sqrt{n} \rfloor}$ possibilidades para os $b_i, 1 \leq i \leq q(\pi)$ e portanto para os $a_j, j > q(\pi)$. Assim, temos

$$p(n) \leq \sum_{1 \leq q \leq \lfloor \sqrt{n} \rfloor} (n^q)^2 \leq \lfloor \sqrt{n} \rfloor (n^{\lfloor \sqrt{n} \rfloor})^2 = \lfloor \sqrt{n} \rfloor \cdot n^{2\lfloor \sqrt{n} \rfloor}.$$

□

Para estimativas um pouco mais precisas, vamos usar a *função geratriz* de $p(n)$. Note que $p(n)$ é o número de soluções (m_1, m_2, m_3, \dots) com os m_k inteiros não negativos de $\sum_{k \geq 1} km_k = n$. Assim, convencionando $p(0) = 1$, temos a igualdade seguinte:

$$\sum_{n \geq 0} p(n)x^n = \prod_{k \geq 1} \left(\sum_{m \geq 0} x^{km} \right) = \prod_{k \geq 1} \left(\frac{1}{1 - x^k} \right).$$

A igualdade em princípio é formal mas a estimativa acima garante a convergência se $|x| < 1$. Assim, para todo $N \in \mathbb{N}$, e todo $x \in [0, 1)$,

$$\sum_{n \geq 0} p(n)x^n \leq \prod_{k=1}^N \left(\sum_{m \geq 0} x^{km} \right) = \prod_{k=1}^N \left(\frac{1}{1 - x^k} \right).$$

Usaremos esses fatos para provar o seguinte

Teorema 5.42. *Para todo $N \in \mathbb{N}$, temos $p(N) \leq e^{\pi\sqrt{2N/3}}$. Além disso,*

$$\lim_{n \rightarrow +\infty} \frac{\log p(n)}{\sqrt{n}} = \pi\sqrt{\frac{2}{3}}.$$

DEMONSTRAÇÃO: Da discussão anterior, temos que, para todo $x > 0$,

$$p(N)x^N \leq \sum_{n \geq 0} p(n)x^n \leq \prod_{k \geq 1} \left(\frac{1}{1 - x^k} \right) \leq \prod_{k \geq 1} \left(\frac{1}{1 - x^k} \right).$$

Tomando $x = e^{-\varepsilon}$, com $\varepsilon > 0$, obtemos $p(N)e^{-\varepsilon N} \leq \prod_{k \geq 1} \left(\frac{1}{1 - e^{-\varepsilon k}} \right)$, donde $\log p(N) - \varepsilon N \leq \sum_{k \geq 1} -\log(1 - e^{-\varepsilon k})$. Temos que $\varepsilon \sum_{k \geq 1} -\log(1 - e^{-\varepsilon k})$ é a soma inferior de Riemann associada à partição $\{0, \varepsilon, 2\varepsilon, 3\varepsilon, \dots\}$ para a integral $\int_0^\infty -\log(1 - e^{-t})dt = \frac{\pi^2}{6}$ (essa última igualdade segue de

$$\begin{aligned} \int_0^\infty -\log(1 - e^{-t})dt &= \int_0^\infty \left(\sum_{n \geq 1} e^{-nt}/n \right) dt \\ &= \sum_{n \geq 1} \frac{1}{n} \int_0^\infty e^{-nt} dt = \sum_{n \geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}, \end{aligned}$$

sendo a troca da ordem da soma e da integral justificada pelo fato de os termos serem todos positivos), e logo $\varepsilon \sum_{k \geq 1} -\log(1 - e^{-\varepsilon k}) \leq \frac{\pi^2}{6}$.

Assim, $\log p(N) - \varepsilon N \leq \sum_{k \geq 1} -\log(1 - e^{-\varepsilon k}) \leq \frac{\pi^2}{6\varepsilon}$, donde $\log p(N) \leq \varepsilon N + \frac{\pi^2}{6\varepsilon}$, para todo $\varepsilon > 0$. Escolhendo $\varepsilon = \frac{\pi}{\sqrt{6N}}$, obtemos

$$\log p(N) \leq 2\pi\sqrt{\frac{N}{6}} = \pi\sqrt{\frac{2N}{3}},$$

o que prova a primeira parte do teorema.

Da estimativa da proposição 5.41 (ou da primeira parte do teorema) e da discussão sobre a função geratriz de $p(n)$ segue que, $\forall x \in [0, 1)$, a série $\sum_{n \geq 0} p(n)x^n$ converge e vale a igualdade $\sum_{n \geq 0} p(n)x^n = \prod_{k \geq 1} \left(\frac{1}{1-x^k}\right)$. Vamos tomar $x = e^{-\varepsilon}$, onde $\varepsilon = \frac{\pi}{\sqrt{6m}}$ ($m \gg 1$ vai ser escolhido posteriormente). Temos $\log \prod_{k \geq 1} \left(\frac{1}{1-e^{-\varepsilon k}}\right) = \sum_{k \geq 1} -\log(1 - e^{-\varepsilon k}) \leq \frac{\pi^2}{6\varepsilon}$, como acima, e, por outro lado, como $\varepsilon \sum_{k \geq 1} -\log(1 - e^{-\varepsilon k})$ é a soma superior de Riemann associada à partição $\{\varepsilon, 2\varepsilon, 3\varepsilon, \dots\}$ para a integral

$$\int_{\varepsilon}^{\infty} -\log(1 - e^{-t})dt = \frac{\pi^2}{6} - O(\varepsilon \log \varepsilon^{-1}),$$

temos

$$\log \prod_{k \geq 1} \left(\frac{1}{1 - e^{-\varepsilon k}}\right) = \frac{\pi^2}{6\varepsilon} - O(\log \varepsilon^{-1}) = \pi\sqrt{\frac{m}{6}} - O(\log m),$$

e portanto $\sum_{n \geq 0} p(n)x^n = \exp(\pi\sqrt{\frac{m}{6}} - O(\log m))$.

Por outro lado, temos, para cada $n \in \mathbb{N}$,

$$\begin{aligned} p(n)x^n &= p(n) \exp(-\varepsilon n) \leq \exp(-\varepsilon n + \pi\sqrt{2n/3}) \\ &= \exp\left(\pi\left(-\frac{n}{\sqrt{6m}} + \sqrt{2n/3}\right)\right) = \exp\left(\frac{\pi}{\sqrt{6m}}(2\sqrt{mn} - n)\right) \\ &= \exp\left(\frac{\pi}{\sqrt{6m}}(m - (\sqrt{n} - \sqrt{m})^2)\right). \end{aligned}$$

Tomando $m = N - N^{5/6}$ e $n = N + k$, $k \geq 0$,

$$\sqrt{n} - \sqrt{m} = \frac{n - m}{\sqrt{n} + \sqrt{m}} > \frac{N^{5/6} + k}{2\sqrt{N + k}} > \frac{N^{1/3}}{2} + \frac{1}{3}\sqrt{\frac{k}{N}},$$

e logo

$$\begin{aligned} p(n)x^n &\leq \exp\left(\frac{\pi}{\sqrt{6m}}\left(m - \left(\frac{N^{1/3}}{2} + \frac{1}{3}\sqrt{\frac{k}{N}}\right)^2\right)\right) \\ &< \exp\left(\frac{\pi}{\sqrt{6m}}\left(m - \left(\frac{N^{2/3}}{4} + \frac{k}{9N}\right)\right)\right). \end{aligned}$$

Assim,

$$\begin{aligned} \sum_{n \geq N} p(n)x^n &< \exp\left(\pi\sqrt{\frac{m}{6}}\right) \exp\left(-\frac{\pi m^{1/6}}{4\sqrt{6}}\right) \sum_{k \geq 0} \exp\left(-\frac{\pi k}{9N\sqrt{6m}}\right) \\ &= O\left(\exp\left(\pi\sqrt{\frac{m}{6}}\right) \exp\left(-\frac{\pi m^{1/6}}{4\sqrt{6}}\right) N\sqrt{m}\right) \\ &= o\left(\exp\left(\pi\sqrt{\frac{m}{6}} - \frac{\pi m^{1/6}}{10}\right)\right). \end{aligned}$$

Analogamente, se $n \leq N - 2N^{5/6} = m - N^{5/6}$,

$$\sqrt{m} - \sqrt{n} = \frac{m - n}{\sqrt{n} + \sqrt{m}} > \frac{N^{5/6}}{2\sqrt{N}} = \frac{N^{1/3}}{2} > \frac{m^{1/3}}{2},$$

donde

$$p(n)x^n \leq \exp\left(\frac{\pi}{\sqrt{6m}}\left(m - \frac{m^{2/3}}{4}\right)\right) = \exp\left(\pi\sqrt{\frac{m}{6}}\right) \exp\left(-\frac{\pi m^{1/6}}{4\sqrt{6}}\right).$$

Assim,

$$\begin{aligned} \sum_{n \leq N - 2N^{5/6}} p(n)x^n &< N \exp\left(\pi\sqrt{\frac{m}{6}}\right) \exp\left(-\frac{\pi m^{1/6}}{4\sqrt{6}}\right) \\ &= o\left(\exp\left(\pi\sqrt{\frac{m}{6}} - \frac{\pi m^{1/6}}{10}\right)\right). \end{aligned}$$

Portanto, como $\sum_{n \geq 0} p(n)x^n = \exp(\pi\sqrt{\frac{m}{6}} - O(\log m))$, temos

$$\sum_{n \geq N} p(n)x^n = o\left(\sum_{n \geq 0} p(n)x^n\right), \quad \sum_{n \leq N - 2N^{5/6}} p(n)x^n = o\left(\sum_{n \geq 0} p(n)x^n\right),$$

donde $\sum_{n=N-2N^{5/6}}^{N-1} p(n)x^n > \frac{1}{2} \sum_{n \geq 0} p(n)x^n$, e portanto existe k com

$$N - 2N^{5/6} \leq k \leq N - 1, \quad p(k)x^k > \frac{1}{4N^{5/6}} \sum_{n \geq 0} p(n)x^n,$$

donde

$$\begin{aligned} \log p(k) - \frac{k\pi}{\sqrt{6m}} &= \log p(k) + k \log x \\ &> \log \sum_{n \geq 0} p(n)x^n - \log(4N^{5/6}) = \pi \sqrt{\frac{m}{6}} - O(\log m), \end{aligned}$$

e portanto

$$\begin{aligned} \log p(k) &> \pi \sqrt{\frac{m}{6}} - O(\log m) + \frac{k\pi}{\sqrt{6m}} \\ &= \pi \sqrt{\frac{m}{6}} - O(\log m) + (m - O(m^{5/6})) \frac{\pi}{\sqrt{6m}} \\ &= \pi \sqrt{\frac{2m}{3}} - O(m^{1/3}). \end{aligned}$$

Como $p(n)$ é crescente,

$$\log p(N) \geq \log p(k) > \pi \sqrt{\frac{2m}{3}} - O(m^{1/3}) = \pi \sqrt{\frac{2N}{3}} - O(N^{1/3}).$$

Junto com a estimativa da primeira parte do teorema, isto implica a segunda afirmação do teorema. \square

Com métodos mais sofisticados, Hardy e Ramanujan provaram em [70] que $\lim_{n \rightarrow \infty} 4n\sqrt{3} \cdot p(n) \exp(-\pi\sqrt{2n/3}) = 1$.

Posteriormente, Rademacher provou em [122] um resultado ainda mais preciso, que fornece, para cada inteiro positivo n , uma série que converge a $p(n)$. Para cada inteiro positivo k , seja

$$A_k(n) = \sum_{\substack{1 \leq h \leq k \\ \text{mdc}(h, k) = 1}} \exp\left(\pi i s(h, k) - 2\pi i \frac{nh}{k}\right)$$

onde

$$s(h, k) = \sum_{j=1}^{k-1} \frac{j}{k} \left(\left\{ \frac{hj}{k} \right\} - \frac{1}{2} \right)$$

(lembre que $\{x\} = x - \lfloor x \rfloor$). Então

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n) \sqrt{k} \frac{d}{dn} \left(\frac{\sinh \left(\pi \sqrt{\frac{2}{3}(n - 1/24)/k} \right)}{\sqrt{n - 1/24}} \right).$$

Aqui a notação $\frac{d}{dn}$ significa derivada em relação a n , considerando a expressão acima definida para todo número real $n \geq 1$. Estimativas cuidadosas mostram que este resultado implica que, para todo $n \geq 576$, $p(n)$ é o inteiro mais próximo a

$$\frac{1}{2\pi\sqrt{2}} \sum_{k=1}^{\lfloor 2\sqrt{n}/3 \rfloor} A_k(n) \sqrt{k} \frac{d}{dn} \left(\frac{\exp \left(\pi \sqrt{\frac{2}{3}(n - 1/24)/k} \right)}{\sqrt{n - 1/24}} \right).$$

É possível mostrar que o erro da aproximação acima de $p(n)$ é $O(n^{-3/8})$ (veja o capítulo 14 de [123]).

5.10 A Função Custo Aritmético $\tau(n)$

O custo de um número inteiro é definido como o número mínimo de operações aritméticas necessárias para obter esse inteiro a partir de 1. Mais precisamente, dado $k \in \mathbb{N}$, definimos $\tau(k)$ como o menor $m \in \mathbb{N}$ para o qual existe uma sequência (s_0, s_1, \dots, s_m) onde $s_0 = 1$, $s_m = k$ e para cada $l \geq 1$, existem i, j com $0 \leq i, j < l$ com $s_l = s_i * s_j$, onde $*$ $\in \{+, -, \cdot\}$. Essa função tem um papel importante em [136], e também é estudada em [100]. Esta seção é baseada em [107].

Não é difícil ver que $|\tau(n) - \tau(-n)| \leq 2$ para todo $n \in \mathbb{Z}$. Vamos nos restringir ao caso $n \in \mathbb{N}$, e queremos dar estimativas assintóticas para $\tau(n)$, $n \in \mathbb{N}$.

Proposição 5.43. $\log_2 \log_2 n + 1 \leq \tau(n) \leq 2 \log_2 n$.

DEMONSTRAÇÃO: Dada a sequência (s_0, \dots, s_m) como na definição de $\tau(n)$ temos que $s_k \leq 2^{k-1}$ para todo $k \geq 1$, de fato, isso segue por

indução de $s_k \leq \max\{2s, s^2\}$, onde $s = \max\{|s_j| : j < k\}$. Por outro lado, como $\tau(2n) \leq \tau(n) + 1$ e $\tau(2n+1) \leq \tau(n) + 2$ para todo $n \in \mathbb{N}$, por indução segue que $\tau(n) \leq 2\log_2 n$ para todo $n \geq 1$, assim temos a segunda desigualdade. A primeira desigualdade não pode ser melhorada para todo $n \in \mathbb{N}$ grande já que $\tau(2^{2^k}) = k + 1$ para todo $k \in \mathbb{N}$. \square

Vamos provar que $\tau(n) > \frac{\log n}{\log \log n}$ para quase todo $n \in \mathbb{N}$. Mas precisamente, temos

Teorema 5.44. *Dado $\epsilon > 0$ temos que*

1. $\tau(n) \geq \frac{\log n}{\log \log n} + (1 - \epsilon) \frac{\log n \cdot \log \log \log n}{(\log \log n)^2}$ para quase todo $n \in \mathbb{N}$
2. $\tau(n) \leq \frac{\log n}{\log \log n} + (3 + \epsilon) \frac{\log n \cdot \log \log \log n}{(\log \log n)^2}$ para $n \in \mathbb{N}$ suficientemente grande.

Na verdade o mesmo resultado vale se tivéssemos um número arbitrário de operações binárias, incluindo $+$, \cdot . Vamos dividir a prova do teorema acima nos seguintes resultados

Proposição 5.45. *Suponha que temos s operações binárias na definição de τ . Então $N(k) = \#\{n \in \mathbb{N} \mid \tau(n) \leq k\}$ satisfaz $N(k) \leq A^k \cdot k^k$, para uma certa constante $A = A(s) > 0$.*

DEMONSTRAÇÃO: Seja $\Lambda = \{*_1, \dots, *_s\}$ o conjunto de operações. Se $\tau(n) = k$ então existe (s_0, \dots, s_k) com $s_0 = 1$, $s_k = n$, e para cada $l \geq 1$ existem $t_l \leq s$, i_l, j_l com $0 \leq i_l, j_l < l$ tais que $s_l = s_{i_l} *_l s_{j_l}$. Devemos ter $\{i_1, j_1, i_2, j_2, \dots, i_k, j_k\} = \{0, 1, \dots, k-1\}$, se não teríamos criado um s_i desnecessário, e logo $\tau(n) < k$. Além disso, se $(r_1, \dots, r_{2k}) = (i_1, j_1, \dots, i_k, j_k)$, podemos supor que existe uma sequência $1 \leq l_1 < l_2 < \dots < l_k \leq 2k$ tal que $r_{l_i} = i - 1$, para $1 \leq i \leq k$. De fato, se $P(j) = \min\{i \mid r_i = j\}$ podemos supor sem perda de generalidade que $P(0) < P(1) < \dots < P(k-1)$, já que caso contrário, se $P(j) > P(j+1)$, então s_j não é usado para criar s_{j+1} , e portanto s_{j+1} pode ser criado antes de s_j . Assim, escolhendo (s_0, s_1, \dots, s_k) com $M = \max\{m \geq 1 \mid P(j) < P(j+1), \forall j < m\}$ máximo, devemos ter $M = k-1$, pois, caso contrário, $P(M) > P(M+1)$ e, trocando as posições de s_{M+1} e s_M , aumentaríamos o valor de M , o que é uma contradição. Podemos então tomar $l_i = P(i)$, para $0 \leq i \leq k-1$.

Seja $N'(k) = \#\{n \in \mathbb{N} \mid \tau(n) = k\}$. Pelos argumentos acima, segue que $N'(k) \leq s^k N''(k)$, onde

$$N''(k) = \# \left\{ (r_1, \dots, r_{2k}) \left| \begin{array}{l} r_i \in \{0, 1, \dots, k-1\} \text{ e existe uma se-} \\ \text{quência } 1 \leq l_1 < \dots < l_k \leq 2k \text{ com} \\ r_{l_j} = j-1 \text{ para } j = 1, \dots, k \end{array} \right. \right\}$$

Por outro lado, $N''(k) \leq \binom{2k}{k} k^k < 2^{2k} \cdot k^k = (4k)^k$, donde $N'(k) \leq (4sk)^k$. Portanto $N(k) \leq \sum_{r=0}^k N'(r) \leq (4s+1)^k \cdot k^k$. \square

Corolário 5.46. *Dado $\epsilon > 0$, temos, para quase todo $n \in \mathbb{N}$, $\tau(n) \geq f(n)$ onde*

$$f(n) = \frac{\log n}{\log \log n} + (1 - \epsilon) \frac{\log n \cdot \log \log \log n}{(\log \log n)^2}$$

DEMONSTRAÇÃO: Vamos estimar $B(n) = \#\{k \leq n \mid \tau(k) \leq f(k)\}$. Se $k \in B(n)$ então $\tau(k) \leq f(k) \leq f(n)$, e, pela proposição acima, temos no máximo $N(f(n)) \leq (Af(n))^{f(n)}$ naturais k com essa propriedade, onde $A = 4s + 1$, mas então para n grande, $\#B(n)$ é menor ou igual a

$$\begin{aligned} (Af(n))^{f(n)} &= \exp(f(n) \log(Af(n))) \\ &< \exp \left(f(n) \log \left(\frac{\log n}{(\log \log n)^{1-\epsilon/2}} \right) \right) \\ &= \exp \left(\frac{\log n}{\log \log n} \left(1 + \frac{(1-\epsilon) \log \log \log n}{\log \log n} \right) \times \right. \\ &\quad \left. \times \left(\log \log n - \left(1 - \frac{\epsilon}{2}\right) \log \log \log n \right) \right) \\ &\leq \exp \left(\log n - \frac{\epsilon}{2} \frac{\log n \cdot \log \log \log n}{\log \log n} \right) \\ &= n \cdot \exp \left(-\frac{\epsilon}{2} \frac{\log n \cdot \log \log \log n}{\log \log n} \right) = o(n). \end{aligned}$$

\square

Se tivermos operações p -árias em vez de operações binárias ($p \geq 2$) temos um resultado análogo trocando $N(k) \leq A^k \cdot k^k$ por $N(k) \leq A^k \cdot k^{(p-1)k}$ no enunciado da proposição 5.45 e $f(n)$ por $\frac{f(n)}{p-1}$ no corolário.

Vamos agora obter a estimativa superior do teorema, usando somente as operações $+$ e \cdot .

Proposição 5.47. *Dado $\epsilon > 0$, temos, para n suficientemente grande, $\tau(n) \leq g(n)$ onde*

$$g(n) = \frac{\log n}{\log \log n} + (3 + \epsilon) \frac{\log n \cdot \log \log \log n}{(\log \log n)^2}.$$

DEMONSTRAÇÃO: Sejam $B = \lfloor \frac{\log n}{(\log \log n)^3} \rfloor$ e $C = B^k$, onde $k = \lfloor \log \log n \rfloor$. Nos cálculos a seguir vamos omitir as partes inteiras. Tome

$$\begin{array}{llll} s_0 = 1, & s_1 = 2, & \dots & s_{B-2} = B - 1, \\ s_{B-1} = B, & s_B = 2B, & \dots & s_{2B-3} = (B-1)B \\ & & \vdots & \\ s_{(k-1)(B-1)} = B^{k-1}, & s_{(k-1)(B-1)+1} = 2B^{k-1} & \dots & s_{k(B-1)-1} = (B-1)B^{k-1} \\ s_{k(B-1)} = B^k & & & \end{array}$$

Considere agora a representação de n na base C , isto é

$$\begin{aligned} n &= a_0 + a_1 C + \dots + a_r C^r, \quad 0 \leq a_i \leq C - 1, \\ r &= \left\lfloor \frac{\log n}{\log C} \right\rfloor \sim \frac{\log n}{(\log \log n)^2}, \end{aligned}$$

e as representações dos a_i na base B

$$a_i = b_{i1} + b_{i2}B + \dots + b_{ik}B^{k-1} \text{ onde } 0 \leq b_{ij} \leq B - 1.$$

Observe agora que já construímos os números $b_{ij}B^{j-1}$ e logo podemos construir cada a_i fazendo $k-1$ somas. Como temos $r+1$ coeficientes a_i , gastamos no total $(k-1)(r+1)$ operações para gerar todos os a_i . Uma vez gerados os a_i , podemos gerar n com os seguintes $2r$ passos:

$$\begin{aligned} a_r &\rightarrow a_r C \\ &\rightarrow a_r C + a_{r-1} \\ &\rightarrow (a_r C + a_{r-1})C \rightarrow \dots \\ &\rightarrow a_r C^r + \dots + a_1 C + a_0 = N. \end{aligned}$$

O número total de passos que usamos é no máximo $k(B-1) +$

$(k-1)(r-1) + 2r$, assim

$$\begin{aligned}
 \tau(n) &\leq k(B-1) + (k-1)(r-1) + 2r = rk + O\left(\frac{\log n}{(\log \log n)^2}\right) \\
 &= \left\lfloor \frac{\log n}{\log C} \right\rfloor \cdot \frac{\log C}{\log B} + O\left(\frac{\log n}{(\log \log n)^2}\right) \\
 &= \frac{\log n}{\log B} + O\left(\frac{\log n}{(\log \log n)^2}\right) \\
 &= \frac{\log n}{\log \log n - 3 \log \log \log n} + O\left(\frac{\log n}{(\log \log n)^2}\right) \\
 &= \frac{\log n}{\log \log n} + \frac{3 \log n \cdot \log \log \log n}{(\log \log n)^2} + O\left(\frac{\log n}{(\log \log n)^2}\right) < g(n).
 \end{aligned}$$

□

Usando a prova acima, podemos trocar $g(n)$ por $\frac{g(n)}{p-1}$ se tivermos o produto binário e a soma p -ária $\oplus(x_1, x_2, \dots, x_p) = x_1 + \dots + x_p$.

Vamos agora considerar o caso em que temos apenas a operação soma: dado $n \in \mathbb{N}_{>0}$, definimos

$$\tau_+(n) = \min \left\{ m \in \mathbb{N} \left| \begin{array}{l} \exists (s_0, \dots, s_m) \text{ com } s_0 = 1, s_m = n \text{ e, para} \\ \text{cada } l \geq 1, \text{ existem } i, j \text{ com } 0 \leq i, j < l \text{ e} \\ s_l = s_i + s_j \end{array} \right. \right\}$$

Nesse caso podemos provar o seguinte resultado devido a Erdős

Teorema 5.48. $\lim_{n \rightarrow \infty} \frac{\tau_+(n)}{\log_2 n} = 1.$

DEMONSTRAÇÃO: Se (s_0, \dots, s_m) é uma sequência como na definição de $\tau_+(n)$ então $s_j \leq 2^j$ para todo $j \leq m$. Em particular, se $m = \tau_+(n)$, temos $n = s_m \leq 2^m = 2^{\tau_+(n)}$ donde $\tau_+(n) \geq \log_2 n$ para todo $n \in \mathbb{N}_{>0}$. Dado $n \in \mathbb{N}^*$, fixamos $k = k(n) \geq 1$ e começamos gerando os números

$$s_0 = 1, s_1 = 2, s_2 = 3, \dots, s_{2^k-1} = 2^k.$$

Escrevemos agora n na base $B = 2^k$

$$n = a_0 + a_1 B + \dots + a_r B^r$$

onde

$$r = \left\lfloor \frac{\log n}{\log B} \right\rfloor \quad \text{e} \quad 0 \leq a_j \leq B-1, \quad \forall j \leq r.$$

Observemos que os a_j já foram gerados, assim fazemos agora

$$\begin{aligned} s_{2^k} &= a_r + a_r = 2a_r, & s_{2^{k+1}} &= 2a_r + 2a_r = 4a_r, & \dots & & s_{2^k + k - 1} &= 2^k a_r = Ba_r \\ s_{2^k + k} &= Ba_r + a_{r-1}, & s_{2^k + k + 1} &= 2(Ba_r + a_{r-1}), & \dots & & s_{2^k + 2k} &= B^2 a_r + Ba_{r-1} \\ & & & & & & \vdots & \\ s_{2^k - 1 + (k+1)r} &= B^r a_r + B^{r-1} a_{r-1} + \dots + Ba_1 + a_0 = n \end{aligned}$$

Temos

$$2^k - 1 + (k+1)r \leq 2^k + \frac{(k+1)\log n}{k \log 2} = \log_2 n + 2^k + \frac{\log_2 n}{k}.$$

Escolhendo $k = \lceil \log_2(\frac{\log n}{(\log \log n)^2}) \rceil = \lceil \log_2 \log n - 2 \log_2 \log \log n \rceil$, temos que

$$\tau_+(n) \leq (1 + o(1)) \log_2 n$$

o que prova o resultado. \square

Problemas Propostos

5.31. *Mostrar que para todo $n \gg 0$*

$$\sum_{k=1}^n \frac{\sigma(k)}{k} = \frac{\pi^2 n}{6} + O(n \log n).$$

5.32. *Mostrar que para todo $\alpha \leq 0$ e $n \gg 0$*

$$\sum_{k=1}^n \frac{d(k)}{k^\alpha} = \frac{1}{(1-\alpha)} n^{1-\alpha} \log n + \frac{\pi^4}{36} + O(n^{1-\alpha}).$$

5.33. *Mostrar que*

$$\sum_{k=1}^n \frac{d(k)}{k} = \frac{1}{2} \log^2 n + 2 \log n + O(1).$$

5.34. *Prove que, para todo inteiro positivo n , existem exatamente 2^{n-1} vetores (a_1, a_2, \dots, a_k) , onde k, a_1, a_2, \dots, a_k são inteiros positivos e $a_1 + a_2 + \dots + a_k = n$.*

5.35. Seja P_n o conjunto das partições de n . Dada $\pi = (a_1, a_2, \dots, a_r) \in P_n$, definimos $a(\pi) = |\{j \leq r | a_j = 1\}|$, o número de termos iguais a 1 na partição π e $b(\pi) = |\{a_1, a_2, \dots, a_r\}|$, o número de termos distintos na partição π .

Prove que, para todo $n \in \mathbb{N}$, $\sum_{\pi \in P_n} a(\pi) = \sum_{\pi \in P_n} b(\pi)$.

5.36. Prove que, para todo $n \geq 1$,

$$n \cdot p(n) = \sum_{\ell k \leq n} \ell \cdot p(n - \ell k) = \sum_{v=1}^n \sigma(v) p(n - v).$$

(Sugestão: use a função geratriz de $p(n)$.)

5.37 (OIBM1994). Demonstrar que todo número natural $n \leq 2^{1\,000\,000}$ pode ser obtido a partir de 1 fazendo menos do que 1 100 000 de somas, isto é, existe uma sequência finita de números naturais tais que

$$x_0, x_1, \dots, x_k$$

com $k \leq 1\,100\,000$, tais que $x_0 = 1$, $x_k = n$, e para cada $i = 1, 2, \dots, k$, existem r, s , com $0 \leq r, s < i$ e $x_i = x_r + x_s$.

5.38 (OBM2009). Para n inteiro positivo seja $f(n)$ o número de produtos de inteiros maiores que 1 cujo resultado é no máximo n , isto é, $f(n)$ é o número de k -uplas (a_1, a_2, \dots, a_k) onde k é algum natural, $a_i \geq 2$ é inteiro para todo i e $a_1 \cdot a_2 \cdot \dots \cdot a_k \leq n$ (contando a 0-upla vazia $()$, cujo produto dos termos é 1).

Assim, por exemplo, $f(1) = 1$, por causa da 0-upla $()$ e $f(6) = 9$, por causa da 0-upla $()$, das 1-uplas $(2), (3), (4), (5)$ e (6) e das 2-uplas $(2, 2), (2, 3)$ e $(3, 2)$.

Seja $\alpha > 1$ tal que $\sum_{m=1}^{\infty} \frac{1}{m^\alpha} = 2$.

a) Prove que existe uma constante $K > 0$ tal que $f(n) \leq K \cdot n^\alpha$ para todo inteiro positivo n .

b) Prove que existe uma constante $c > 0$ tal que $f(n) \geq c \cdot n^\alpha$ para todo inteiro positivo n .

5.39. Seja $f(n)$ o número de inteiros entre 1 e n^2 que podem ser escritos como um produto de dois inteiros entre 1 e n . Prove que

$$\lim_{n \rightarrow +\infty} \frac{f(n)}{n^2} = 0.$$

Parte II

Tópicos adicionais bacanas

Capítulo 6

Inteiros Algébricos

Neste capítulo, estenderemos o estudo das propriedades aritméticas dos inteiros a domínios mais gerais, como $\mathbb{Z}[i]$ e $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Veremos que entender a aritmética destes anéis, além do interesse próprio, ajuda também a resolver e compreender melhor vários problemas envolvendo números inteiros.

6.1 Inteiros de Gauß e Eisenstein

O anel dos inteiros de Gauß é o subanel de \mathbb{C}

$$\mathbb{Z}[i] \stackrel{\text{def}}{=} \mathbb{Z} + \mathbb{Z} \cdot i = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

O mapa *norma* é definido por

$$\begin{aligned} N: \mathbb{Z}[i] &\rightarrow \mathbb{Z} \\ z = a + bi &\mapsto |z|^2 = z\bar{z} = a^2 + b^2. \end{aligned}$$

Como o valor absoluto em \mathbb{C} é uma função multiplicativa, temos que o mesmo vale para a norma:

$$N(wz) = N(w)N(z) \quad \text{para todo } w, z \in \mathbb{Z}[i].$$

Inteiros de Gauß possuem propriedades aritméticas muito similares às dos inteiros. Por exemplo, podemos definir divisibilidade exatamente da mesma forma:

$$\alpha \mid \beta \iff \text{existe } \gamma \in \mathbb{Z}[i] \text{ tal que } \beta = \alpha\gamma.$$

Assim, por exemplo, temos que $1 + i \mid 5 + 3i$ pois $5 + 3i = (1 + i)(4 - i)$. Note que, da multiplicatividade da norma, temos que $\alpha \mid \beta$ em $\mathbb{Z}[i]$ implica $N(\alpha) \mid N(\beta)$ em \mathbb{Z} .

Podemos definir congruências para inteiros de Gauß:

$$\alpha \equiv \beta \pmod{\gamma} \iff \gamma \mid \alpha - \beta.$$

As mesmas demonstrações do caso \mathbb{Z} mostram que congruências módulo γ definem uma relação de equivalência em $\mathbb{Z}[i]$ compatível com a soma, a subtração e o produto. Podemos portanto formar o anel quociente $\mathbb{Z}[i]/(\gamma)$, cujos elementos são as classes de congruência módulo γ .

Exemplo 6.1. *Mostre que $(1 + i)^{2009} + 1$ é divisível por $2 + i$ em $\mathbb{Z}[i]$.*

SOLUÇÃO: Da “congruência tautológica” $2 + i \equiv 0 \pmod{2 + i}$, temos $i \equiv -2 \pmod{2 + i} \iff 1 + i \equiv -1 \pmod{2 + i}$. Logo $(1 + i)^{2009} \equiv (-1)^{2009} \pmod{2 + i} \iff (1 + i)^{2009} + 1 \equiv 0 \pmod{2 + i}$. \square

Dado $\gamma \in \mathbb{Z}[i]$, $\gamma \neq 0$, quantas são as classes de congruência módulo γ ? Escrevendo $\gamma = a + bi$ com $a, b \in \mathbb{Z}$, o conjunto dos múltiplos de γ em $\mathbb{Z}[i]$ é dado por

$$\mathbb{Z}[i] \cdot \gamma = \mathbb{Z} \cdot \gamma + \mathbb{Z} \cdot i\gamma = \mathbb{Z} \cdot (a + bi) + \mathbb{Z} \cdot (-b + ai)$$

de modo que o número de classes de congruência módulo γ é igual ao índice em \mathbb{Z}^2 do subgrupo gerado pelos vetores (a, b) e $(-b, a)$. Intuitivamente, este índice é igual à razão entre as áreas dos “paralelogramos fundamentais” do reticulado

$$\Lambda \stackrel{\text{def}}{=} \mathbb{Z} \cdot (a, b) + \mathbb{Z} \cdot (-b, a)$$

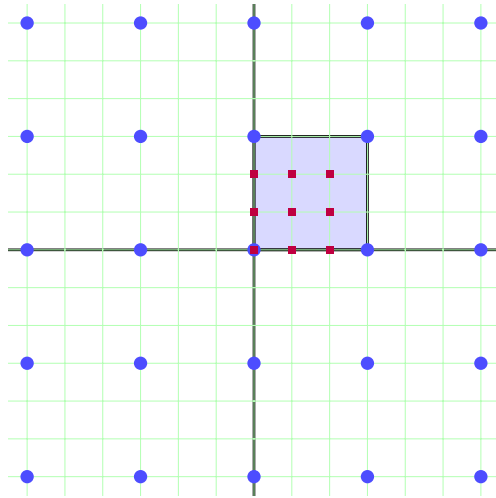
e do reticulado \mathbb{Z}^2 (ver seção 4.2.4), que conta quantas vezes o subreticulado Λ “cabe” dentro de \mathbb{Z}^2 . A razão entre estas áreas é igual ao módulo do determinante

$$\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 = N(\gamma)$$

Por exemplo, para $\gamma = 3$, temos que os $N(3) = 9$ elementos de $\mathbb{Z}[i]$

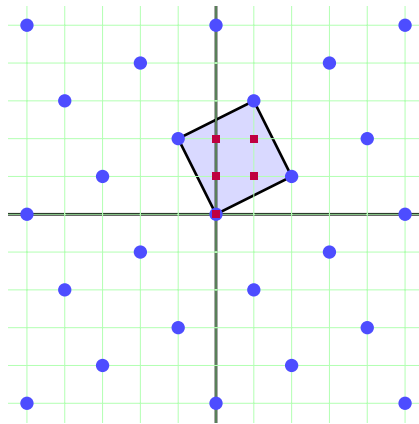
$$\{r + si \mid r, s = 0, 1, 2\}$$

formam um sistema completo de restos módulo $\gamma = 3$. Estes elementos correspondem aos pontos no interior do paralelogramo fundamental de Λ de base $(3, 0)$ e $(0, 3)$, como mostra a figura a seguir:



A próxima figura mostra outro exemplo, em que os múltiplos de $\gamma = 2 + i$ correspondem a 1 em cada $N(2 + i) = 5$ pontos do reticulado $\mathbb{Z}[i]$. Um conjunto de representantes de classe módulo $\gamma = 2 + i$ é

$$\{0, i, 2i, 1 + i, 1 + 2i\}$$



Em geral, temos

Lema 6.2. *Seja $\gamma \in \mathbb{Z}[i]$, $\gamma \neq 0$. Então há exatamente $N(\gamma)$ classes de congruência módulo γ :*

$$\left| \frac{\mathbb{Z}[i]}{(\gamma)} \right| = N(\gamma)$$

DEMONSTRAÇÃO: Da discussão acima, basta mostrarmos que, dados dois vetores (a, b) e (c, d) em \mathbb{Z}^2 , linearmente independentes sobre \mathbb{R} , o índice do subreticulado

$$\Lambda \stackrel{\text{def}}{=} \mathbb{Z} \cdot (a, b) + \mathbb{Z} \cdot (c, d)$$

de \mathbb{Z}^2 é igual ao módulo do determinante

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Inicialmente, provemos o caso particular em que $c = 0$. Neste caso, temos $a \neq 0$ (pois (a, b) e (c, d) são linearmente independentes sobre \mathbb{R}) e

$$R \stackrel{\text{def}}{=} \{(r, s) \in \mathbb{Z}^2 \mid 0 \leq r \leq |a| - 1, 0 \leq s \leq |d| - 1\}$$

é um sistema completo de classes de congruência módulo Λ , que possui exatamente o número desejado $|ad|$ de elementos. De fato:

- TODO ELEMENTO $(x, y) \in \mathbb{Z}^2$ É CONGRUENTE A UM ELEMENTO DE R MÓDULO Λ : podemos dividir x por $a \neq 0$, obtendo quociente q e resto r :

$$x = aq + r, \quad 0 \leq r \leq |a| - 1$$

Assim,

$$(x, y) = q \cdot (a, b) + (r, y - qb) \equiv (r, y - qb) \pmod{\Lambda}$$

Analogamente, dividindo $y - qb$ por d , obtemos resto s com $0 \leq s \leq |d| - 1$ e portanto subtraindo um múltiplo adequado de $(0, d)$ obtemos

$$(x, y) \equiv (r, y - qb) \equiv (r, s) \pmod{\Lambda}$$

como desejado.

- OS ELEMENTOS DE R SÃO DOIS A DOIS NÃO CONGRUENTES ENTRE SI: se (r, s) e (r', s') são dois elementos de R tais que

$$(r, s) \equiv (r', s') \pmod{\Lambda} \iff (r - r', s - s') \in \Lambda = \mathbb{Z} \cdot (a, b) + \mathbb{Z} \cdot (0, d),$$

então existem inteiros u, v tais que

$$(r - r', s - s') = u \cdot (a, b) + v \cdot (0, d) \iff \begin{cases} r - r' = ua \\ s - s' = ub + vd \end{cases}$$

Assim, $a \mid r - r'$, e como $0 \leq r, r' < |a|$ temos que $r = r'$ e portanto $u = 0$. Desta forma, $d \mid s - s'$ e como $0 \leq s, s' < |d|$, temos $s = s'$.

Para obter o caso geral, dentre todos os conjuntos de geradores $\omega = (a, b)$ e $\tau = (c, d)$ de Λ (sobre \mathbb{Z}), escolha um tal que $|c|$ seja mínimo. Se $c \neq 0$, podemos dividir a por c obtendo quociente q e resto r :

$$a = cq + r, \quad 0 \leq r < |c|$$

Mas agora τ e $\omega - q\tau = (r, b - qd)$ é um conjunto de geradores com $|r| < |c|$, o que contraria a minimalidade de $|c|$. Assim, $c = 0$ e caímos no caso anterior. \square

Temos também

Lema 6.3 (Divisão Euclidiana). *Sejam $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$. Então existem inteiros de Gauß $q, r \in \mathbb{Z}[i]$ (quociente e resto da divisão, respectivamente) tais que*

$$\alpha = \beta q + r \quad \text{com} \quad N(r) < N(\beta).$$

DEMONSTRAÇÃO: Escreva $\frac{\alpha}{\beta} = x + yi$ com $x, y \in \mathbb{Q}$. Agora sejam $m, n \in \mathbb{Z}$ os inteiros mais próximos de x e y , ou seja, sejam m e n tais que $|x - m| \leq \frac{1}{2}$ e $|y - n| \leq \frac{1}{2}$. Agora basta tomar $q = m + ni$ e $r = \alpha - \beta q$, pois temos

$$\left| \frac{\alpha}{\beta} - q \right|^2 = |(x - m) + (y - n)i|^2 = (x - m)^2 + (y - n)^2 \leq \frac{1}{4} + \frac{1}{4} < 1.$$

Multiplicando por $|\beta|^2$, temos portanto

$$N(r) = |\alpha - \beta q|^2 < |\beta|^2 = N(\beta).$$

\square

Note que, ao contrário da divisão euclidiana em inteiros, o quociente e o resto na divisão em $\mathbb{Z}[i]$ nem sempre estão unicamente determinados. Por exemplo, dividindo-se $\alpha = 5$ por $\beta = 1 + i$, temos mais de uma possibilidade:

$$\begin{aligned} 5 &= (1 + i)(2 - 2i) + 1 & \text{com} \quad 1 = N(1) < N(1 + i) = 2 \\ 5 &= (1 + i)(2 - 3i) + i & \text{com} \quad 1 = N(i) < N(1 + i) = 2. \end{aligned}$$

Felizmente, poucas provas em \mathbb{Z} utilizaram a unicidade da divisão euclidiana, de modo que os resultados se generalizam para $\mathbb{Z}[i]$ sem maiores problemas.

Nosso próximo passo será obter o teorema fundamental da aritmética para inteiros de Gauß. Inicialmente, precisamos generalizar o conceito de primo.

Definição 6.4. *Seja A um domínio. Dizemos que um elemento $u \in A$ é uma unidade se ele possui inverso multiplicativo em A , isto é, existe $v \in A$ tal que $uv = 1$. O conjunto de todas as unidades de A com a operação de produto é um grupo multiplicativo, o grupo de unidades de A , que denotamos por A^\times .*

Definição 6.5. *Seja A um domínio e seja $\pi \in A$, $\pi \neq 0$ e $\pi \notin A^\times$. Dizemos que π é irredutível se toda fatoração de π em A é trivial, isto é, π não pode ser escrito como produto de dois elementos em $A \setminus A^\times$:*

$$\pi = \alpha\beta \implies \alpha \in A^\times \text{ ou } \beta \in A^\times$$

Dois irredutíveis π_1 e π_2 são ditos associados se eles diferem de uma unidade: $\pi_1 = u\pi_2$ com $u \in A^\times$.

Por exemplo, em $A = \mathbb{Z}$, as unidades são ± 1 e os elementos irredutíveis são os da forma $\pm p$, onde p é um número primo; p e $-p$ são associados. Intuitivamente, elementos associados devem ser vistos não como primos distintos mas como um “único primo” para efeitos de fatoração.

Primos em \mathbb{Z} não necessariamente são irredutíveis em $\mathbb{Z}[i]$. Por exemplo, temos que $5 = (2 + i)(2 - i)$. Por outro lado, $2 + i$ e $2 - i$ possuem norma $N(2 \pm i) = 5$ prima e logo são irredutíveis pelo seguinte

Lema 6.6. 1. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Em particular $u \in \mathbb{Z}[i]^\times \iff N(u) = 1$.

2. Se $\pi \in \mathbb{Z}[i]$ é tal que $N(\pi)$ é um número primo, então π é irredutível.

3. Se $p \in \mathbb{Z}$ é um primo $p \equiv 3 \pmod{4}$ então p é irredutível em $\mathbb{Z}[i]$.

DEMONSTRAÇÃO: É fácil verificar que $\pm 1, \pm i$ são unidades. Por outro lado, se $u \in \mathbb{Z}[i]^\times$, então existe $v \in \mathbb{Z}[i]$ tal que $uv = 1$, logo $N(u)N(v) = 1$. Como $N(u), N(v)$ são inteiros positivos, temos $N(u) = N(v) = 1$.

Escrevendo $u = a + bi$ com $a, b \in \mathbb{Z}$, temos que $N(u) = 1 \iff a^2 + b^2 = 1 \iff (a, b) = (\pm 1, 0)$ ou $(a, b) = (0, \pm 1)$, ou seja, $u \in \{\pm 1, \pm i\}$.

Agora suponha que $N(\pi)$ seja primo. Se $\pi = \alpha\beta$ com $\alpha, \beta \in \mathbb{Z}[i]$ então $N(\pi) = N(\alpha)N(\beta)$. Como $N(\pi)$ é primo, ou $N(\alpha) = 1$ ou $N(\beta) = 1$, ou seja, ou α ou β é uma unidade e portanto π é irredutível.

Finalmente, seja $p \equiv 3 \pmod{4}$. Se p pode ser fatorado como $p = \alpha\beta$ com $\alpha, \beta \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$, temos $p^2 = N(p) = N(\alpha)N(\beta)$. Como α e β não são unidades, $N(\alpha) \neq 1$ e $N(\beta) \neq 1$, logo $N(\alpha) = N(\beta) = p$. Porém, escrevendo $\alpha = a + bi$ com $a, b \in \mathbb{Z}$, temos que $a^2 + b^2 = p \equiv 3 \pmod{4}$, o que é impossível, visto que um quadrado perfeito é congruente a 0 ou a 1 módulo 4, logo $a^2 + b^2$ é congruente a 0, 1 ou 2 módulo 4, mas nunca a 3 módulo 4. \square

Exatamente a mesma demonstração do caso \mathbb{Z} fornece

Teorema 6.7 (Bachet-Bézout). *Sejam α e β dois elementos em $\mathbb{Z}[i]$ primos entre si, isto é, dois elementos cujos únicos divisores comuns são unidades. Então existem $x, y \in \mathbb{Z}[i]$ tais que*

$$\alpha x + \beta y = 1.$$

Exemplo 6.8. *Encontre $x, y \in \mathbb{Z}[i]$ tais que*

$$(20 + 13i) \cdot x + (2 + 3i) \cdot y = 1.$$

SOLUÇÃO: Observe inicialmente que $20 + 13i$ e $2 + 3i$ são primos entre si: se δ é um divisor comum, temos

$$N(\delta) \mid N(20 + 13i) = 569 \quad \text{e} \quad N(\delta) \mid N(2 + 3i) = 13$$

e como $\text{mdc}(569, 13) = 1$ temos $N(\delta) = 1$, ou seja, δ é unidade.

Podemos aplicar agora o algoritmo de Euclides; fazendo as divisões sucessivas, obtemos

$$\begin{aligned} \boxed{20 + 13i} &= \boxed{2 + 3i} \cdot (6 - 3i) + \boxed{-1 + i} \\ \boxed{2 + 3i} &= \boxed{-1 + i} \cdot (-2i) + \boxed{i} \end{aligned}$$

Assim,

$$\begin{aligned}
 [i] &= [2 + 3i] - [-1 + i] \cdot (-2i) \\
 &= [2 + 3i] - ([20 + 13i] - [2 + 3i] \cdot (6 - 3i)) \cdot (-2i) \\
 &= [20 + 13i] \cdot (2i) + [2 + 3i] \cdot (-5 - 12i)
 \end{aligned}$$

e dividindo por i (que é uma unidade), obtemos finalmente

$$[20 + 13i] \cdot 2 + [2 + 3i] \cdot (-12 + 5i) = 1$$

de modo que podemos tomar $x = 2$ e $y = -12 + 5i$. \square

Note que, como no caso de \mathbb{Z} , o teorema de Bachet-Bézout implica

Lema 6.9. *Seja $\pi \in \mathbb{Z}[i]$ um elemento irredutível. Então*

$$\pi \mid \alpha\beta \implies \pi \mid \alpha \quad \text{ou} \quad \pi \mid \beta$$

para $\alpha, \beta \in \mathbb{Z}[i]$.

Como “corolário”, obtemos a fatoração única:

Teorema 6.10 (Fatoração única). *Qualquer elemento $\alpha \neq 0$ de $\mathbb{Z}[i]$ admite uma fatoração*

$$\alpha = \pi_1 \pi_2 \dots \pi_n$$

em elementos irredutíveis π_i . Tal fatoração é única a menos da ordem dos fatores e de multiplicação por unidades (isto é, a menos de associa-

DEMONSTRAÇÃO: A prova da unicidade da fatoração é idêntica à dos inteiros, utilizando o lema anterior. A prova da existência da fatoração é também similar, mas agora utilizamos indução em $N(\alpha)$: se $N(\alpha) = 2$ (base) então α é irredutível (ver lema) e se α é irredutível, não há nada a fazer; caso contrário, existe uma fatoração $\alpha = \beta\gamma$ onde nem β nem γ são unidades, isto é, $N(\beta) \neq 1$ e $N(\gamma) \neq 1$. Como $N(\alpha) = N(\beta)N(\gamma)$, temos que β e γ possuem norma estritamente menor do que $N(\alpha)$. Por hipótese de indução, β e γ podem ser fatorados em irredutíveis e, combinando as duas fatorações, obtemos uma fatoração de α . \square

Exemplo 6.11. *Escreva 50 e $6 + 7i$ como produto de irredutíveis em $\mathbb{Z}[i]$.*

SOLUÇÃO: Como $50 = 2 \cdot 5^2$ e já sabemos fatorar $5 = (2 + i)(2 - i)$ em irredutíveis, basta agora fatorar 2. Temos que $2 = (1 + i)(1 - i) = i(1 - i)^2$ e $1 - i$ é irredutível pois sua norma $N(1 - i) = 2$ é prima. Logo $50 = i(1 - i)^2(2 + i)^2(2 - i)^2$ é a fatoração em irredutíveis de 50.

Se π é um fator irredutível de $6 + 7i$, temos que $N(\pi) \mid N(6 + 7i) = 85 = 5 \cdot 17$. Como $5 = (2 + i)(2 - i)$ e $17 = (4 + i)(4 - i)$ são as fatorações em irredutíveis de 5 e 17 em $\mathbb{Z}[i]$ e como $\pi \mid N(\pi) = \pi\bar{\pi}$, temos que $\pi \mid 85 \implies \pi \in \{2 \pm i, 4 \pm i\}$. Testando, obtemos que $2 - i$ e $4 - i$ dividem $6 + 7i$, de modo que $6 + 7i = i(2 - i)(4 - i)$ é a fatoração procurada. \square

Agora podemos novamente provar que todo primo da forma $4k + 1$ é soma de dois quadrados (c.f. seção 4.2.1 e teorema 4.19).

Teorema 6.12. *Qualquer primo $p \equiv 1 \pmod{4}$ fatora-se como $p = (a + bi)(a - bi)$ com $a, b \in \mathbb{Z}$. Em particular, p pode ser escrito como soma de dois quadrados perfeitos em \mathbb{Z} .*

DEMONSTRAÇÃO: Como $p \equiv 1 \pmod{4}$, temos $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, ou seja, existe $x \in \mathbb{Z}$ tal que $x^2 + 1 \equiv 0 \pmod{p}$. Agora suponha que p seja irredutível em $\mathbb{Z}[i]$. Então, de $p \mid x^2 + 1 = (x + i)(x - i)$, temos que $p \mid x + i$ ou $p \mid x - i$. Mas isto é impossível: um múltiplo de p em $\mathbb{Z}[i]$ é da forma $p(a + bi) = pa + pbi$ com $a, b \in \mathbb{Z}$, isto é, possui parte real e imaginária múltiplos de p , o que não é o caso para $x \pm i$.

Assim, temos que p é redutível e existem $\beta, \gamma \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ tais que $p = \beta\gamma$. Tomando normas, temos $p^2 = N(\beta)N(\gamma) \implies N(\beta) = N(\gamma) = p$ já que $\beta, \gamma \notin \mathbb{Z}[i]^\times$. Escrevendo $\beta = a + bi$ com $a, b \in \mathbb{Z}$, temos portanto que $p = N(\beta) = a^2 + b^2$, donde obtemos a fatoração $p = (a + bi)(a - bi)$ desejada. Note que $a \pm bi$ são ambos irredutíveis pois possuem norma prima. \square

Como $2 = i(1 - i)^2$, combinando os resultados anteriores temos uma caracterização completa dos irredutíveis em $\mathbb{Z}[i]$:

Teorema 6.13. *Os elementos irredutíveis de $\mathbb{Z}[i]$ são, a menos de associados,*

- *números primos $p \in \mathbb{Z}$ tais que $p \equiv 3 \pmod{4}$;*
- *números da forma $a + bi$ onde $N(a + bi)$ é primo (necessariamente igual a 2 ou congruente a 1 módulo 4).*

Podemos utilizar ainda inteiros de Gauß na resolução de problemas sobre \mathbb{Z} :

Exemplo 6.14. *Resolva a equação diofantina $y^3 = x^2 + 4$.*

SOLUÇÃO: Temos a fatoração $y^3 = (x + 2i)(x - 2i)$ em $\mathbb{Z}[i]$ e queremos concluir a partir dela que $x + 2i$ e $x - 2i$ são cubos perfeitos em $\mathbb{Z}[i]$. Observe primeiramente que se π é um irredutível que divide $x + 2i$ e $x - 2i$, então π deve dividir a diferença $4i = -i(1 - i)^4$, ou seja, π é associado a $1 - i$. Assim, podemos escrever

$$\begin{aligned} x + 2i &= u \cdot \pi_1^{e_1} \cdot \pi_2^{e_2} \cdot \dots \cdot \pi_n^{e_n} \\ x - 2i &= \bar{u} \cdot \bar{\pi}_1^{e_1} \cdot \bar{\pi}_2^{e_2} \cdot \dots \cdot \bar{\pi}_n^{e_n} \end{aligned}$$

onde $u \in \mathbb{Z}[i]^\times$ e os π_j são irredutíveis dois a dois não associados e $\pi_1 = 1 - i$. Note que $\bar{\pi}_j$ também são irredutíveis dois a dois não associados e que, com exceção de $j = 1$, π_j não é associado a nenhum $\bar{\pi}_k$. Como $(x + 2i)(x - 2i) = y^3$, temos pela fatoração única que π_j e $\bar{\pi}_j$ são os irredutíveis que aparecem na fatoração de y e que portanto $3 \mid e_j$, com a possível exceção de $j = 1$. Mas como $\bar{\pi}_1$ e π_1 são associados, temos que $2e_1$ deve ser divisível por 3, logo $3 \mid e_1$ também. Por outro lado, toda unidade em $\mathbb{Z}[i]$ é um cubo perfeito em $\mathbb{Z}[i]$, assim concluímos que $x + 2i$ e $x - 2i$ são cubos perfeitos em $\mathbb{Z}[i]$.

Agora escrevendo $x + 2i = (a + bi)^3$ com $a, b \in \mathbb{Z}$ e expandindo, obtemos $x = a^3 - 3ab^2$ e $2 = 3a^2b - b^3$. Da última equação, temos $b \mid 2$, e testando as possibilidades obtemos as soluções $(a, b) = (\pm 1, -2)$ e $(a, b) = (\pm 1, 1)$, ou seja, $(x, y) = (\pm 11, 5)$ ou $(x, y) = (\pm 2, 2)$. \square

Outros resultados sobre \mathbb{Z} também são facilmente estendidos para $\mathbb{Z}[i]$. Por exemplo, dados $\mu, \nu \in \mathbb{Z}[i]$ não nulos e primos entre si, o mapa

natural de anéis

$$\frac{\mathbb{Z}[i]}{(\mu\nu)} \rightarrow \frac{\mathbb{Z}[i]}{(\mu)} \times \frac{\mathbb{Z}[i]}{(\nu)}$$

$$\gamma \bmod \mu\nu \mapsto (\gamma \bmod \mu, \gamma \bmod \nu)$$

é injetor, pois se $\gamma \bmod \mu\nu$ está no kernel, então $\mu \mid \gamma$ e $\nu \mid \gamma$, logo $\mu\nu \mid \gamma$ já que μ, ν são primos entre si (utilizando a fatoração única em $\mathbb{Z}[i]$). Como ambos os anéis possuem a mesma quantidade de elementos $N(\mu\nu) = N(\mu)N(\nu)$, este mapa é um isomorfismo e assim como no caso \mathbb{Z} obtemos o teorema chinês dos restos para inteiros de Gauß! Igualmente fácil é obter o

Teorema 6.15. *Seja $\mu \in \mathbb{Z}[i]$ não nulo e seja*

$$\xi(\mu) = \left| \left(\frac{\mathbb{Z}[i]}{(\mu)} \right)^\times \right| = \text{número de inversíveis módulo } \mu$$

Note que por Bachet-Bézout $\xi(\mu)$ é a quantidade de elementos módulo μ que são primos com μ .

1. (Euler-Fermat-Gauß) *Se $\alpha, \mu \in \mathbb{Z}[i]$ são primos entre si então*

$$\alpha^{\xi(\mu)} \equiv 1 \pmod{\mu}.$$

2. *A função ξ é multiplicativa: se $\mu, \nu \in \mathbb{Z}[i]$ são primos entre si, então $\xi(\mu\nu) = \xi(\mu)\xi(\nu)$.*

3. *Se $\pi \in \mathbb{Z}[i]$ é irredutível, então*

$$\xi(\pi^e) = N(\pi)^e \left(1 - \frac{1}{N(\pi)} \right)$$

Portanto, para $\mu \neq 0$ em $\mathbb{Z}[i]$, temos

$$\xi(\mu) = N(\mu) \prod_{\substack{\pi \mid \mu \\ \pi \text{ irredutível}}} \left(1 - \frac{1}{N(\pi)} \right)$$

DEMONSTRAÇÃO: As provas de 1 e 2 são análogas ao caso \mathbb{Z} : para 1, podemos tanto copiar a demonstração do teorema de Euler-Fermat

como aplicar diretamente o teorema de Lagrange, enquanto que 2 segue olhando para o grupo de unidades no isomorfismo do teorema chinês dos restos acima. Finalmente, para mostrar 3, note que temos um morfismo natural de anéis

$$\begin{aligned} \frac{\mathbb{Z}[i]}{(\pi^e)} &\rightarrow \frac{\mathbb{Z}[i]}{(\pi)} \\ \gamma \bmod \pi^e &\mapsto \gamma \bmod \pi \end{aligned}$$

que é claramente sobrejetor. Além disso, como π é irredutível, o kernel deste morfismo, o conjunto dos múltiplos de π , é justamente o conjunto dos elementos que não são primos com π^e . Assim, como $N(\pi) = |\mathbb{Z}[i]/(\pi)|$, a razão entre a quantidade de elementos não inversíveis módulo π^e e o total de elementos em $\mathbb{Z}[i]/(\pi^e)$ é $1/N(\pi)$, logo

$$\frac{\xi(\pi^e)}{|\mathbb{Z}[i]/(\pi^e)|} = 1 - \frac{1}{N(\pi)} \iff \frac{\xi(\pi^e)}{N(\pi^e)} = 1 - \frac{1}{N(\pi)}$$

e o resultado segue. \square

Outro anel com propriedades aritméticas interessantes é o *anel de inteiros de Eisenstein*. Seja $\omega = \frac{-1+i\sqrt{3}}{2}$, que é uma raiz cúbica da unidade. O anel em questão é definido como o subanel dos complexos dado por

$$\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}\}.$$

Definimos a *norma* de um inteiro de Eisenstein via

$$\begin{aligned} N: \mathbb{Z}[\omega] &\rightarrow \mathbb{Z} \\ z = a + b\omega &\mapsto |z|^2 = z\bar{z} = a^2 - ab + b^2 \end{aligned}$$

(utilize o fato de que ω e $\omega^2 = \bar{\omega}$ são as raízes da equação $x^2 + x + 1 = 0$). Novamente, como o valor absoluto em \mathbb{C} é uma função multiplicativa, temos que a norma também é multiplicativa: $N(wz) = N(w)N(z)$ para todo $w, z \in \mathbb{Z}[\omega]$.

Do mesmo modo, temos a fatoração única em irredutíveis de $\mathbb{Z}[\omega]$. As provas são idênticas aos casos anteriores \mathbb{Z} e $\mathbb{Z}[i]$, graças ao

Lema 6.16 (Divisão Euclidiana). *Sejam $\alpha, \beta \in \mathbb{Z}[\omega]$ com $\beta \neq 0$. Então existem $q, r \in \mathbb{Z}[\omega]$ tais que*

$$\alpha = \beta q + r \quad \text{com} \quad N(r) < N(\beta).$$

DEMONSTRAÇÃO: Como $1, \omega$ formam uma base do corpo $\mathbb{Q}(\omega) = \mathbb{Q} + \mathbb{Q}\omega$ sobre \mathbb{Q} , podemos escrever $\frac{\alpha}{\beta} = x + y\omega$ com $x, y \in \mathbb{Q}$. Sejam m e n os inteiros mais próximos de x e y respectivamente, de modo que $|x - m| \leq \frac{1}{2}$ e $|y - n| \leq \frac{1}{2}$. Tome $q = m + n\omega$ e $r = \alpha - \beta q$. Pela desigualdade triangular temos

$$\left| \frac{\alpha}{\beta} - q \right| = |(x - m) + (y - n)\omega| \leq |x - m| + |y - n| \leq \frac{1}{2} + \frac{1}{2} = 1.$$

Note que como $1, \omega$ são linearmente independentes sobre \mathbb{R} , a primeira desigualdade é estrita, a menos que $x - m = 0$ ou $y - n = 0$, mas nestes dois casos a segunda desigualdade é estrita. Assim, multiplicando por $|\beta|$, obtemos $|r| < |\beta| \implies N(r) < N(\beta)$. \square

Deixamos como exercício ao leitor verificar a seguinte caracterização de unidades e irredutíveis em $\mathbb{Z}[\omega]$:

Teorema 6.17. 1. $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$.

2. Os irredutíveis em $\mathbb{Z}[\omega]$ são da forma

(a) $p \in \mathbb{Z}$ primo tal que $p \equiv 5 \pmod{6}$;

(b) $a + b\omega$ onde $N(a + b\omega)$ é um número primo (necessariamente 3 ou da forma $6k + 1$).

Vejamos uma aplicação:

Exemplo 6.18. Resolver a equação diofantina $y^5 = x^2 + x + 1$.

SOLUÇÃO: Como $y^5 = (x - \omega)(x - \omega^2) = N(x - \omega)$, é natural trabalhar em $\mathbb{Z}[\omega]$. Seja $\delta \in \mathbb{Z}[\omega]$ tal que $\delta \mid (x - \omega)$ e $\delta \mid (x - \omega^2)$. Então $\delta \mid (\omega - \omega^2)$; como ω é unidade e $1 - \omega$ é irredutível ($N(1 - \omega) = 3$ é primo), temos que $x - \omega$ e $x - \omega^2$ têm no máximo $1 - \omega$ como fator comum. Como o produto de $x - \omega$ e $x - \omega^2$ é uma quinta potência e os elementos de $\mathbb{Z}[\omega]^\times$

também são quintas potências perfeitas, podemos concluir utilizando a fatoração única que $x - \omega = (1 - \omega)^k \alpha^5$ com $\alpha \in \mathbb{Z}[\omega]$. Tomando normas, temos $y^5 = 3^k N(\alpha)^5$, e assim k também é um múltiplo de 5. Concluimos portanto que $x - \omega = \beta^5$ para algum $\beta \in \mathbb{Z}[\omega]$.

Agora escrevendo $\beta = m + n\omega$, $m, n \in \mathbb{Z}$ e usando $\omega^2 = -1 - \omega$, obtemos que $x - \omega = \beta^5$ é igual a

$$(m^5 - 10m^3n^2 + 10m^2n^3 - n^5) + (5m^4n - 10m^3n^2 + 5mn^4 - n^5)\omega.$$

Portanto $n(5m^4 - 10m^3n + 5mn^3 - n^4) = -1$ e assim $n = \pm 1$; verificando as possibilidades, obtemos $(m, n) = (0, 1)$ ou $(m, n) = (1, 1)$, que correspondem às soluções $(x, y) = (-1, 1)$ e $(x, y) = (0, 1)$. \square

Observação 6.19. *Seja d um inteiro livre de quadrados. Considere os subanéis de \mathbb{C} (ver próxima seção)*

$$\mathbb{Z}[\sqrt{d}] \stackrel{\text{def}}{=} \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

se $d \equiv 2$ ou $3 \pmod{4}$ e

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \stackrel{\text{def}}{=} \mathbb{Z} + \mathbb{Z} \cdot \frac{1+\sqrt{d}}{2} = \left\{a + b \cdot \frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\right\}$$

se $d \equiv 1 \pmod{4}$.

É fácil modificar as provas acima para mostrar que também temos divisão euclidiana para estes anéis se $d = -1, -2, -3, -7, -11, 2, 5$, onde agora a comparação do “tamanho” entre β e o resto r é feita utilizando-se o módulo da função norma, definida por

$$N(a + b\sqrt{d}) \stackrel{\text{def}}{=} (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d$$

se $d \equiv 2$ ou $3 \pmod{4}$ e

$$N\left(a + b \cdot \frac{1+\sqrt{d}}{2}\right) \stackrel{\text{def}}{=} \left(a + b \cdot \frac{1+\sqrt{d}}{2}\right)\left(a + b \cdot \frac{1-\sqrt{d}}{2}\right) = a^2 + ab + b^2 \cdot \frac{1-d}{4}$$

se $d \equiv 1 \pmod{4}$. No jargão da Álgebra, dizemos que estes anéis são domínios euclidianos. Sabe-se (ver [87]) que estes anéis são domínios euclidianos com o módulo da função norma se, e só se,

$$d = -1, -2, -3, -7, -11,$$

$$2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 \text{ ou } 73$$

6.2 Extensões Quadráticas e Ciclotômicas

Seja d um inteiro que não é um quadrado perfeito. O conjunto

$$\mathbb{Z}[\sqrt{d}] \stackrel{\text{def}}{=} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

é um subanel de \mathbb{C} : este conjunto é claramente fechado por soma e subtração e também por produto, já que

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}.$$

Como no caso dos inteiros de Gauß e Eisenstein, podemos tentar estender o estudo de propriedades aritméticas a este anel também. Alguns conceitos se estendem de forma imediata. Por exemplo, podemos definir divisibilidade da maneira usual: dados $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$,

$$\alpha \mid \beta \iff \text{existe } \gamma \in \mathbb{Z}[\sqrt{d}] \text{ tal que } \beta = \alpha\gamma.$$

Da mesma forma, definimos a relação de congruência

$$\alpha \equiv \beta \pmod{\delta} \iff \delta \mid \alpha - \beta$$

e o anel quociente $\mathbb{Z}[\sqrt{d}]/(\delta)$, cujos elementos são as classes de congruência módulo δ . Por exemplo, temos a seguinte generalização do pequeno teorema de Fermat:

Teorema 6.20. *Seja $p \in \mathbb{Z}$ um número primo tal que $p \neq 2$ e $p \nmid d$. Para todo elemento $\alpha \in \mathbb{Z}[\sqrt{d}]$,*

$$\alpha^{p^2} \equiv \alpha \pmod{p}.$$

DEMONSTRAÇÃO: Escrevendo $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$, temos (c.f. proposição 1.38, o “sonho de todo estudante”)

$$\alpha^p = (a + b\sqrt{d})^p = \sum_{0 \leq i \leq p} \binom{p}{i} a^{p-i} (b\sqrt{d})^i \equiv a^p + b^p (\sqrt{d})^p \pmod{p}$$

pois $p \mid \binom{p}{i}$ para $i = 1, 2, \dots, p-1$. Porém, pelo pequeno teorema de Fermat, $p \mid a^p - a$ e $p \mid b^p - b$ em \mathbb{Z} (e portanto em $\mathbb{Z}[\sqrt{d}]$ também). Assim,

$$\alpha^p \equiv a + b \cdot (\sqrt{d})^p \pmod{p}.$$

Elevando novamente a p , obtemos portanto

$$\alpha^{p^2} \equiv a + b \cdot (d^{p-1})^{(p+1)/2} \sqrt{d} \pmod{p}.$$

Como $p \neq 2$ e $p \nmid d$, temos que $(p+1)/2$ é inteiro e pelo pequeno teorema de Fermat $(d^{p-1})^{(p+1)/2} \equiv 1 \pmod{p}$. Assim, $\alpha^{p^2} \equiv \alpha \pmod{p}$. \square

Se n é um inteiro positivo, temos que o anel $\mathbb{Z}[\sqrt{d}]/(n)$ possui n^2 elementos:

$$\mathbb{Z}[\sqrt{d}]/(n) = \left\{ a + b\sqrt{d} \mid a, b = 0, 1, 2, \dots, n-1 \right\}.$$

A seguinte proposição fornece um critério para decidir quando este anel é um corpo:

Proposição 6.21. *Seja p um primo tal que $p \nmid d$. Então $\mathbb{Z}[\sqrt{d}]/(p)$ é um corpo (com p^2 elementos) se, e somente se, $\left(\frac{d}{p}\right) = -1$.*

DEMONSTRAÇÃO: Suponha inicialmente que $\left(\frac{d}{p}\right) = -1$ e seja $a + b\sqrt{d} \not\equiv 0 \pmod{p}$, $a, b \in \mathbb{Z}$, ou seja, ou a ou b não é divisível por p . Temos que $a^2 - b^2d$ é invertível módulo p : isto é claro se $b \equiv 0 \pmod{p}$ (pois neste caso $a \not\equiv 0 \pmod{p}$); e se $b \not\equiv 0 \pmod{p}$ então $a^2 - b^2d \equiv 0 \pmod{p} \implies \left(\frac{a}{b}\right)^2 \equiv d \pmod{p}$, o que contradiz $\left(\frac{d}{p}\right) = -1$. Logo

$$(a + b\sqrt{d}) \cdot \frac{a - b\sqrt{d}}{a^2 - b^2d} \equiv 1 \pmod{p}$$

mostra que $a + b\sqrt{d}$ também é invertível módulo p , logo $\mathbb{Z}[\sqrt{d}]/(p)$ é corpo.

Reciprocamente, se $\left(\frac{d}{p}\right) = 1$ e $a^2 \equiv d \pmod{p}$, $a \in \mathbb{Z}$, então $a \pm \sqrt{d} \pmod{p}$ seriam não nulos em $\mathbb{Z}[\sqrt{d}]/(p)$ mas não teriam inversos pois

$$(a + \sqrt{d})(a - \sqrt{d}) \equiv 0 \pmod{p}.$$

\square

Quando $d \equiv 1 \pmod{4}$, podemos definir também o subanel de \mathbb{C}

$$\mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right] \stackrel{\text{def}}{=} \left\{ a + b \cdot \frac{1 + \sqrt{d}}{2} \mid a, b \in \mathbb{Z} \right\}$$

que é claramente fechado por soma e subtração, mas também produto: note que $\theta = \frac{1+\sqrt{d}}{2}$ satisfaz a equação mônica com coeficientes inteiros

$$\theta^2 - \theta + \frac{1-d}{4} = 0 \iff \theta^2 = \theta + \frac{d-1}{4}$$

de modo que

$$(a_1 + b_1\theta)(a_2 + b_2\theta) = \left(a_1a_2 + b_1b_2 \cdot \frac{d-1}{4}\right) + (a_1b_2 + a_2b_1 + b_1b_2) \cdot \theta.$$

Exemplo 6.22. *Seja F_n o n -ésimo número de Fibonacci e $p \neq 5$ um número primo. Mostre que $p \mid F_{p^2-1}$.*

SOLUÇÃO: O resultado é claro para $p = 2$, logo podemos assumir que $p \neq 2, 5$. Sejam $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2} = 1 - \alpha$ as raízes do polinômio $x^2 - x - 1$. Trabalhando no anel $\mathbb{Z}[\alpha]$, basta mostrar que

$$F_{p^2-1} = \frac{\alpha^{p^2-1} - \beta^{p^2-1}}{\alpha - \beta} \equiv 0 \pmod{p}$$

pois se F_{p^2-1} é múltiplo de p em $\mathbb{Z}[\alpha]$, então F_{p^2-1} é múltiplo de p em \mathbb{Z} : se $a, b \in \mathbb{Z}$ são tais que $F_{p^2-1} = p \cdot (a + b\alpha)$, então $b = 0$ e $F_{p^2-1} = pa$ pois 1 e α são linearmente independentes sobre \mathbb{Q} (i.e., $\alpha \notin \mathbb{Q}$). Note ainda que $\alpha - \beta = \sqrt{5}$ é invertível módulo p pois $(\sqrt{5})^{2(p-1)} \equiv 1 \pmod{p}$ pelo pequeno teorema de Fermat. Assim, o problema se resume a mostrar que

$$\alpha^{p^2-1} \equiv \beta^{p^2-1} \pmod{p}.$$

Mas como na demonstração do teorema anterior, aplicando o “sonho de todo estudante” e o pequeno teorema de Fermat ($p \neq 2, 5$ por hipótese), obtemos

$$\alpha^{p^2} \equiv \frac{1^{p^2} + (\sqrt{5})^{p^2}}{2^{p^2}} \pmod{p} \iff \alpha^{p^2} \equiv \frac{1 + \sqrt{5}}{2} = \alpha \pmod{p}.$$

Como α é invertível em $\mathbb{Z}[\alpha]$ ($\alpha\beta = -1$), obtemos portanto $\alpha^{p^2-1} \equiv 1 \pmod{p}$. Analogamente, $\beta^{p^2-1} \equiv 1 \pmod{p}$, o que completa a prova. \square

Um outro subanel de \mathbb{C} que é particularmente interessante do ponto de vista aritmético é o *anel de inteiros ciclotômicos*. Seja p um primo e $\zeta_p = e^{2\pi i/p}$, uma p -ésima raiz primitiva da unidade. Definimos

$$\mathbb{Z}[\zeta_p] \stackrel{\text{def}}{=} \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2} \mid a_0, a_1, \dots, a_{p-2} \in \mathbb{Z}\}.$$

Por exemplo, quando $p = 3$, temos que o anel acima é o anel de inteiros de Eisenstein.

O conjunto $\mathbb{Z}[\zeta_p]$ é claramente fechado por soma e subtração; para mostrar que ele também é fechado por produto, basta utilizar a relação

$$\begin{aligned} \zeta_p^{p-1} + \zeta_p^{p-2} + \zeta_p^{p-3} + \cdots + 1 &= 0 \\ \implies \zeta_p^{p-1+j} &= -\zeta_p^{p-2+j} - \zeta_p^{p-3+j} - \cdots - \zeta_p^j \quad (j \geq 0) \end{aligned}$$

que permite expressar qualquer potência de ζ_p de expoente maior ou igual a $p - 1$ em função de potências com expoente menor.

Vamos mostrar uma aplicação dos inteiros ciclotômicos fornecendo uma nova demonstração da lei de reciprocidade quadrática. O caso $\left(\frac{2}{p}\right)$ com p primo ímpar será o primeiro a ser analisado. Para isso, denotemos por ζ_8 uma raiz oitava primitiva da unidade, isto é, ζ_8 é raiz do polinômio $x^4 + 1 = 0$, e portanto $\zeta_8^2 + \zeta_8^{-2} = 0$. Se denotamos por $\omega = \zeta_8 + \zeta_8^{-1}$, segue que $\omega^2 = 2$. Pelo “sonho de todo estudante” sabemos que

$$\omega^p = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod{p} \equiv \begin{cases} \zeta_8 + \zeta_8^{-1} & \text{se } p \equiv \pm 1 \pmod{8} \\ -\zeta_8 - \zeta_8^{-1} & \text{se } p \equiv \pm 3 \pmod{8}, \end{cases}$$

e como ω é invertível módulo p , pois 2 é invertível, segue que $\omega^{p-1} \equiv (-1)^{(p^2-1)/8} \pmod{p}$. Portanto

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} = \omega^{p-1} \equiv (-1)^{(p^2-1)/8} \pmod{p},$$

donde concluímos que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Observe que neste caso ω é uma raiz quadrada de 2. Este é o ponto chave da demonstração do caso geral, isto é, determinar “explicitamente” uma fórmula para a raiz quadrada de $\pm p$:

Proposição 6.23 (Soma de Gauß). *Seja p um primo e seja ζ_p uma p -ésima raiz primitiva da unidade. Seja*

$$S = \sum_{a \in \mathbb{Z}/(p)} \left(\frac{a}{p} \right) \zeta_p^a.$$

Então

$$S^2 = (-1)^{(p-1)/2} p.$$

DEMONSTRAÇÃO: Observe que

$$\begin{aligned} S^2 &= \sum_{a \in \mathbb{Z}/(p)} \left(\frac{a}{p} \right) \zeta_p^a \cdot \sum_{b \in \mathbb{Z}/(p)} \left(\frac{b}{p} \right) \zeta_p^b = \sum_{a, b \in \mathbb{Z}/(p)} \left(\frac{ab}{p} \right) \zeta_p^{a+b} \\ &= \sum_{n \in \mathbb{Z}/(p)} \sum_{a \in \mathbb{Z}/(p)} \left(\frac{a(n-a)}{p} \right) \zeta_p^n \\ &= \sum_{n \in \mathbb{Z}/(p)} \zeta_p^n \cdot \sum_{a \in (\mathbb{Z}/(p))^\times} \left(\frac{a^2}{p} \right) \left(\frac{na^{-1} - 1}{p} \right) \\ &= \sum_{n \in \mathbb{Z}/(p)} \zeta_p^n \cdot \sum_{a \in (\mathbb{Z}/(p))^\times} \left(\frac{na^{-1} - 1}{p} \right). \end{aligned}$$

Para $n \neq \bar{0}$ fixo, $na^{-1} = nb^{-1} \iff a = b$, assim a expressão na^{-1} percorre todos os elementos de $(\mathbb{Z}/(p))^\times$ quando a percorre $(\mathbb{Z}/(p))^\times$. Logo, como há o mesmo número de resíduos e não resíduos quadráticos, temos que, para $n \neq \bar{0}$,

$$\sum_{a \in (\mathbb{Z}/(p))^\times} \left(\frac{na^{-1} - 1}{p} \right) = -\left(\frac{-1}{p} \right) + \sum_{a \in \mathbb{Z}/(p)} \left(\frac{a}{p} \right) = -\left(\frac{-1}{p} \right)$$

enquanto que para $n = \bar{0}$ temos

$$\sum_{a \in (\mathbb{Z}/(p))^\times} \left(\frac{na^{-1} - 1}{p} \right) = \sum_{a \in (\mathbb{Z}/(p))^\times} \left(\frac{-1}{p} \right) = (p-1) \left(\frac{-1}{p} \right).$$

Portanto, como $\zeta_p^{p-1} + \zeta_p^{p-2} + \zeta_p^{p-3} + \dots + 1 = 0$, temos

$$S^2 = (p-1) \left(\frac{-1}{p} \right) - \left(\frac{-1}{p} \right) \sum_{n \in (\mathbb{Z}/(p))^\times} \zeta_p^n = p \left(\frac{-1}{p} \right) = p \cdot (-1)^{\frac{p-1}{2}}.$$

□

Agora podemos completar a demonstração da lei de reciprocidade quadrática. Sejam p, q dois primos ímpares distintos. Módulo q , pelo critério de Euler e pela proposição anterior temos

$$\begin{aligned} \left(\frac{p \cdot (-1)^{\frac{p-1}{2}}}{q} \right) &\equiv (p \cdot (-1)^{\frac{p-1}{2}})^{\frac{q-1}{2}} \pmod{q} \\ \iff \left(\frac{p}{q} \right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} &\equiv S^{q-1} \pmod{q}. \end{aligned}$$

Assim, basta calcular $S^{q-1} \pmod{q}$. Pelo “sonho de todo estudante”, temos

$$\begin{aligned} S^q &\equiv \sum_{a \in \mathbb{Z}/(p)} \left(\frac{a}{p} \right)^q \zeta_p^{aq} = \sum_{a \in \mathbb{Z}/(p)} \left(\frac{a}{p} \right) \zeta_p^{aq} \\ &= \left(\frac{q}{p} \right) \sum_{a \in \mathbb{Z}/(p)} \left(\frac{aq}{p} \right) \zeta_p^{aq} \\ &= \left(\frac{q}{p} \right) S \pmod{q}, \end{aligned}$$

já que $aq \pmod{p}$ percorre um sistema completo de resíduos módulo p (q é invertível módulo p). Como $S^2 = \pm p$, temos que S é invertível módulo q e portanto

$$S^q \equiv \left(\frac{q}{p} \right) S \pmod{q} \iff S^{q-1} \equiv \left(\frac{q}{p} \right) \pmod{q}.$$

Substituindo na primeira expressão temos

$$\begin{aligned} \left(\frac{p}{q} \right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} &\equiv \left(\frac{q}{p} \right) \pmod{q} \\ \iff \left(\frac{p}{q} \right) \left(\frac{q}{p} \right) &\equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \pmod{q} \end{aligned}$$

o que completa a demonstração, já que ambos os lados da expressão são ± 1 , logo a congruência acima é uma igualdade.

A proposição anterior também é importante para a demonstração do seguinte resultado:

Teorema 6.24 (Pólya-Vinogradov). *Seja p primo. Para quaisquer $0 \leq m \leq m+n < p$, temos*

$$\left| \sum_{k=m}^{m+n} \left(\frac{k}{p} \right) \right| < \sqrt{p} \log p.$$

DEMONSTRAÇÃO: Como $\sum_{k=0}^{p-1} \left(\frac{k}{p} \right) = 0$ e, para $0 \leq s < p$ e $-p < j < p$,

$$\sum_{s=0}^{p-1} e^{2js\pi i/p} = \begin{cases} p & \text{se } j = 0 \text{ ou } s = 0 \\ 0 & \text{caso contrário} \end{cases}$$

temos

$$\begin{aligned} \sum_{k=m}^{m+n} \left(\frac{k}{p} \right) &= \frac{1}{p} \sum_{k=0}^{p-1} \sum_{r=m}^{m+n} \sum_{s=0}^{p-1} \left(\frac{k}{p} \right) e^{2(r-k)s\pi i/p} = \\ &= \frac{1}{p} \sum_{s=1}^{p-1} \sum_{r=m}^{m+n} e^{2rs\pi i/p} \sum_{k=0}^{p-1} \left(\frac{k}{p} \right) e^{-2ks\pi i/p}. \end{aligned}$$

Como, para $1 \leq s \leq p-1$, $\left| \sum_{k=0}^{p-1} \left(\frac{k}{p} \right) e^{-2ks\pi i/p} \right| = \sqrt{p}$, e $\sum_{k=0}^{p-1} \left(\frac{k}{p} \right) e^{-2ks\pi i/p}$ não depende de r , segue que

$$\begin{aligned} \left| \sum_{k=m}^{m+n} \left(\frac{k}{p} \right) \right| &\leq \frac{\sqrt{p}}{p} \sum_{s=1}^{p-1} \left| \sum_{r=m}^{m+n} e^{2rs\pi i/p} \right| = \frac{\sqrt{p}}{p} \sum_{s=1}^{p-1} \left| \sum_{r=0}^n e^{2rs\pi i/p} \right| = \\ &= \frac{\sqrt{p}}{p} \sum_{s=1}^{p-1} \left| \frac{e^{2(n+1)s\pi i/p} - 1}{e^{2s\pi i/p} - 1} \right| = \frac{\sqrt{p}}{p} \sum_{s=1}^{p-1} \left| \frac{\text{sen}((n+1)s\pi/p)}{\text{sen}(s\pi/p)} \right| \leq \\ &\leq \frac{\sqrt{p}}{p} \sum_{s=1}^{p-1} \left| \frac{1}{\text{sen}(s\pi/p)} \right| = \frac{2\sqrt{p}}{p} \sum_{s=1}^{\frac{p-1}{2}} \left| \frac{1}{\text{sen}(s\pi/p)} \right| \leq \frac{\sqrt{p}}{p} \sum_{s=1}^{\frac{p-1}{2}} \frac{p}{s} = \sqrt{p} \sum_{s=1}^{\frac{p-1}{2}} \frac{1}{s}. \end{aligned}$$

(usamos na penúltima passagem a desigualdade $\text{sen}(x) \geq 2x/\pi$, válida para $0 \leq x \leq \pi/2$). Para $x > 1$, temos

$$\begin{aligned} \log(2x+1) - \log(2x-1) &= \int_{2x-1}^{2x+1} \frac{dt}{t} = \int_0^1 \left(\frac{1}{2x-t} + \frac{1}{2x+t} \right) dt = \\ &= \int_0^1 \frac{4x}{4x^2 - t^2} dt > \int_0^1 \frac{dt}{x} = \frac{1}{x}, \end{aligned}$$

donde $\sqrt{p} \sum_{s=1}^{\frac{p-1}{2}} \frac{1}{s} < \sqrt{p} \sum_{s=1}^{\frac{p-1}{2}} (\log(2s+1) - \log(2s-1)) = \sqrt{p} \log p.$ \square

Problemas Propostos

6.1. *Determine os possíveis restos da divisão em $\mathbb{Z}[i]$ de*

(a) $(2 + 7i)^{1000}$ por $3 + 5i$;

(b) $(1 - 3i)^{2009}$ por $13 + 2i$.

6.2. *Encontre as fatorações em irredutíveis de 50 , $7 + 4i$ e $11 + 2i$ em $\mathbb{Z}[i]$.*

6.3. *Utilize o algoritmo de Euclides para calcular o mdc de $5 + 12i$ e $7 - 10i$ em $\mathbb{Z}[i]$. Em seguida, expresse este mdc como combinação linear destes dois números.*

6.4. *Sejam n um número inteiro positivo com todos seus fatores primos da forma $4k + 1$ e $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sua fatoração em fatores primos. Mostrar que o número de soluções inteiras de $x^2 + y^2 = n$ com $x \leq y$ é*

$$\left\lfloor \frac{(\alpha_1 + 1) \cdots (\alpha_k + 1) + 1}{2} \right\rfloor.$$

6.5. *Resolva a equação diofantina $y^3 = x^2 + 9$.*

6.6. *Seja n um número inteiro maior que 1. Mostre que $x^n - y^2 = 1$ não possui soluções inteiras não nulas.*

6.7. *Prove que existem duas sequências estritamente crescentes (a_n) e (b_n) tais que*

$$a_n(a_n + 1) \mid b_n^2 + 1$$

para todo n .

6.8 (OBM2010). *Encontre todos os inteiros positivos a, b tais que $3^a = 2b^2 + 1$.*

6.9. Suponha que $\left(\frac{d}{p}\right) = -1$. Demonstrar que, em $\mathbb{Z}[\sqrt{d}]/(p)$,

$$\prod_{\alpha} \alpha = -1$$

onde α percorre todos os elementos não nulos de $\mathbb{Z}[\sqrt{d}]/(p)$.

6.10 (IMO2001). Sejam a, b, c, d inteiros com $a > b > c > d > 0$. Suponha que

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove que $ab + cd$ não é um número primo

6.11. Em $\mathbb{Z}[i]$, mostre que

(a) $\alpha^9 - \alpha$ é múltiplo de 3 para todo $\alpha \in \mathbb{Z}[i]$.

(b) $\alpha^5 - \alpha$ é múltiplo de $2 + i$ para todo $\alpha \in \mathbb{Z}[i]$.

Você consegue generalizar estes resultados?

6.12. Seja F_n a sequência de Fibonacci. Demonstrar que

(a) se p é um número primo da forma $5k \pm 1$ então $p \mid F_{p-1}$;

(b) se p é um primo da forma $5k \pm 2$ então $p \mid F_{p+1}$.

6.13. Considere o anel $\mathbb{Z}[\sqrt{3}] \stackrel{\text{def}}{=} \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ e seja $N: \mathbb{Z}[\sqrt{3}] \rightarrow \mathbb{Z}$ a função dada por $N(a + b\sqrt{3}) = a^2 - 3b^2$ para $a, b \in \mathbb{Z}$.

(a) Mostre N é multiplicativa, isto é, $N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[\sqrt{3}]$.

(b) Mostre que $\mathbb{Z}[\sqrt{3}]^\times = \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}$.

6.14. Mostre que a fatoração única em irredutíveis vale em $\mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$. Utilize este fato para resolver a equação diofantina de Ramanujan-Nagell $2^n = x^2 + 7$.

6.15. Sejam a, b e c inteiros positivos, tais que existe um triângulo T de lados \sqrt{a} , \sqrt{b} e \sqrt{c} . Prove que são equivalentes:

(a) Existe um triângulo congruente a T cujos vértices têm coordenadas inteiras em \mathbb{R}^2 .

(b) T tem área racional e existem x e y inteiros com $a = x^2 + y^2$.

(c) T tem área racional e existem u e v inteiros com $\text{mdc}(a, b, c) = u^2 + v^2$.

6.3 Alguns Resultados de Álgebra

Nesta seção, faremos um breve resumo de alguns resultados algébricos clássicos que serão utilizados nas seções subseqüentes.

6.3.1 Polinômios Simétricos

Um polinômio $p(x_1, \dots, x_n)$ é chamado de *polinômio simétrico* se ele é invariante por qualquer permutação das variáveis x_1, \dots, x_n . Por exemplo, os seguintes polinômios s_i , somas de todos os produtos de i variáveis, são simétricos:

$$\begin{aligned} s_1(x_1, \dots, x_n) &= x_1 + x_2 + \dots + x_n \\ s_2(x_1, \dots, x_n) &= x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n \\ &\vdots \\ s_n(x_1, \dots, x_n) &= x_1x_2 \dots x_n. \end{aligned}$$

Estes são os chamados *polinômios simétricos elementares*. É claro que um produto e uma soma de polinômios simétricos também é um polinômio simétrico, então a partir dos polinômios simétricos elementares podemos construir uma infinidade de polinômios simétricos. O principal resultado sobre polinômios simétricos diz que esta é a única maneira de obtermos polinômios simétricos. Por exemplo, temos que o polinômio simétrico

$$x_1^2 + \dots + x_n^2$$

pode ser escrito como $s_1^2 - 2s_2$.

Teorema 6.25. *Todo polinômio simétrico $p(x_1, \dots, x_n)$ pode ser escrito como um polinômio nos $s_i(x_1, \dots, x_n)$.*

DEMONSTRAÇÃO: Vamos definir uma relação de ordem total nos polinômios simétricos em n variáveis. Primeiro, comparamos monômios: escrevemos

$$ax_1^{e_1} \dots x_n^{e_n} \succ bx_1^{f_1} \dots x_n^{f_n}$$

se

$$1. \ e_1 + \dots + e_n > f_1 + \dots + f_n;$$

2. ou $e_1 + \dots + e_n = f_1 + \dots + f_n$ e (e_1, \dots, e_n) é *lexicograficamente* maior que (f_1, \dots, f_n) , ou seja, existe um i tal que $e_1 = f_1, \dots, e_{i-1} = f_{i-1}$ mas $e_i > f_i$.

Para polinômios, escrevemos $p(x_1, \dots, x_n) \succ q(x_1, \dots, x_n)$ se o maior monômio de $p(x_1, \dots, x_n)$ (seu *termo inicial*) é maior do que o maior monômio de $q(x_1, \dots, x_n)$. Note que em um polinômio simétrico, seu termo inicial $ax_1^{e_1} \dots x_n^{e_n}$ é tal que $e_1 \geq e_2 \geq \dots \geq e_n$.

A demonstração do teorema é por indução com relação à ordem total acima definida, sendo a base constituída pelos polinômios constantes (que são simétricos!), para os quais a proposição é trivialmente verdadeira. Agora, dado um polinômio simétrico $p(x_1, \dots, x_n)$ com termo inicial $ax_1^{e_1} \dots x_n^{e_n}$, considere o polinômio simétrico

$$as_1^{e_1-e_2} s_2^{e_2-e_3} \dots s_{n-1}^{e_{n-1}-e_n} s_n^{e_n}$$

cujos termo inicial é

$$ax_1^{e_1-e_2} (x_1 x_2)^{e_2-e_3} \dots (x_1 x_2 \dots x_{n-1})^{e_{n-1}-e_n} (x_1 x_2 \dots x_n)^{e_n} = ax_1^{e_1} \dots x_n^{e_n}$$

ou seja, o mesmo de p . Assim,

$$p \succ p - as_1^{e_1-e_2} s_2^{e_2-e_3} \dots s_{n-1}^{e_{n-1}-e_n} s_n^{e_n}.$$

Como o polinômio $p - as_1^{e_1-e_2} s_2^{e_2-e_3} \dots s_{n-1}^{e_{n-1}-e_n} s_n^{e_n}$ é simétrico, por hipótese de indução ele pode ser escrito em função de polinômios simétricos elementares. Logo o mesmo vale para p , como desejado. \square

Observe que a demonstração acima fornece um algoritmo, que pode ser efetivamente utilizado para escrever polinômios simétricos em função de polinômios simétricos elementares.

6.3.2 Extensões de Corpos e Números Algébricos

Dada uma extensão de corpos $L \supset K$, definimos o *grau* $[L : K]$ de L sobre K como a dimensão de L visto como K -espaço vetorial. Por exemplo, $[\mathbb{C} : \mathbb{R}] = 2$ pois 1 e i formam uma base de \mathbb{C} sobre \mathbb{R} .

Proposição 6.26. *O grau é multiplicativo: se $M \supset L \supset K$ são extensões de corpos, então*

$$[M : K] = [M : L] \cdot [L : K].$$

DEMONSTRAÇÃO: Sejam $m = [M : L]$ e $n = [L : K]$ e sejam $\omega_1, \dots, \omega_m$ e τ_1, \dots, τ_n respectivamente bases de M sobre L e de L sobre K . Basta então mostrar que os mn elementos $\omega_i \tau_j$, $1 \leq i \leq m$ e $1 \leq j \leq n$, formam uma base de M sobre K .

Primeiramente temos que $\omega_i \tau_j$ são linearmente independentes sobre K , pois se $a_{ij} \in K$ são tais que

$$\sum_{1 \leq i \leq m} \sum_{1 \leq j \leq n} a_{ij} \omega_i \tau_j = 0 \iff \sum_{1 \leq i \leq m} \left(\sum_{1 \leq j \leq n} a_{ij} \tau_j \right) \omega_i = 0$$

então $\sum_{1 \leq j \leq n} a_{ij} \tau_j = 0$ para $i = 1, 2, \dots, m$ pois os ω_i são linearmente independentes sobre L . Agora, para cada i fixo, temos também que $a_{ij} = 0$ para $j = 1, \dots, n$, pela independência linear dos τ_j sobre K .

Agora vamos mostrar que todo elemento $\alpha \in M$ é uma K -combinação linear dos $\omega_i \tau_j$. Como os ω_i formam uma base de M sobre L , existem $b_i \in L$ tais que

$$\alpha = b_1 \omega_1 + \dots + b_m \omega_m.$$

Da mesma forma, para cada i fixo, existem $a_{ij} \in K$ tais que

$$b_i = a_{i1} \tau_1 + \dots + a_{in} \tau_n.$$

Assim, $\alpha = \sum_{1 \leq i \leq m} \sum_{1 \leq j \leq n} a_{ij} \omega_i \tau_j$, como desejado. \square

Definição 6.27. *Seja $L \supset K$ uma extensão de corpos.*

1. *Um elemento $\alpha \in L$ é dito algébrico sobre K se existe um polinômio não nulo $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Um número $\alpha \in \mathbb{C}$ é algébrico se ele é algébrico sobre \mathbb{Q} .*
2. *Se $\alpha \in L$ é algébrico, então um polinômio mônico $f(x) \in K[x]$ de grau mínimo que admite α como raiz é chamado de polinômio minimal de α sobre K .*

Por exemplo, i , $\sqrt{2}$ são números algébricos com polinômios minimais sobre \mathbb{Q} dados por $x^2 + 1$ e $x^2 - 2$, respectivamente. Pode-se demonstrar que π e e não são algébricos, ou seja, não satisfazem nenhum polinômio não nulo com coeficientes racionais.

Teorema 6.28. *Seja $L \supset K$ uma extensão de corpos e $\alpha \in L$ um número algébrico sobre K com polinômio minimal $p(x) \in K[x]$. Então se $f(x) \in K[x]$,*

$$f(\alpha) = 0 \iff p(x) \mid f(x).$$

Em particular, isto mostra que α possui um único polinômio minimal.

DEMONSTRAÇÃO: É claro que se $p(x) \mid f(x)$ então $f(\alpha) = 0$. Agora suponha que $f(\alpha) = 0$ e sejam $q(x)$ e $r(x)$ o quociente e o resto na divisão euclidiana de $f(x)$ por $p(x)$:

$$f(x) = q(x)p(x) + r(x), \quad \deg r(x) < \deg p(x).$$

Substituindo $x = \alpha$, obtemos $r(\alpha) = 0$. Pela minimalidade do grau de $p(x)$, temos portanto que $r(x)$ é o polinômio nulo, ou seja, $p(x) \mid f(x)$.

Para a última asserção, se houvesse dois polinômios minimais $p_1(x)$ e $p_2(x)$ de α , teríamos que $p_1(x) \mid p_2(x)$ e $p_2(x) \mid p_1(x)$. Mas como $p_1(x)$ e $p_2(x)$ são mônicos por definição temos que isto implica $p_1(x) = p_2(x)$. \square

Note que o polinômio minimal $p(x) \in K[x]$ de um número algébrico α é sempre irredutível em $K[x]$, pois caso ele pudesse ser escrito como produto de dois fatores de graus menores do que $\deg p(x)$, α seria raiz de algum desses fatores, uma contradição. Por outro lado, o teorema implica que se $f(x)$ é um polinômio mônico e irredutível em $K[x]$ tal que $f(\alpha) = 0$, então $p(x) \mid f(x) \implies p(x) = f(x)$, ou seja, $f(x)$ é o polinômio minimal de α . Por exemplo, vimos que pelo critério de Eisenstein e pelo lema de Gauß, para p primo o polinômio

$$x^{p-1} + x^{p-2} + \cdots + x + 1$$

é irredutível sobre $\mathbb{Q}[x]$, logo ele é o polinômio minimal de $\zeta_p = e^{2\pi i/p}$ sobre \mathbb{Q} .

Definição 6.29. *Seja $L \supset K$ uma extensão de corpos e seja $\alpha \in L$ um número algébrico sobre K com polinômio minimal $p(x) \in K[x]$. As raízes de $p(x)$ em L são chamadas de conjugados de α .*

Por exemplo, sobre \mathbb{Q} os complexos i e $-i$ são conjugados entre si, bem como $\sqrt{2}$ e $-\sqrt{2}$. A importância dos conjugados é que eles são,

do ponto de vista algébrico, indistinguíveis. Mais precisamente, temos o seguinte corolário do teorema anterior:

Corolário 6.30. *Seja $L \supset K$ uma extensão de corpos e seja $\alpha \in L$ um número algébrico sobre K . Sejam α_i seus conjugados. Se $f(x) \in K[x]$ é um polinômio tal que $f(\alpha) = 0$, então $f(\alpha_i) = 0$ para todo i .*

Se $L \supset K$ é uma extensão de corpos e $\alpha \in L$, denotamos por $K[\alpha]$ o menor subanel de L que contém K e α , ou seja, $K[\alpha]$ consiste nos polinômios em α com coeficientes em K . Por outro lado, escrevemos $K(\alpha)$ para o menor subcorpo de L que contém K e α , isto é, $K(\alpha)$ consiste em todas as expressões da forma $f(\alpha)/g(\alpha)$, onde $f(x), g(x) \in K[x]$ e $g(\alpha) \neq 0$. Analogamente, para $\alpha_1, \dots, \alpha_n \in L$, denotamos por $K[\alpha_1, \dots, \alpha_n]$ e $K(\alpha_1, \dots, \alpha_n)$ os menores subanel e subcorpo de L contendo K e $\alpha_1, \dots, \alpha_n$. Se existe α tal que $L = K(\alpha)$, diremos que L é uma *extensão simples* de K .

O fato notável é que, quando α é algébrico, podemos nos livrar do “denominador” nas expressões $f(\alpha)/g(\alpha) \in K(\alpha)$:

Proposição 6.31. *Seja $L \supset K$ uma extensão de corpos e seja $\alpha \in L$ um número algébrico sobre K com polinômio minimal $p(x) \in K[x]$ de grau n . Então*

$$K(\alpha) = K[\alpha] = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}.$$

Em particular, $[K(\alpha) : K] = n$.

DEMONSTRAÇÃO: Observe que se $p(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$, temos, para $j \geq 0$,

$$\alpha^n = -c_{n-1}\alpha^{n-1} - \dots - c_0 \implies \alpha^{n+j} = -c_{n-1}\alpha^{n-1+j} - \dots - c_0\alpha^j$$

e utilizando repetidamente esta relação podemos expressar qualquer elemento de $K[\alpha]$ como um polinômio em α de grau menor ou igual a $n-1$. Assim, basta agora mostrar que o anel $K[\alpha]$ é um corpo, pois neste caso ele será claramente o menor subcorpo de L contendo K e α .

Para mostrar que todo elemento não nulo $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$ de $K[\alpha]$ é invertível, considere o polinômio (não nulo) correspondente $g(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$. Note que $g(x)$ e $p(x)$ são primos entre si,

pois $p(x)$ é irredutível e não divide $g(x)$, já que $\deg g(x) \leq n-1$. Assim, pelo teorema de Bachet-Bézout, existem polinômios $r(x), s(x) \in K[x]$ tais que

$$r(x)g(x) + s(x)p(x) = 1.$$

Substituindo $x = \alpha$, obtemos $r(\alpha)g(\alpha) = 1$ com $r(\alpha) \in K[\alpha]$, como queríamos.

Finalmente, $[K(\alpha) : K] = n$ pois $K[\alpha]$ é um K -espaço vetorial de dimensão n com base $1, \alpha, \dots, \alpha^{n-1}$: este conjunto claramente gera $K[\alpha]$ e, além disso, é linearmente independente sobre K , pois caso contrário α seria raiz de um polinômio de grau no máximo $n-1$, contrariando a minimalidade de $n = \deg p(x)$. \square

Agora podemos dar uma caracterização mais intrínseca de um número algébrico:

Proposição 6.32. *Seja $M \supset K$ uma extensão de corpos.*

1. *Um número $\alpha \in M$ é algébrico sobre K se, e somente se, α pertence a uma subextensão finita L de $M \supset K$, ou seja, $M \supset L \supset K$ e $[L : K]$ é finito.*
2. *O subconjunto de M formado por todos os números algébricos sobre K é um subcorpo de M .*

DEMONSTRAÇÃO: Para provar (1), já vimos que se α é algébrico sobre K e seu polinômio minimal tem grau n então $[K(\alpha) : K] = n$, logo podemos tomar $L = K(\alpha)$. Reciprocamente, se $\alpha \in L$ com $n = [L : K]$ finito, então os $n+1$ elementos $1, \alpha, \alpha^2, \dots, \alpha^n$ são linearmente dependentes sobre K . Mas isto é o mesmo que dizer que α satisfaz um polinômio não nulo com coeficientes em K , ou seja, que α é algébrico sobre K .

Para provar (2), note que dados dois números $\alpha, \beta \in M$ algébricos sobre K , temos que $K(\alpha, \beta)$ possui dimensão finita sobre K . De fato, temos $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K]$ e ambos os fatores são finitos: $[K(\alpha) : K] < \infty$ pois α é algébrico sobre K e $[K(\alpha, \beta) : K(\alpha)] < \infty$ pois β é algébrico sobre K , logo sobre $K(\alpha)$ também, e $K(\alpha, \beta) = K(\alpha)(\beta)$ é extensão simples de $K(\alpha)$. Como $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in K(\alpha, \beta)$ (com $\beta \neq 0$ no último caso), o resultado segue do item (1). \square

6.3.3 Imersões, Traço e Norma

O seguinte teorema permite reduzir o estudo de extensões finitas de \mathbb{Q} ao estudo de extensões simples (o que já foi feito no final da subseção anterior):

Teorema 6.33 (Elemento Primitivo). *Seja $K \supset \mathbb{Q}$ uma extensão finita de corpos (i.e. $[K : \mathbb{Q}]$ é finito). Então existe um elemento $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$.*

DEMONSTRAÇÃO: Como K é finitamente gerado sobre \mathbb{Q} (por exemplo, por uma base de K sobre \mathbb{Q}), por indução no número de geradores bastará mostrar que se $K = \mathbb{Q}(\alpha, \beta)$ é gerado por dois elementos α, β então existe θ tal que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. Vamos tomar $\theta = \alpha + c\beta$ para algum $c \in \mathbb{Q}$ conveniente. Assim, bastará mostrar que $\beta \in \mathbb{Q}(\theta)$, pois neste caso $\alpha = \theta - c\beta \in \mathbb{Q}(\theta)$ e portanto $\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(\theta)$, sendo a outra inclusão trivial.

Sejam $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ e $\beta_1 = \beta, \beta_2, \dots, \beta_n$ os conjugados de α e β . Escolha $c \in \mathbb{Q}$ de modo que os elementos $\alpha_i + c\beta_j$, $1 \leq i \leq m$, $1 \leq j \leq n$, sejam dois a dois distintos. Isto é possível pois há apenas um número finito de restrições, mas há uma infinidade de possíveis escolhas de $c \in \mathbb{Q}$. Sejam $p(x), q(x) \in \mathbb{Q}[x]$ respectivamente os polinômios minimais de α e β (que são números algébricos pois pertencem a uma extensão finita de \mathbb{Q}). Temos que β é raiz de $p(\theta - cx) \in \mathbb{Q}(\theta)[x]$, logo o polinômio minimal de β sobre $\mathbb{Q}(\theta)$ divide $\text{mdc}(p(\theta - cx), q(x))$. Mas as raízes de $q(x)$ são os β_j , e $\theta - c\beta_j \neq \alpha_i$ a não ser que $i = j = 1$, logo a única raiz comum de $p(\theta - cx)$ e $q(x)$ é β . Mas toda raiz do polinômio minimal de β sobre $\mathbb{Q}(\theta)$ é uma raiz comum destes dois polinômios, logo este polinômio minimal é $x - \beta$ e portanto $\beta \in \mathbb{Q}(\theta)$. \square

Definição 6.34. *Seja $K \supset \mathbb{Q}$ uma extensão finita de corpos. Uma imersão $\sigma: K \hookrightarrow \mathbb{C}$ é uma função injetora que preserva soma e produto de elementos em K :*

$$\sigma(a + b) = \sigma(a) + \sigma(b) \quad e \quad \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$$

para todo $a, b \in K$.

Observe que qualquer imersão $\sigma: K \hookrightarrow \mathbb{C}$ é a identidade quando restrita a \mathbb{Q} . De fato, temos que $\sigma(0 + 0) = \sigma(0) + \sigma(0) \implies \sigma(0) = 0$ e

$\sigma(1 \cdot 1) = \sigma(1) \cdot \sigma(1) \implies \sigma(1) = 1$ ($\sigma(1) \neq 0$ pois σ é injetora). Assim, utilizando repetidamente a compatibilidade com a adição, temos $\sigma(n) = n$ para todo $n \in \mathbb{N}$, e da relação $\sigma(-n) + \sigma(n) = \sigma(0) = 0$, temos que $\sigma(n) = n$ para todo $n \in \mathbb{Z}$. Analogamente, de $\sigma(r) \cdot \sigma(r^{-1}) = \sigma(1) = 1$ para todo $r \in \mathbb{Z}$ não nulo, concluímos finalmente que $\sigma(q) = q$ para todo $q \in \mathbb{Q}$.

Teorema 6.35. *Se $[K : \mathbb{Q}] = n$, existem exatamente n imersões $\sigma: K \hookrightarrow \mathbb{C}$.*

DEMONSTRAÇÃO: Escreva $K = \mathbb{Q}(\theta)$ para algum elemento primitivo. Note que para qualquer polinômio $p(x) \in \mathbb{Q}[x]$ e qualquer imersão $\sigma: K \hookrightarrow \mathbb{C}$ temos $\sigma(p(\theta)) = p(\sigma(\theta))$. De fato, se $p(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_0$, $a_i \in \mathbb{Q}$, temos

$$\begin{aligned} \sigma(p(\theta)) &= \sigma(a_m \theta^m + a_{m-1} \theta^{m-1} + \dots + a_0) \\ &= a_m \sigma(\theta)^m + a_{m-1} \sigma(\theta)^{m-1} + \dots + a_0 = p(\sigma(\theta)) \end{aligned}$$

Como qualquer elemento de $K = \mathbb{Q}(\theta)$ escreve-se como um polinômio em θ com coeficientes racionais, a conta acima mostra que σ está unicamente determinado pelo valor de $\sigma(\theta)$. Mas se $p(x)$ é o polinômio minimal de θ sobre \mathbb{Q} , então $p(\theta) = 0 \implies 0 = \sigma(p(\theta)) = p(\sigma(\theta))$, ou seja, $\sigma(\theta)$ só pode ser uma das raízes de $p(x)$, logo há no máximo $n = \deg p(x) = [K : \mathbb{Q}]$ imersões $\sigma: K \hookrightarrow \mathbb{C}$.

Reciprocamente, vamos mostrar que, para cada conjugado θ_i de θ sobre \mathbb{Q} , podemos definir uma imersão com $\sigma_i(\theta) = \theta_i$. Como $1, \theta, \dots, \theta^{n-1}$ é uma base de K sobre \mathbb{Q} , cada elemento de $K = \mathbb{Q}(\theta)$ pode ser unicamente escrito como $a_0 + a_1 \theta + \dots + a_{n-1} \theta^{n-1}$, $a_i \in \mathbb{Q}$, e basta definir

$$\sigma_i(a_0 + a_1 \theta + \dots + a_{n-1} \theta^{n-1}) = a_0 + a_1 \theta_i + \dots + a_{n-1} \theta_i^{n-1}$$

e é imediato verificar que σ_i preserva somas. Por outro lado, se

$$(a_0 + \dots + a_{n-1} \theta^{n-1}) \cdot (b_0 + \dots + b_{n-1} \theta^{n-1}) = c_0 + \dots + c_{n-1} \theta^{n-1}$$

com $a_j, b_j, c_j \in \mathbb{Q}$, temos

$$(a_0 + \dots + a_{n-1} \theta_i^{n-1}) \cdot (b_0 + \dots + b_{n-1} \theta_i^{n-1}) = c_0 + \dots + c_{n-1} \theta_i^{n-1}$$

para todo i pelo corolário 6.30 aplicado ao polinômio

$$f(x) = (a_0 + \dots + a_{n-1} x^{n-1}) \cdot (b_0 + \dots + b_{n-1} x^{n-1}) - (c_0 + \dots + c_{n-1} x^{n-1}).$$

Portanto

$$\begin{aligned}
 & \sigma_i((a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1})(b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1})) \\
 &= \sigma_i(c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}) = c_0 + c_1\theta_i + \cdots + c_{n-1}\theta_i^{n-1} \\
 &= (a_0 + a_1\theta_i + \cdots + a_{n-1}\theta_i^{n-1}) \cdot (b_0 + b_1\theta_i + \cdots + b_{n-1}\theta_i^{n-1}) \\
 &= \sigma_i(a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}) \cdot \sigma_i(b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}).
 \end{aligned}$$

Assim, para concluir a prova basta mostrar que há $n = \deg p(x)$ conjugados θ_i em \mathbb{C} , ou seja, que $p(x)$ não tem raízes múltiplas ou ainda que $\text{mdc}(p(x), p'(x)) = 1$. De fato, $p(x)$ é irredutível em $\mathbb{Q}[x]$, logo $p(x)$ e $p'(x)$ são primos entre si pois a derivada $p'(x)$ possui grau estritamente menor do que o grau de $p(x)$. \square

Uma variação da demonstração acima fornece a seguinte generalização, cuja prova deixamos como exercício para o leitor.

Proposição 6.36. *Sejam $L \supset K \supset \mathbb{Q}$ extensões finitas de corpos. Dada uma imersão $\sigma: K \hookrightarrow \mathbb{C}$, existem exatamente $[L:K]$ imersões $\tilde{\sigma}: L \hookrightarrow \mathbb{C}$ que estendem σ , i.e., tais que $\tilde{\sigma}|_K = \sigma$.*

Definição 6.37. *Seja $K \supset \mathbb{Q}$ uma extensão finita de corpos e $\alpha \in K$. Sejam $\sigma_i: K \hookrightarrow \mathbb{C}$, $i = 1, \dots, n$ todas as $n = [K: \mathbb{Q}]$ imersões de K em \mathbb{C} . O traço $\text{Tr}_{K/\mathbb{Q}}(\alpha)$ e a norma $N_{K/\mathbb{Q}}(\alpha)$ de α são definidos respectivamente por*

$$\text{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{1 \leq i \leq n} \sigma_i(\alpha) \quad e \quad N_{K/\mathbb{Q}}(\alpha) = \prod_{1 \leq i \leq n} \sigma_i(\alpha).$$

Por exemplo, para $K = \mathbb{Q}(i)$, as imersões são a identidade e a conjugação complexa, de modo que, para $a, b \in \mathbb{Q}$,

$$\begin{aligned}
 \text{Tr}_{K/\mathbb{Q}}(a + bi) &= a + bi + a - bi = 2a & e \\
 N_{K/\mathbb{Q}}(a + bi) &= (a + bi)(a - bi) = a^2 + b^2.
 \end{aligned}$$

Ou seja, a norma definida acima coincide com a norma dos inteiros de Gauß, quando restrita a $\mathbb{Z}[i]$.

Proposição 6.38. *Com a notação acima, sejam $\alpha, \beta \in K$. Temos*

1. *O traço é aditivo e a norma, multiplicativa:*

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(\alpha + \beta) &= \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta) & e \\ N_{K/\mathbb{Q}}(\alpha\beta) &= N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta).\end{aligned}$$

2. $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ e $N_{K/\mathbb{Q}}(\alpha)$ são números racionais.

3. *se $T_\alpha: K \rightarrow K$ denota a transformação \mathbb{Q} -linear dada pela multiplicação por α , então $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ e $N_{K/\mathbb{Q}}(\alpha)$ são respectivamente iguais ao traço e ao determinante de T_α .*

DEMONSTRAÇÃO: O primeiro item é consequência direta das definições. O segundo item é consequência imediata do terceiro. Uma outra prova é a seguinte: escreva $K = \mathbb{Q}(\theta)$ para algum elemento primitivo θ e sejam $\theta_1 = \sigma_1(\theta), \theta_2 = \sigma_2(\theta), \dots, \theta_n = \sigma_n(\theta)$ os seus n conjugados. Podemos escrever $\alpha = p(\theta)$ para algum polinômio $p(x) \in \mathbb{Q}[x]$. Temos portanto

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{1 \leq i \leq n} \sigma_i(\alpha) = \sum_{1 \leq i \leq n} \sigma_i(p(\theta)) = \sum_{1 \leq i \leq n} p(\sigma_i(\theta)) = \sum_{1 \leq i \leq n} p(\theta_i).$$

Assim, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ é uma expressão simétrica dos conjugados θ_i de θ , logo pelo teorema 6.25 pode ser escrita em termos dos coeficientes do polinômio minimal de θ , que são polinômios simétricos elementares em θ_i . Mas os coeficientes do polinômio minimal de θ são racionais, logo $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$. A prova de que $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ é análoga.

Finalmente, seja $m = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ o grau do polinômio minimal de α

$$p(x) = x^m + c_{m-1}x^{m-1} + \dots + c_0, \quad c_i \in \mathbb{Q},$$

$n = [K : \mathbb{Q}(\alpha)]$ e $\omega_1 = 1, \omega_2, \dots, \omega_n$ uma base de K sobre $\mathbb{Q}(\alpha)$. Então

$$\begin{array}{ccccccc} 1, & \alpha, & \alpha^2, & \dots, & \alpha^{m-1} \\ \omega_2, & \alpha\omega_2, & \alpha^2\omega_2, & \dots, & \alpha^{m-1}\omega_2 \\ & & \vdots & & \\ \omega_n, & \alpha\omega_n, & \alpha^2\omega_n, & \dots, & \alpha^{m-1}\omega_n \end{array}$$

é uma base de K sobre \mathbb{Q} . Nesta base, a matriz de T_α é dada por n

blocos na diagonal compostos por matrizes $m \times m$ da forma

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & & & & \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{pmatrix}.$$

Assim, o polinômio característico de T_α é $p(x)^n$ e temos $\text{Tr}(T_\alpha) = -nc_{m-1}$ e $\det(T_\alpha) = (-1)^{mn}c_0^n$. Assim, pela proposição anterior, temos que dado um conjugado α' de α , existem n imersões σ de K em \mathbb{C} tais que $\sigma(\alpha) = \alpha'$ e, portanto, quando σ percorre todas as imersões de K em \mathbb{C} , $\sigma(\alpha)$ percorre todos os m conjugados de α , cada um n vezes. Portanto, das relações entre coeficientes e raízes de $p(x)$, temos

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(\alpha) &= -nc_{m-1} = \text{Tr}(T_\alpha) & \text{e} \\ N_{K/\mathbb{Q}}(\alpha) &= (-1)^{mn}c_0^n = \det(T_\alpha). \end{aligned}$$

□

Problemas Propostos

6.16. *Calcule os graus das seguintes extensões:*

(a) $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$

(b) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$

(c) $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}]$ para $n = 3, 4, 5, 6, 7, 8$

(d) $[\mathbb{Q}(\cos 36^\circ) : \mathbb{Q}]$

6.17. *Mostre que $\sin \frac{2\pi}{n}$ e $\cos \frac{2\pi}{n}$ são números algébricos sobre \mathbb{Q} para todo inteiro positivo n (Dica: use a fórmula de Moivre $e^{i\theta} = \cos \theta + i \sin \theta$).*

6.18. *Seja $\alpha \in \mathbb{C}$ um número algébrico sobre \mathbb{Q} . Mostre que se $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é ímpar, então $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$.*

6.19. Seja $p(X) \in \mathbb{Q}[X]$ um polinômio irredutível de grau n e seja $L \supset \mathbb{Q}$ uma extensão de grau m onde $\text{mdc}(m, n) = 1$. Prove que $p(X)$ também é irredutível em $L[X]$.

6.20. Seja $f(X)$ um polinômio irredutível em $\mathbb{Q}[X]$ de grau n e seja $g(X) \in \mathbb{Q}[X]$ um polinômio qualquer. Mostre que todo fator irredutível de $f(g(X))$ tem grau divisível por n .

6.21 (Identidades de Newton). Seja s_i o i -ésimo polinômio simétrico elementar e

$$t_i(x_1, \dots, x_n) = x_1^i + x_2^i + \dots + x_n^i.$$

Prove que, para todo $k \geq 1$,

$$ks_k(x_1, \dots, x_n) = \sum_{i=1}^k (-1)^{i-1} s_{k-i}(x_1, \dots, x_n) t_i(x_1, \dots, x_n).$$

Conclua que os polinômios simétricos podem também ser escritos como polinômios em t_i .

6.22. Seja $p(x)$ um polinômio irredutível em $\mathbb{Q}[x]$ de grau maior do que 1. Prove que se $p(x)$ admite duas raízes r e s cujo produto é 1 então o grau de $p(x)$ é par.

6.23. Sejam $p(x), q(x) \in \mathbb{Q}[x]$ polinômios mônicos irredutíveis e sejam a e b tais que $p(a) = q(b) = 0$ e $a + b \in \mathbb{Q}$. Prove que o polinômio $p(x)^2 - q(x)^2$ possui uma raiz racional.

6.24. Seja $p(x)$ um polinômio irredutível em $\mathbb{Q}[x]$ de grau ímpar. Sejam $q(x), r(x) \in \mathbb{Q}[x]$ tais que $p(x)$ divide $q(x)^2 + q(x) \cdot r(x) + r(x)^2$. Prove que na verdade $p(x)^2$ divide $q(x)^2 + q(x) \cdot r(x) + r(x)^2$.

6.25. Seja $f(x)$ um polinômio de coeficientes racionais e α tal que $\alpha^3 - 21\alpha = (f(\alpha))^3 - 21f(\alpha) = 7$; por exemplo, podemos tomar $f(x) = (x^2 - 2x - 14)/3$ (verifique!). Prove que, para todo $n \geq 1$,

$$\left(f^{(n)}(\alpha)\right)^3 - 21 \cdot f^{(n)}(\alpha) = 7,$$

onde $f^{(n)}(\alpha) = \underbrace{f(f(\dots f(\alpha)))}_{n \text{ vezes}}$.

6.26. Seja $p(x) \in \mathbb{Z}[x]$ um polinômio mônico irredutível tal que $|p(0)|$ não é um quadrado perfeito. Mostre que $p(x^2)$ também é irredutível em $\mathbb{Z}[x]$.

6.4 Inteiros Algébricos

Queremos estender o estudo anterior para outros subanéis de \mathbb{C} . O primeiro passo é identificar os elementos que assumirão o papel de “inteiros” neste contexto mais geral.

Definição 6.39. *Seja $B \supset A$ uma extensão de anéis. Um elemento $\theta \in B$ é dito integral sobre A se ele é raiz de um polinômio mônico em $A[x]$:*

$$\theta^n + a_{n-1} \cdot \theta^{n-1} + a_{n-2} \cdot \theta^{n-2} + \cdots + a_0 = 0 \quad (a_i \in A).$$

Um número complexo θ que é integral sobre \mathbb{Z} é chamado de inteiro algébrico.

Por exemplo, qualquer inteiro $n \in \mathbb{Z}$ é um inteiro algébrico (pois n é raiz do polinômio $x - n$). Os números $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ também são inteiros algébricos pois são raízes do polinômio mônico com coeficientes inteiros $x^2 - x - 1 = 0$.

Uma das principais motivações para esta definição é o seguinte lema, que caracteriza os elementos de \mathbb{Z} como sendo exatamente os inteiros algébricos que moram dentro de \mathbb{Q} :

Lema 6.40. *Se $\theta \in \mathbb{Q}$ é um inteiro algébrico, então $\theta \in \mathbb{Z}$.*

DEMONSTRAÇÃO: Seja $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \mathbb{Z}[x]$ um polinômio mônico tal que $f(\theta) = 0$ e escreva $\theta = a/b$ com $a, b \in \mathbb{Z}$ primos entre si. Temos

$$f(\theta) = 0 \iff a^n + c_{n-1}a^{n-1}b + c_{n-2}a^{n-2}b^2 + \cdots + c_0b^n = 0.$$

Como b divide todos os termos a partir do segundo, temos que b divide a^n também. Mas como a e b são primos entre si temos que isto só ocorre se $b = \pm 1$, logo $\theta = \pm a \in \mathbb{Z}$. \square

O próximo lema permite “limpar os denominadores” de um número algébrico arbitrário:

Lema 6.41. *Se θ é um número algébrico, existe um inteiro $a \in \mathbb{Z} \setminus \{0\}$ tal que $a\theta$ é um inteiro algébrico.*

DEMONSTRAÇÃO: Suponha que $a_n\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_0 = 0$ com $a_i \in \mathbb{Z}$, $a_n \neq 0$. Multiplicando por a_n^{n-1} obtemos $(a_n\theta)^n + a_{n-1}(a_n\theta)^{n-1} + \cdots + a_n^{n-1}a_0 = 0$, logo podemos tomar $a = a_n$. \square

Se $B \supset A$ é uma extensão de anéis e $\theta_1, \dots, \theta_n \in B$ são elementos quaisquer, denotamos por $A[\theta_1, \dots, \theta_n]$ o menor subanel de B que contém A e $\theta_1, \dots, \theta_n$. Se θ é um inteiro algébrico, raiz de um polinômio mônico $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \mathbb{Z}[x]$ de grau n , temos que

$$\mathbb{Z}[\theta] = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid a_i \in \mathbb{Z}\}.$$

De fato, aplicando várias vezes a relação

$$\begin{aligned} f(\theta) = 0 &\iff \theta^n = -c_{n-1}\theta^{n-1} - \cdots - c_0 \\ &\implies \theta^{n+i} = -c_{n-1}\theta^{n+i-1} - \cdots - c_0\theta^i \end{aligned}$$

para $i \geq 0$ podemos escrever qualquer potência em θ de grau maior ou igual a n em termos de potências de grau menor do que n . Note a importância do fato de $f(x)$ ser mônico, o que dispensa a necessidade de dividir a relação acima pelo coeficiente líder de $f(x)$.

Assim como no teorema 6.32, a observação anterior permitirá obter uma caracterização mais intrínseca dos inteiros algébricos, com a qual poderemos provar que o conjunto de todos os inteiros algébricos forma um anel. Primeiro, precisamos de uma

Definição 6.42. *Uma extensão de anéis $B \supset A$ é dita finita se existem elementos $\omega_1, \dots, \omega_n \in B$ tais que qualquer elemento de B se escreve como combinação A -linear dos ω_i :*

$$B = A\omega_1 + \cdots + A\omega_n \stackrel{\text{def}}{=} \{a_1\omega_1 + \cdots + a_n\omega_n \mid a_i \in A\}.$$

Por exemplo, temos que se θ é um inteiro algébrico então $\mathbb{Z}[\theta]$ é finito sobre \mathbb{Z} . Observe que a representação acima como combinação linear dos ω_i não é, necessariamente, única (i.e., os ω_i não precisam ser “linearmente independentes” sobre A).

Teorema 6.43. *Seja $C \supset A$ uma extensão de anéis.*

1. *Um elemento $\theta \in C$ é integral sobre A se, e somente se, θ pertence a uma subextensão finita B de $C \supset A$, isto é, $\theta \in B$ onde B é um subanel de C tal que $B \supset A$ é uma extensão finita de anéis.*
2. *O subconjunto de C formado por todos os elementos integrais sobre A é um subanel de C . Em particular, o conjunto de todos os inteiros algébricos é um subanel de \mathbb{C} .*

DEMONSTRAÇÃO: (1) Se $\theta \in C$ é integral sobre A , basta tomar $C = A[\theta]$. Para mostrar a recíproca, vamos aplicar o chamado “truque do determinante”. Suponha que $\theta \in B$, onde B é uma extensão finita de A :

$$B = A\omega_1 + \cdots + A\omega_n$$

com $\omega_1 = 1$, digamos. Então, como B é um anel, temos que $\theta\omega_i \in B$ para $i = 1, 2, \dots, n$, ou seja, existem $a_{ij} \in A$ tais que

$$\begin{aligned}\theta\omega_1 &= a_{11}\omega_1 + \cdots + a_{1n}\omega_n \\ \theta\omega_2 &= a_{21}\omega_1 + \cdots + a_{2n}\omega_n \\ &\vdots \\ \theta\omega_n &= a_{n1}\omega_1 + \cdots + a_{nn}\omega_n\end{aligned}$$

Seja $M = (a_{ij})$ a matriz $n \times n$ formada pelos a_{ij} e I_n a matriz identidade de ordem n . Se ω é o vetor coluna formado pelos ω_i , podemos reescrever o “sistema” acima em forma matricial como $(I_n\theta - M) \cdot \omega = \mathbf{0}$. Como o sistema homogêneo na variável ω possui solução não trivial, temos que $\det(I_n\theta - M) = 0$ (multiplique $(I_n\theta - M) \cdot \omega = \mathbf{0}$ pela matriz adjunta de $(I_n\theta - M)$). Em outras palavras, θ é raiz do polinômio característico de M , que é mônico e com coeficientes em A , logo θ é um integral sobre A .

(2) Sejam α e β dois elementos integrais sobre A , raízes de polinômios mônicos em $A[x]$ de graus m e n respectivamente. Então o subanel de C

$$A[\alpha, \beta] \stackrel{\text{def}}{=} \left\{ \sum_{1 \leq i < m} \sum_{1 \leq j < n} a_{ij} \alpha^i \beta^j \mid a_{ij} \in A \right\}$$

é finito sobre A , como é fácil ver utilizando as relações mônicas satisfeitas por α e β . Como $\alpha \pm \beta, \alpha\beta \in A[\alpha, \beta]$, o resultado segue do critério já provado acima. \square

Exemplo 6.44. *Seja F_n o n -ésimo número de Fibonacci. Mostre que*

$$m \mid n \implies F_m \mid F_n.$$

SOLUÇÃO: Sejam $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ as raízes da equação $x^2 - x - 1 = 0$. Suponha que $m \mid n$, digamos $n = mk$ com $k \in \mathbb{Z}$. Temos

$$\begin{aligned} \frac{F_n}{F_m} &= \frac{F_{km}}{F_m} = \frac{\alpha^{km} - \beta^{km}}{\alpha^m - \beta^m} \\ &= (\alpha^m)^{k-1} + (\alpha^m)^{k-2}(\beta^m) + (\alpha^m)^{k-3}(\beta^m)^2 + \cdots + (\beta^m)^{k-1} \end{aligned}$$

Como α e β são inteiros algébricos e os inteiros algébricos formam um anel, temos da expressão acima que F_n/F_m é um inteiro algébrico. Mas $F_n/F_m \in \mathbb{Q}$ também, logo $F_n/F_m \in \mathbb{Z}$, ou seja, $F_m \mid F_n$. \square

Exemplo 6.45. *A sequência de Perrin é definida por*

$$s_0 = 3, \quad s_1 = 0, \quad s_2 = 2 \quad e$$

$$s_{n+3} = s_{n+1} + s_n \quad \text{para todo } n \geq 0.$$

Prove que $p \mid s_p$, para todo p primo.

SOLUÇÃO: Seja $f(x) = x^3 - x - 1$ o polinômio característico da recursão (ver apêndice) e sejam α, β, γ as suas raízes. Afirmamos que $s_n = \alpha^n + \beta^n + \gamma^n$. De fato, temos que esta última expressão satisfaz a relação $s_{n+3} = s_{n+1} + s_n$, assim basta verificar que os valores iniciais coincidem. Mas isto é claro a partir das relações entre coeficientes e raízes:

$$\alpha^0 + \beta^0 + \gamma^0 = 3 = s_0$$

$$\alpha^1 + \beta^1 + \gamma^1 = 0 = s_1$$

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \alpha\gamma) = 0^2 - 2 \cdot (-1) = 2 = s_2$$

Como α, β, γ são inteiros algébricos, basta mostrar que $s_p \equiv 0 \pmod{p}$ no anel $\mathbb{Z}[\alpha, \beta, \gamma]$, já que neste caso $s_p/p \in \mathbb{Z}[\alpha, \beta, \gamma]$ seria um inteiro algébrico racional, portanto inteiro. Mas pelo “sonho de todo estudante” temos

$$s_p = \alpha^p + \beta^p + \gamma^p \equiv (\alpha + \beta + \gamma)^p = 0 \pmod{p}$$

e o resultado segue. \square

Observação 6.46. *A recíproca do resultado acima não é verdadeira. Os naturais n não primos tais que $n \mid s_n$ são os chamados pseudoprimos de Perrin. Há infinitos pseudoprimos de Perrin [61]. Os primeiros são:*

$$\begin{aligned}
 271441 &= 521 \cdot 521 \\
 904631 &= 7 \cdot 13 \cdot 9941 \\
 16532714 &= 2 \cdot 11 \cdot 11 \cdot 53 \cdot 1289 \\
 24658561 &= 19 \cdot 271 \cdot 4789 \\
 27422714 &= 2 \cdot 11 \cdot 11 \cdot 47 \cdot 2411 \\
 27664033 &= 3037 \cdot 9109 \\
 46672291 &= 4831 \cdot 9661 \\
 102690901 &= 5851 \cdot 17551 \\
 130944133 &= 6607 \cdot 19819 \\
 196075949 &= 5717 \cdot 34297
 \end{aligned}$$

Agora seja $K \supset \mathbb{Q}$ uma extensão finita de corpos. Denotamos por \mathcal{O}_K o conjunto dos inteiros algébricos pertencentes a K . Este conjunto é um subanel de K , chamado de *anel de inteiros* de K . Este anel \mathcal{O}_K está para K assim como \mathbb{Z} está para \mathbb{Q} e é o ambiente para o qual queremos estender os resultados obtidos em \mathbb{Z} .

Um corolário imediato do fato de \mathcal{O}_K ser um anel é o seguinte

Corolário 6.47. *Seja $K \supset \mathbb{Q}$ uma extensão finita de corpos e $\theta \in \mathcal{O}_K$. Então $\text{Tr}_{K/\mathbb{Q}}(\theta) \in \mathbb{Z}$ e $N_{K/\mathbb{Q}}(\theta) \in \mathbb{Z}$. Além disso, o polinômio minimal de θ sobre \mathbb{Q} também possui coeficientes inteiros.*

DEMONSTRAÇÃO: Sejam $\sigma_i: K \hookrightarrow \mathbb{C}$, $i = 1, \dots, n$, as n imersões de K em \mathbb{C} e sejam $\theta_i = \sigma_i(\theta)$. Se $p(x) \in \mathbb{Z}[x]$ é um polinômio mônico tal que $p(\theta) = 0$, então $\sigma_i(p(\theta)) = 0 \iff p(\theta_i) = 0$ também, logo os θ_i também são inteiros algébricos. Assim, $\text{Tr}_{K/\mathbb{Q}}(\theta)$ é um inteiro algébrico, sendo soma de inteiros algébricos. Mas como $\text{Tr}_{K/\mathbb{Q}}(\theta) \in \mathbb{Q}$, temos portanto que $\text{Tr}_{K/\mathbb{Q}}(\theta) \in \mathbb{Z}$. O mesmo raciocínio mostra que $N_{K/\mathbb{Q}}(\theta) \in \mathbb{Z}$ e também que os coeficientes do polinômio minimal de θ estão em \mathbb{Z} . \square

Temos a seguinte propriedade, que generaliza o fato de os inteiros algébricos racionais serem inteiros e que será importante no desenvolvimento a seguir.

Proposição 6.48. *O anel \mathcal{O}_K é integralmente fechado em K : se θ é integral sobre \mathcal{O}_K , então $\theta \in \mathcal{O}_K$.*

DEMONSTRAÇÃO: Seja $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ um polinômio mônico com coeficientes em \mathcal{O}_K e tal que $p(\theta) = 0$. Do fato de os a_i serem inteiros algébricos e da relação mônica satisfeita por θ , temos que o anel $\mathbb{Z}[a_0, \dots, a_{n-1}, \theta]$, o menor subanel de \mathbb{C} que contém $a_0, \dots, a_{n-1}, \theta$, é finito sobre \mathbb{Z} . Como $\theta \in \mathbb{Z}[a_0, \dots, a_{n-1}, \theta]$, temos que θ é inteiro algébrico e está em K , ou seja, pertence a \mathcal{O}_K . \square

O primeiro resultado interessante sobre \mathcal{O}_K é que este anel é finito sobre \mathbb{Z} e, ainda melhor, admite uma chamada *base integral*: existe uma base $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ de K sobre \mathbb{Q} tal que qualquer elemento de \mathcal{O}_K se escreve (de maneira única) como combinação linear dos ω_i com coeficientes em \mathbb{Z} . O passo essencial nesta demonstração é o seguinte lema, que fornece um limitante *global* (isto é, um limitante uniforme para todos os elementos de \mathcal{O}_K) para os “denominadores” dos elementos de \mathcal{O}_K :

Lema 6.49 (“Sanduíche”). *Seja $n = [K : \mathbb{Q}]$. Então existe uma base $\omega_1, \dots, \omega_n$ de K sobre \mathbb{Q} e um inteiro $D \in \mathbb{Z}$ não nulo tal que*

$$\mathbb{Z} \cdot \omega_1 + \cdots + \mathbb{Z} \cdot \omega_n \subset \mathcal{O}_K \subset \mathbb{Z} \cdot \frac{\omega_1}{D} + \cdots + \mathbb{Z} \cdot \frac{\omega_n}{D}$$

(isto é, qualquer inteiro algébrico é combinação \mathbb{Z} -linear dos ω_i/D e qualquer combinação \mathbb{Z} -linear dos ω_i é um inteiro algébrico)

DEMONSTRAÇÃO: Seja $\omega_1, \dots, \omega_n$ uma base de K sobre \mathbb{Q} . Como os ω_i são algébricos (pois pertencem a uma extensão finita de \mathbb{Q}), podemos multiplicá-los por um inteiro conveniente de modo a torná-los inteiros algébricos, logo podemos assumir sem perda de generalidade que $\omega_i \in \mathcal{O}_K$ para $i = 1, \dots, n$. Assim, como \mathcal{O}_K é um anel, já temos automaticamente que $\mathbb{Z} \cdot \omega_1 + \cdots + \mathbb{Z} \cdot \omega_n \subset \mathcal{O}_K$.

Por outro lado, seja $\alpha \in \mathcal{O}_K$. Como os ω_i formam uma base de K sobre \mathbb{Q} , podemos escrever $\alpha = a_1\omega_1 + \cdots + a_n\omega_n$ com $a_i \in \mathbb{Q}$. Vamos aplicar novamente o “truque do determinante” (c.f. teorema 6.43): multiplicando a relação anterior por ω_j e tomando traços, obtemos o

“sistema linear” nos a_i :

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega_1) &= a_1 \mathrm{Tr}_{K/\mathbb{Q}}(\omega_1\omega_1) + \cdots + a_n \mathrm{Tr}_{K/\mathbb{Q}}(\omega_n\omega_1) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega_2) &= a_1 \mathrm{Tr}_{K/\mathbb{Q}}(\omega_1\omega_2) + \cdots + a_n \mathrm{Tr}_{K/\mathbb{Q}}(\omega_n\omega_2) \\ &\vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega_n) &= a_1 \mathrm{Tr}_{K/\mathbb{Q}}(\omega_1\omega_n) + \cdots + a_n \mathrm{Tr}_{K/\mathbb{Q}}(\omega_n\omega_n)\end{aligned}$$

Note que como $\alpha\omega_i$ e $\omega_i\omega_j$ são todos inteiros algébricos, todos os traços são inteiros. Assim, o determinante $D = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j))$ (chamado de *discriminante* da base ω_i) pertence a \mathbb{Z} . O lema a seguir mostra que $D \neq 0$. Pela regra de Cramer temos que $a_i \in \mathbb{Z} \cdot D^{-1}$, logo $\mathcal{O}_K \subset \mathbb{Z} \cdot \frac{\omega_1}{D} + \cdots + \mathbb{Z} \cdot \frac{\omega_n}{D}$. \square

O seguinte lema sobre discriminantes termina a prova do lema anterior.

Lema 6.50. *Sejam $\omega_1, \dots, \omega_n$ e τ_1, \dots, τ_n bases de K sobre \mathbb{Q} e seja $C = (c_{ij})$ a matriz de mudança de base:*

$$\omega_i = c_{i1}\tau_1 + \cdots + c_{in}\tau_n \quad i = 1, \dots, n.$$

Sejam $\Delta(\omega_1, \dots, \omega_n) = (\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j))$ e $\Delta(\tau_1, \dots, \tau_n) = (\mathrm{Tr}_{K/\mathbb{Q}}(\tau_i\tau_j))$ os discriminantes das duas bases. Então

$$\Delta(\omega_1, \dots, \omega_n) = \Delta(\tau_1, \dots, \tau_n) \cdot (\det C)^2$$

e ambos os discriminantes são não nulos.

DEMONSTRAÇÃO: Sejam $\sigma_i: K \hookrightarrow \mathbb{C}$ as imersões de K em \mathbb{C} e considere a matriz $\delta(\omega_1, \dots, \omega_n) = (\sigma_j(\omega_i))$. Multiplicando pela transposta, temos

$$\delta(\omega_1, \dots, \omega_n) \cdot \delta(\omega_1, \dots, \omega_n)^T = \left(\sum_{1 \leq k \leq n} \sigma_k(\omega_i) \sigma_k(\omega_j) \right) = \left(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j) \right).$$

Por outro lado,

$$\delta(\omega_1, \dots, \omega_n) = \left(\sum_{1 \leq k \leq n} c_{ik} \sigma_j(\tau_k) \right) = C \cdot \delta(\tau_1, \dots, \tau_n).$$

Assim,

$$\begin{aligned}\Delta(\omega_1, \dots, \omega_n) &= (\det \delta(\omega_1, \dots, \omega_n))^2 = (\det C)^2 \cdot (\det \delta(\tau_1, \dots, \tau_n))^2 \\ &= (\det C)^2 \cdot \Delta(\tau_1, \dots, \tau_n)\end{aligned}$$

Como $\det C \neq 0$, para mostrar que estes discriminantes são não nulos, basta mostrar isto para uma base específica. Escrevendo $K = \mathbb{Q}(\theta)$ (teorema do elemento primitivo 6.33), temos que $1, \theta, \dots, \theta^{n-1}$ é uma base de K sobre \mathbb{Q} . Sendo $\theta_i = \sigma_i(\theta)$ os conjugados de θ , temos o determinante de Vandermonde

$$\det \delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = \det(\theta_j^{i-1}) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \neq 0.$$

Este determinante, e portanto $\Delta(1, \theta, \dots, \theta^{n-1}) = \det \delta(1, \theta, \dots, \theta^{n-1})^2$, são não nulos pois os conjugados θ_i são dois a dois distintos (ver final da demonstração do teorema 6.35). \square

Agora podemos completar a prova do

Teorema 6.51 (Base Integral). *Seja $n = [K : \mathbb{Q}]$. Então existe uma base de K sobre \mathbb{Q} $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ tal que qualquer inteiro algébrico em \mathcal{O}_K se escreve (de maneira única) como combinação linear dos ω_i com coeficientes em \mathbb{Z} :*

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n.$$

DEMONSTRAÇÃO: Já sabemos que existe uma base $\tau_1, \dots, \tau_n \in \mathcal{O}_K$ de K sobre \mathbb{Q} e um inteiro positivo D tal que

$$\mathbb{Z} \cdot \tau_1 + \dots + \mathbb{Z} \cdot \tau_n \subset \mathcal{O}_K \subset \mathbb{Z} \cdot \frac{\tau_1}{D} + \dots + \mathbb{Z} \cdot \frac{\tau_n}{D}.$$

Agora, para $i = 1, 2, \dots, n$, defina

$$N_i = \left\{ a_i \frac{\tau_i}{D} + \dots + a_n \frac{\tau_n}{D} \in \mathcal{O}_K \mid a_i, a_{i+1}, \dots, a_n \in \mathbb{Z} \right\}.$$

Note que como $\tau_i = D \cdot \frac{\tau_i}{D} \in N_i$, temos que $N_i \neq \{0\}$. Escolha $\omega_i \in N_i$ tal que o coeficiente $a_i > 0$ de $\frac{\tau_i}{D}$ seja mínimo.

Vamos mostrar que os elementos ω_i assim obtidos geram \mathcal{O}_K sobre \mathbb{Z} . Seja β um elemento qualquer de \mathcal{O}_K e escreva $\beta = b_1 \frac{\tau_1}{D} + \dots + b_n \frac{\tau_n}{D} \in$

\mathcal{O}_K , $b_i \in \mathbb{Z}$. Seja a_1 o coeficiente de $\frac{\tau_1}{D}$ em ω_1 . Dividindo b_1 por a_1 , obtemos quociente q_1 e resto r_1 : $b_1 = a_1 q_1 + r_1$ com $0 \leq r_1 < a_1$. Como \mathcal{O}_K é um anel, $\beta - q_1 \omega_1 \in \mathcal{O}_K$ e como o coeficiente de $\frac{\tau_1}{D}$ neste elemento é r_1 , pela minimalidade de a_1 devemos ter $r_1 = 0$, de modo que $\beta - q_1 \omega_1 \in N_2$. Procedendo analogamente, obtemos $q_2 \in \mathbb{Z}$ tal que $\beta - q_1 \omega_1 - q_2 \omega_2 \in N_3$, e assim sucessivamente até que finalmente tenhamos $\beta - q_1 \omega_1 - \cdots - q_n \omega_n = 0$, mostrando que β é uma combinação \mathbb{Z} -linear dos ω_i . Assim,

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

Como qualquer elemento de K é o quociente de um elemento de \mathcal{O}_K e um inteiro, temos que os ω_i geram K sobre \mathbb{Q} . Como há n elementos, os ω_i formam portanto uma base de K sobre \mathbb{Q} . \square

Exemplo 6.52. *Mostre que $1, \frac{1+\sqrt{5}}{2}$ é uma base integral do anel de inteiros em $\mathbb{Q}(\sqrt{5})$.*

SOLUÇÃO: Temos que 1 e $\omega = \frac{1+\sqrt{5}}{2}$ formam uma base de $\mathbb{Q}(\sqrt{5})$ sobre \mathbb{Q} . Como são inteiros algébricos, temos $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \supset \mathbb{Z} + \mathbb{Z}\omega$. Reciprocamente, seja $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. Podemos escrever α como $\alpha = \frac{a+b\omega}{d}$ para $a, b, d \in \mathbb{Z}$ e sem fatores comuns. Temos

$$\text{Tr}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(\alpha) = \frac{2a+b}{d} \in \mathbb{Z} \quad \text{e} \quad N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(\alpha) = \frac{a^2 + ab - b^2}{d^2} \in \mathbb{Z}.$$

Queremos mostrar que $d = \pm 1$. Suponha que não e seja p um fator primo de d . Temos $b \equiv -2a \pmod{p}$ e $a^2 + ab - b^2 \equiv 0 \pmod{p}$, donde obtemos $5a^2 \equiv 0 \pmod{p}$. Se $p \mid a$, então de $b \equiv -2a \pmod{p}$ temos que $p \mid b$, o que contradiz o fato de a, b, d não terem fatores comuns. Logo a única possibilidade é $p = 5$ com $5 \nmid a$ e $5 \nmid b$. Mas de $a^2 + ab - b^2 \equiv 0 \pmod{25}$, temos que $(\frac{a}{b})^2 + \frac{a}{b} - 1 \equiv 0 \pmod{25}$, que não possui solução, uma contradição. \square

6.5 Ideais

A aritmética do anel de inteiros de extensões finitas de \mathbb{Q} não é tão simples como os casos estudados no início deste capítulo. Um dos principais empecilhos é a falta de fatoração única em elementos irredutíveis.

Considere por exemplo $K = \mathbb{Q}(i\sqrt{5})$, cujo anel de inteiros é $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$. Temos

$$3 \cdot 7 = (1 + 2i\sqrt{5})(1 - 2i\sqrt{5})$$

e todos os fatores $3, 7, 1 \pm 2i\sqrt{5}$ são irredutíveis em $\mathbb{Z}[i\sqrt{5}]$! Por exemplo, suponha que $1 + 2i\sqrt{5} = \alpha\beta$ com $\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$. Então, tomando normas, obtemos $21 = N(1 + 2i\sqrt{5}) = N(\alpha)N(\beta)$ e portanto $N(\alpha) \in \{1, 3, 7, 21\}$. Escrevendo $\alpha = m + ni\sqrt{5}$ com $m, n \in \mathbb{Z}$, temos $m^2 + 5n^2 = 1, 3, 7$ ou 21 e checando as possibilidades concluímos que α ou β é igual a ± 1 . Da mesma forma, mostra-se que $3, 7, 1 - 2i\sqrt{5}$ são também irredutíveis.

O que deu errado? O problema é que os elementos irredutíveis ainda não são os “blocos atômicos”, ou seja, a fatoração acima ainda pode ser refinada. Por exemplo, 3 e $1 + 2i\sqrt{5}$ não são “relativamente primos”: se este fosse o caso, esperaríamos que a equação $3\alpha + (1 + 2i\sqrt{5})\beta = 1$ tivesse solução em $\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$, o que não ocorre: se $\alpha = a + bi\sqrt{5}$ e $\beta = c + di\sqrt{5}$ com $a, b, c, d \in \mathbb{Z}$, temos

$$\begin{aligned} 1 &= 3(a + bi\sqrt{5}) + (1 + 2i\sqrt{5})(c + di\sqrt{5}) \\ \implies 1 &\equiv (c - 10d) + (2c + d)i\sqrt{5} \pmod{3} \\ \iff \begin{cases} c - d \equiv 1 \pmod{3} \\ 2c + d \equiv 0 \pmod{3}. \end{cases} \end{aligned}$$

Mas multiplicando a primeira equação do sistema por 2, obtemos $2c + d \equiv 2 \pmod{3}$, o que é impossível.

O “conserto” se dá considerando-se fatorações não em elementos mas sim nos chamados *ideais*, que são subconjuntos de \mathcal{O}_K que generalizam a noção de conjunto de múltiplos. No exemplo acima, o conjunto $\{3\alpha + (1 + 2i\sqrt{5})\beta \mid \alpha, \beta \in \mathbb{Z}[i\sqrt{5}]\}$ tomará o papel de “mdc” entre 3 e $1 + 2i\sqrt{5}$ e assim poderemos recuperar a tão preciosa fatoração única.

Definição 6.53. *Seja A um anel comutativo. Um subconjunto $\mathfrak{a} \subset A$ é chamado de ideal se*

1. \mathfrak{a} é um subgrupo aditivo de A , i.e., $a, b \in \mathfrak{a} \implies a + b, a - b \in \mathfrak{a}$;
2. \mathfrak{a} é fechado por multiplicação por elementos arbitrários de A : se $a \in \mathfrak{a}$ e $r \in A$ então $ra \in \mathfrak{a}$.

Por exemplo, dados elementos $a_1, \dots, a_n \in A$, o conjunto de suas

combinações A -lineares

$$(a_1, \dots, a_n) \stackrel{\text{def}}{=} \{a_1 \cdot x_1 + \dots + a_n \cdot x_n \mid x_1, \dots, x_n \in A\}$$

é um ideal de A , chamado *ideal gerado por* a_1, \dots, a_n . Em particular, temos que (d) é o conjunto dos múltiplos de d . Ideais que podem ser gerados por um único elemento são chamados de *ideais principais*. Por exemplo, em \mathbb{Z} temos que o ideal $(12, 21)$ é principal, pois ele é igual ao ideal (3) , já que o conjunto das combinações \mathbb{Z} -lineares de 12 e 21 é o conjunto dos múltiplos de $\text{mdc}(12, 21) = 3$. Mais geralmente, a mesma demonstração do teorema de Bachet-Bézout mostra que

Proposição 6.54. *Nos anéis \mathbb{Z} , $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ e $K[x]$, K um corpo, todos os ideais são principais.*

Em jargão algébrico, dizemos que todo *domínio euclidiano* é *domínio de ideais principais*. Veremos mais tarde (teorema 6.79) que o contrário não é necessariamente verdadeiro, por exemplo o anel de inteiros de $\mathbb{Q}(i\sqrt{19})$ é principal mas não euclidiano.

Ideais não são muito diferentes de números. Por exemplo, podemos somar e multiplicar ideais: dados dois ideais \mathfrak{a} e \mathfrak{b} , definimos

$$\begin{aligned}\mathfrak{a} + \mathfrak{b} &\stackrel{\text{def}}{=} \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \\ \mathfrak{a}\mathfrak{b} &\stackrel{\text{def}}{=} \{a_1b_1 + \dots + a_nb_n \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}\end{aligned}$$

Por exemplo, para ideais finitamente gerados temos

$$\begin{aligned}(a_1, \dots, a_m) \cdot (b_1, \dots, b_n) &= (a_1b_1, a_1b_2, \dots, a_ib_j, \dots, a_mb_n) \\ (a_1, \dots, a_m) + (b_1, \dots, b_n) &= (a_1, \dots, a_m, b_1, \dots, b_n)\end{aligned}$$

Observe que (1) funciona como identidade para multiplicação de ideais.

Por exemplo, em \mathbb{Z} temos que $(a) + (b) = (a, b) = (\text{mdc}(a, b))$ pelo teorema de Bachet-Bézout e que $(a) \cdot (b) = (ab)$. Por outro lado, $(a) \supset (b) \iff a \mid b$. Assim, estas operações com ideais generalizam operações numéricas usuais, e é bom ter em mente o seguinte “dicionário”:

números	ideais
$a \mid b$	$\mathfrak{a} \supset \mathfrak{b}$
$\text{mdc}(a, b)$	$\mathfrak{a} + \mathfrak{b}$
$a \cdot b$	$\mathfrak{a} \cdot \mathfrak{b}$

Podemos ainda definir congruências para ideais: se \mathfrak{a} é um ideal do anel A , escrevemos

$$a \equiv b \pmod{\mathfrak{a}} \iff a - b \in \mathfrak{a}$$

para $a, b \in A$. Naturalmente, se $\mathfrak{a} = (c)$ é principal, a definição acima nada mais é do que a nossa velha congruência módulo c , mas a nova definição se aplica a mais casos e sem dificuldades adicionais. Temos ainda as mesmas propriedades bem conhecidas:

$$\begin{cases} a \equiv b \pmod{\mathfrak{a}} \\ c \equiv d \pmod{\mathfrak{a}} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{\mathfrak{a}} \\ a - c \equiv b - d \pmod{\mathfrak{a}} \\ ac \equiv bd \pmod{\mathfrak{a}} \end{cases}.$$

Por exemplo, vamos provar a última congruência. Por hipótese, temos $a - b \in \mathfrak{a}$ e $c - d \in \mathfrak{a}$. Logo, multiplicando a primeira relação por c e a segunda por b , obtemos $ac - bc \in \mathfrak{a}$ e $bc - bd \in \mathfrak{a}$. Somando as duas relações, obtemos $ac - bd \in \mathfrak{a} \iff ac \equiv bd \pmod{\mathfrak{a}}$, como queríamos.

Como a relação de congruência é compatível com a soma e o produto, podemos formar o anel quociente A/\mathfrak{a} , cujos elementos são as classes de congruência $\bar{a} = \{b \in A \mid b \equiv a \pmod{\mathfrak{a}}\}$ para $a \in A$. As operações são definidas de maneira natural

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{e} \quad \bar{a} \cdot \bar{b} = \overline{ab}$$

e não dependem da escolha dos representantes a e b pelas propriedades de congruência módulo \mathfrak{a} acima.

Agora precisamos decidir quais ideais farão o papel dos “blocos atômicos”. Dois candidatos surgem naturalmente:

Definição 6.55. *Seja A um anel comutativo.*

1. *Um ideal $\mathfrak{p} \subset A$ é dito primo se \mathfrak{p} é um ideal próprio (i.e. $\mathfrak{p} \neq A$) e $ab \in \mathfrak{p} \iff a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$;*
2. *Um ideal $\mathfrak{m} \subset A$ é dito maximal se \mathfrak{m} é maximal dentre os ideais próprios de A , ordenados por inclusão, ou seja, $A \supsetneq \mathfrak{a} \supset \mathfrak{m} \implies \mathfrak{a} = \mathfrak{m}$.*

Lembre que um anel comutativo A é chamado de *domínio* se $A \neq 0$ e $ab = 0 \implies a = 0$ ou $b = 0$. Por exemplo, \mathbb{Z} é um domínio e \mathbb{Z}/n é

um domínio se, e somente se, n é um número primo, pois se $n = ab$ com $a, b > 1$ então $\bar{a} \neq 0$ e $\bar{b} \neq 0$ mas $\bar{a} \cdot \bar{b} = 0$ em \mathbb{Z}/n . Em termos de anel quociente, temos portanto que um ideal \mathfrak{p} de A é primo se, e só se, A/\mathfrak{p} é um domínio. Assim, um ideal (n) de \mathbb{Z} é primo se, e somente se, $n = 0$ ou n é um número primo.

Podemos também caracterizar um ideal maximal em termos de quocientes. Suponha que \mathfrak{m} seja maximal e seja $a \notin \mathfrak{m}$. Então $(a) + \mathfrak{m} = (1)$, pois o ideal $(a) + \mathfrak{m}$ contém propriamente \mathfrak{m} . Assim, existe b tal que $ab \equiv 1 \pmod{\mathfrak{m}}$, ou seja, mostramos que todo $a \not\equiv 0 \pmod{\mathfrak{m}}$ possui inverso multiplicativo módulo \mathfrak{m} , ou que A/\mathfrak{m} é um corpo. A recíproca também é verdadeira: se A/\mathfrak{m} é corpo e \mathfrak{a} é um ideal que contém propriamente \mathfrak{m} , então $\mathfrak{a} = A$. De fato, tome $a \in \mathfrak{a} \setminus \mathfrak{m}$ e seja b tal que $ab \equiv 1 \pmod{\mathfrak{m}}$, que existe pois \bar{a} não é zero em A/\mathfrak{m} . Assim, $ab - 1 \in \mathfrak{m} \subset \mathfrak{a} \implies -1 \in \mathfrak{a}$ pois $a \in \mathfrak{a}$. Mas então todo elemento de A pertence a \mathfrak{a} . Utilizando este critério, temos que um ideal (n) de \mathbb{Z} é maximal se, e só se, n é um número primo.

Lema 6.56. *Seja A um anel comutativo.*

1. *Um ideal \mathfrak{p} é primo se, e só se, A/\mathfrak{p} é um domínio. Um ideal \mathfrak{m} é maximal se, e só se, A/\mathfrak{m} é um corpo. Em particular, como todo corpo é domínio, todo ideal maximal é primo.*

2. *Se $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ são ideais arbitrários e \mathfrak{p} é um ideal primo então*

$$\mathfrak{p} \supset \mathfrak{a}_1 \cdots \mathfrak{a}_n \implies \mathfrak{p} \supset \mathfrak{a}_i \text{ para algum } i$$

(ou seja, se um ideal primo \mathfrak{p} “divide” um produto de ideais, então ele “divide” um destes ideais)

DEMONSTRAÇÃO: Temos só que provar (2). Suponha, por absurdo, que \mathfrak{p} não contém nenhum \mathfrak{a}_i e sejam $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$. Mas então $\prod_{1 \leq i \leq n} a_i \in \prod_{1 \leq i \leq n} \mathfrak{a}_i \subset \mathfrak{p}$ embora nenhum a_i pertença a \mathfrak{p} , uma contradição. \square

Como provaremos no final desta seção, para anéis “aritméticos,” como os anéis de inteiros \mathcal{O}_K de uma extensão finita K de \mathbb{Q} , os dois conceitos, ideal primo e ideal maximal, coincidem a menos do ideal (0) , que é primo mas não maximal. Na próxima subseção, mostraremos que todo ideal não nulo em \mathcal{O}_K se fatora de maneira única (a menos da ordem dos fatores) em um produto de ideais primos.

Exemplo 6.57. Em $\mathbb{Z}[i\sqrt{5}]$, encontre uma fatoração dos ideais (3) e (7) em ideais maximais.

SOLUÇÃO: De $3 \cdot 7 = (1 - 2i\sqrt{5})(1 + 2i\sqrt{5})$, temos que um bom início é tentar olhar para os ideais $(3, 1 \pm 2i\sqrt{5})$ (o “mdc” de 3 e $1 \pm 2i\sqrt{5}$) e $(7, 1 \pm 2i\sqrt{5})$. Todos estes ideais são maximais. Por exemplo, vamos mostrar que $\mathbb{Z}[i\sqrt{5}]/(3, 1 + 2i\sqrt{5})$ é um corpo, isomorfo a $\mathbb{Z}/(3)$. Temos

$$1 \equiv -2i\sqrt{5} \pmod{(3, 1 + 2i\sqrt{5})} \implies 1 \equiv i\sqrt{5} \pmod{(3, 1 + 2i\sqrt{5})}$$

Assim, para $a, b \in \mathbb{Z}$ temos

$$a + bi\sqrt{5} \equiv a + b \pmod{(3, 1 + 2i\sqrt{5})}.$$

Isto mostra que todo elemento de $\mathbb{Z}[i\sqrt{5}]/(3, 1 + 2i\sqrt{5})$ pode ser representado por um inteiro módulo 3, de modo que o mapa $\mathbb{Z}/(3) \rightarrow \mathbb{Z}[i\sqrt{5}]/(3, 1 + 2i\sqrt{5})$ dado por $a \bmod (3) \mapsto a \bmod (3, 1 + 2i\sqrt{5})$ é sobrejetor. Ele também é injetor, pois, como já vimos no começo desta seção, $1 \notin (3, 1 + 2i\sqrt{5})$, e $2 \in (3, 1 + 2i\sqrt{5}) \implies 1 = 3 - 2 \in (3, 1 + 2i\sqrt{5})$, que também é impossível. Logo este mapa é um isomorfismo.

Temos agora

$$\begin{aligned} (3, 1 + 2i\sqrt{5})(3, 1 - 2i\sqrt{5}) &= (9, 3 + 6i\sqrt{5}, 3 - 6i\sqrt{5}, 21) \\ &= (3) \cdot (3, 1 + 2i\sqrt{5}, 1 - 2i\sqrt{5}, 7) = (3) \end{aligned}$$

pois $(3, 1 + 2i\sqrt{5}, 1 - 2i\sqrt{5}, 7) = (1)$ já que $1 = 7 - 2 \cdot 3$. Da mesma forma, temos que uma fatoração de (7) em ideais maximais é

$$(7, 1 + 2i\sqrt{5})(7, 1 - 2i\sqrt{5}) = (7).$$

Isto “explica” a falha da fatoração única em irredutíveis dada por $3 \cdot 7 = (1 - 2i\sqrt{5})(1 + 2i\sqrt{5})$, pois rearranjando os fatores obtemos

$$\begin{aligned} (3) \cdot (7) &= (3, 1 + 2i\sqrt{5})(3, 1 - 2i\sqrt{5}) \cdot (7, 1 + 2i\sqrt{5})(7, 1 - 2i\sqrt{5}) \\ &= (3, 1 + 2i\sqrt{5})(7, 1 + 2i\sqrt{5}) \cdot (3, 1 - 2i\sqrt{5})(7, 1 - 2i\sqrt{5}) \\ &= (1 + 2i\sqrt{5}) \cdot (1 - 2i\sqrt{5}) \end{aligned}$$

□

Precisamos só de mais um conceito, que servirá de substituto para o PIF e para o princípio da boa ordem quando estivermos trabalhando com ideais. Observe que em inteiros positivos, não podemos ter uma sequência infinita $d_2 \mid d_1, d_3 \mid d_2, d_4 \mid d_3, \dots$ a menos que a sequência estabilize, isto é, $d_i = d_{i+1}$ para todo i suficientemente grande. Traduzindo isto em termos de ideais, temos a

Definição 6.58. *Um anel comutativo A é noetheriano se satisfaz qualquer uma das seguintes propriedades equivalentes:*

1. *todo ideal \mathfrak{a} de A é finitamente gerado;*
2. *toda cadeia ascendente de ideais estabiliza, isto é, dada uma cadeia de ideais*

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \dots$$

então $\mathfrak{a}_i = \mathfrak{a}_{i+1}$ para i suficientemente grande;

3. *todo conjunto não vazio \mathcal{I} de ideais possui um ideal \mathfrak{a} que é maximal em \mathcal{I} com relação à inclusão, i.e., $\mathfrak{b} \in \mathcal{I}$ e $\mathfrak{b} \supseteq \mathfrak{a} \implies \mathfrak{b} = \mathfrak{a}$.*

As equivalências entre as condições acima são simples:

- (1) \implies (2) Tome $\mathfrak{a} = \bigcup_{i \geq 0} \mathfrak{a}_i$, que é um ideal de A : dados $a, b \in \mathfrak{a}$ e $r \in A$, escolha i grande o suficiente para que $a, b \in \mathfrak{a}_i$, de modo que $a + b \in \mathfrak{a}_i \subset \mathfrak{a}$ e $ra \in \mathfrak{a}_i \subset \mathfrak{a}$. Sejam $a_1, \dots, a_n \in A$ geradores de \mathfrak{a} . Então existe um i_0 grande suficiente tal que $a_1, \dots, a_n \in \mathfrak{a}_{i_0}$, logo $\mathfrak{a} = \mathfrak{a}_{i_0}$ e portanto $\mathfrak{a}_i = \mathfrak{a}_{i+1}$ para todo $i \geq i_0$.
- (2) \implies (1) Seja \mathfrak{a} um ideal e tome $a_1 \in \mathfrak{a}$. Se $(a_1) \neq \mathfrak{a}$, tome $a_2 \in \mathfrak{a} \setminus (a_1)$. Se $(a_1, a_2) \neq \mathfrak{a}$, tome $a_3 \in \mathfrak{a} \setminus (a_1, a_2)$. E assim por diante. Como a cadeia $(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \dots$ estabiliza, temos que $\mathfrak{a} = (a_1, \dots, a_n)$ para algum n .
- (2) \implies (3) Suponha que \mathcal{I} não possua elemento maximal e seja $\mathfrak{a}_0 \in \mathcal{I}$. Então existe $\mathfrak{a}_1 \in \mathcal{I}$ tal que $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1$. Repetindo este procedimento, obtemos uma cadeia ascendente estrita $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \dots$, o que é um absurdo.
- (3) \implies (2) Dada uma cadeia ascendente $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$, tome $\mathcal{I} = \{\mathfrak{a}_i \mid i \geq 0\}$. Se \mathfrak{a}_{i_0} é um elemento maximal de \mathcal{I} então devemos ter $\mathfrak{a}_i = \mathfrak{a}_{i+1}$ para todo $i \geq i_0$.

O PIF pode ser utilizado para demonstrar que todo inteiro positivo pode ser fatorado como produto de primos. Como ilustração do “princípio de indução noetheriana”, vamos mostrar que todo ideal não nulo “divide” um produto de ideais primos não nulos:

Lema 6.59. *Seja A um domínio noetheriano. Então todo ideal $\mathfrak{a} \neq (0)$ contém um produto de ideais primos não nulos.*

DEMONSTRAÇÃO: Suponha que isto seja falso e seja \mathcal{I} o conjunto dos ideais não nulos que violam o enunciado. Seja \mathfrak{b} um elemento maximal em \mathcal{I} . Por hipótese, \mathfrak{b} não é primo, logo existem $a, b \notin \mathfrak{b}$ tais que $ab \in \mathfrak{b}$. Como $(a) + \mathfrak{b} \supsetneq \mathfrak{b}$ e $(b) + \mathfrak{b} \supsetneq \mathfrak{b}$, pela maximalidade de \mathfrak{b} em \mathcal{I} temos que ambos os ideais $(a) + \mathfrak{b}$ e $(b) + \mathfrak{b}$ contêm produtos de ideais primos não nulos. Mas neste caso, como $ab \in \mathfrak{b}$, temos que $\mathfrak{b} \supset ((a) + \mathfrak{b}) \cdot ((b) + \mathfrak{b})$ e, assim, \mathfrak{b} também contém um produto de ideais primos não nulos, uma contradição. \square

Seja \mathcal{O}_K o anel de inteiros de uma extensão finita K de \mathbb{Q} . Seja $\omega_1, \dots, \omega_n$ uma base integral de \mathcal{O}_K . Observe que dado um ideal não nulo \mathfrak{a} e um elemento $a \in \mathfrak{a}$, $a \neq 0$, temos

$$\mathbb{Z}a\omega_1 + \dots + \mathbb{Z}a\omega_n \subset \mathfrak{a} \subset \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$$

e portanto a mesma prova do teorema 6.51 mostra a existência de uma base integral para \mathfrak{a} , i.e., uma base τ_1, \dots, τ_n de K sobre \mathbb{Q} tal que

$$\mathfrak{a} = \mathbb{Z}\tau_1 + \dots + \mathbb{Z}\tau_n.$$

Isto mostra em particular que todo ideal de \mathcal{O}_K é finitamente gerado, ou seja, que \mathcal{O}_K é noetheriano.

Escrevendo os τ_i em função dos ω_j , obtemos

$$\tau_i = \sum_{1 \leq j \leq n} a_{ij} \omega_j, \quad a_{ij} \in \mathbb{Z}$$

para $i = 1, \dots, n$. Da prova do teorema 6.51, podemos supor que a matriz (a_{ij}) é uma matriz triangular superior, de modo que é fácil ver que os elementos da forma $\sum_{1 \leq i \leq n} r_i \omega_i$ com $0 \leq r_i < |a_{ii}|$, $i = 1, \dots, n$, formam um sistema completo de restos módulo \mathfrak{a} e assim

$$|\mathcal{O}_K/\mathfrak{a}| = \prod_{1 \leq i \leq n} |a_{ii}| = |\det(a_{ij})|.$$

Em particular, os anéis quociente $\mathcal{O}_K/\mathfrak{a}$ são sempre finitos! Note ainda que se temos outra base integral τ'_j para \mathfrak{a} , escrevendo B e C para as matrizes (com entradas inteiras) de mudança de base de τ'_j para τ_j e vice-versa, temos que $BC = I \implies \det B \det C = 1$, logo $\det B = \det C = \pm 1$ e assim a fórmula $|\mathcal{O}_K/\mathfrak{a}| = |\det(a_{ij})|$ é válida para todas as bases integrais de \mathfrak{a} (e não só para a base “triangular superior” da prova do teorema 6.51).

Resumimos a discussão acima em um

Lema 6.60. *Seja K uma extensão finita de \mathbb{Q} e seja \mathfrak{a} um ideal não nulo de \mathcal{O}_K . Então o anel quociente $\mathcal{O}_K/\mathfrak{a}$ é finito. Além disso, se $\omega_1, \dots, \omega_n$ e τ_1, \dots, τ_n são bases integrais de \mathcal{O}_K e \mathfrak{a} , respectivamente, e $a_{ij} \in \mathbb{Z}$ são tais que*

$$\tau_i = \sum_{1 \leq j \leq n} a_{ij} \omega_j$$

então $|\mathcal{O}_K/\mathfrak{a}| = |\det(a_{ij})|$.

A seguinte proposição será fundamental na demonstração da fatoração única em ideais primos:

Proposição 6.61. *Seja K uma extensão finita de \mathbb{Q} . Então*

1. \mathcal{O}_K é integralmente fechado;
2. \mathcal{O}_K é noetheriano;
3. todo ideal primo não nulo de \mathcal{O}_K é maximal.

DEMONSTRAÇÃO: O primeiro item é o conteúdo da proposição 6.48 e o segundo decorre da discussão acima, tendo sido repetidos aqui apenas por conveniência. Para o terceiro item, seja $\mathfrak{p} \neq (0)$ um ideal primo. Então ele é maximal, pois um domínio finito $D = \mathcal{O}_K/\mathfrak{p}$ é sempre um corpo: se $d \in D$ e $d \neq 0$, as potências $1, d, d^2, \dots$ formam um conjunto finito, logo existe $i > j$ tal que $d^i = d^j \iff d^j(d^{i-j} - 1) = 0$ e como D é domínio, temos $d^{i-j} = 1$ com $i - j > 0$, logo d é invertível em D . \square

Observação 6.62. *Um domínio que satisfaz as três condições da proposição anterior é chamado de domínio de Dedekind. Pode-se mostrar, por exemplo, que o anel de polinômios $K[x]$ com coeficientes em um corpo K é um domínio de Dedekind. Como veremos a seguir, os três axiomas acima são exatamente os ingredientes necessários à prova da fatoração única em ideais primos, que vale em qualquer domínio de Dedekind.*

6.5.1 Fatoração Única em Ideais Primos

Seja K uma extensão finita de \mathbb{Q} . Nesta seção, vamos provar a existência e unicidade da fatoração em ideais primos. Para isto, é conveniente estendermos ligeiramente o conceito de ideal:

Definição 6.63. *Um subconjunto $\mathfrak{f} \subset K$ é chamado de ideal fracionário de \mathcal{O}_K se existe um ideal $\mathfrak{a} \subset \mathcal{O}_K$ e um elemento não nulo $d \in \mathcal{O}_K$ tal que*

$$\mathfrak{f} = \frac{1}{d} \cdot \mathfrak{a} \stackrel{\text{def}}{=} \left\{ \frac{a}{d} \mid a \in \mathfrak{a} \right\}.$$

Por exemplo, dados elementos arbitrários $a_1, \dots, a_n \in K$ temos que

$$(a_1, \dots, a_n) \stackrel{\text{def}}{=} \{a_1x_1 + \dots + a_nx_n \mid x_i \in \mathcal{O}_K\}$$

é um ideal fracionário de \mathcal{O}_K . Ideais fracionários podem ser somados e multiplicados da mesma forma que ideais comuns.

Lema 6.64. *Sejam \mathfrak{f} um ideal fracionário de \mathcal{O}_K . Se $a \in K$ é um elemento tal que $a\mathfrak{f} \subset \mathfrak{f}$, então $a \in \mathcal{O}_K$.*

DEMONSTRAÇÃO: Vamos novamente utilizar o “truque do determinante” (c.f. teorema 6.43). Como todo ideal de \mathcal{O}_K é finitamente gerado, o mesmo vale para seus ideais fracionários, de modo que podemos escrever

$$\mathfrak{f} = (\omega_1, \dots, \omega_n), \quad \omega_i \in K$$

Como $a\mathfrak{f} \subset \mathfrak{f}$, temos o “sistema” linear nas “variáveis” ω_i :

$$a\omega_i = \sum_{1 \leq j \leq n} m_{ij}\omega_j \quad m_{ij} \in \mathcal{O}_K.$$

Sendo M a matriz (m_{ij}) , temos que a é uma raiz do polinômio mônico característico $p(x) = \det(x \cdot I - M)$ com coeficientes em \mathcal{O}_K , logo a é integral sobre \mathcal{O}_K . Como \mathcal{O}_K é integralmente fechado, temos que $a \in \mathcal{O}_K$. \square

O passo essencial na prova da fatoração única é a seguinte proposição, que permite “inverter” ideais primos:

Proposição 6.65. *Seja \mathfrak{p} um ideal primo não nulo de \mathfrak{D}_K . Seja \mathfrak{p}^{-1} o ideal fracionário*

$$\mathfrak{p}^{-1} \stackrel{\text{def}}{=} \{a \in K \mid a\mathfrak{p} \subset \mathcal{O}_K\}.$$

Então $\mathfrak{p}\mathfrak{p}^{-1} = (1)$.

DEMONSTRAÇÃO: Observe primeiramente que para qualquer $d \in \mathfrak{p}$, temos que $d\mathfrak{p}^{-1}$ é um ideal ordinário de \mathcal{O}_K , logo \mathfrak{p}^{-1} é de fato um ideal fracionário. Note também que $\mathfrak{p}^{-1} \supset \mathcal{O}_K$ e que $\mathfrak{p}\mathfrak{p}^{-1}$ é um ideal ordinário de \mathcal{O}_K que contém o ideal maximal \mathfrak{p} , logo para provar que $\mathfrak{p}\mathfrak{p}^{-1} = (1)$, basta mostrar que $\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}$.

Suponha por absurdo que $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Pelo lema, isto implica que $\mathfrak{p}^{-1} = \mathcal{O}_K$. Vamos mostrar que isto leva a uma contradição. Tome qualquer elemento não nulo $a \in \mathfrak{p}$. Pelo lema 6.59, existem ideais primos não nulos \mathfrak{p}_i tais que $(a) \supset \mathfrak{p}_1 \dots \mathfrak{p}_k$; podemos assumir que k é minimal com esta propriedade. Observe que $\mathfrak{p} \supset (a)$ logo $\mathfrak{p} \supset \mathfrak{p}_1$, digamos, e como ambos os ideais são maximais, temos $\mathfrak{p}_1 = \mathfrak{p}$. Agora, pela minimalidade de k , existe $b \in \mathfrak{p}_2 \dots \mathfrak{p}_k$ tal que $b \notin (a)$, i.e., $b/a \notin \mathcal{O}_K$. Como $(a) \supset b \cdot \mathfrak{p}$, temos $(b/a) \cdot \mathfrak{p} \subset \mathcal{O}_K$. Mas então $b/a \in \mathfrak{p}^{-1}$, contradizendo $\mathfrak{p}^{-1} = \mathcal{O}_K$. \square

Teorema 6.66 (Fatoração Única). *Qualquer ideal não nulo de \mathcal{O}_K escreve-se como produto de ideais primos. Esta fatoração é única a menos da ordem dos fatores.*

DEMONSTRAÇÃO: Primeiramente vamos mostrar a existência desta fatoração por indução noetheriana. Suponha que o conjunto S dos ideais não nulos que não admitem tal fatoração seja não vazio e seja \mathfrak{a} um elemento maximal de S . Então \mathfrak{a} não pode ser um ideal maximal em \mathcal{O}_K , assim existe um ideal maximal $\mathfrak{p} \supset \mathfrak{a}$ (utilize novamente indução

noetheriana, desta vez no conjunto dos ideais próprios de \mathcal{O}_K que contém \mathfrak{a}). Temos que $\mathfrak{p}^{-1}\mathfrak{p} \supset \mathfrak{p}^{-1}\mathfrak{a}$, logo $\mathfrak{p}^{-1}\mathfrak{a}$ é um ideal ordinário de \mathcal{O}_K . Além disso, como $\mathfrak{p}^{-1} \supset \mathcal{O}_K$, $\mathfrak{p}^{-1}\mathfrak{a} \supset \mathfrak{a}$ e esta inclusão é própria, pois caso contrário o lema afirma que $\mathfrak{p}^{-1} = \mathcal{O}_K$, o que não ocorre pela prova da proposição anterior. Pela escolha de \mathfrak{a} , temos portanto que $\mathfrak{p}^{-1}\mathfrak{a} \notin S$, isto é, existem ideais primos \mathfrak{p}_i tais que

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r \implies \mathfrak{a} = \mathfrak{p}\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_r$$

o que contradiz a definição de \mathfrak{a} . Logo $S = \emptyset$.

Agora provaremos a unicidade. Suponha que tenhamos duas fatorações

$$\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$$

com \mathfrak{p}_i e \mathfrak{q}_i ideais primos não nulos. Como \mathfrak{p}_1 contém o lado esquerdo, temos que ele contém o produto da direita e portanto contém algum dos fatores, digamos $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Porém, como ambos os ideais são maximais, devemos ter $\mathfrak{p}_1 = \mathfrak{q}_1$. Assim, multiplicando a igualdade acima por \mathfrak{p}_1^{-1} , obtemos

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

Por indução no número de fatores, podemos portanto concluir que $r = s$ e (após reordenamento dos fatores) que $\mathfrak{p}_i = \mathfrak{q}_i$ para $i = 2, \dots, r = s$. Isto conclui a prova. \square

O seguinte corolário conecta os dois sentidos de divisibilidade para ideais:

Corolário 6.67. *Dados ideais ordinários \mathfrak{a} e \mathfrak{b} de \mathcal{O}_K , temos que*

$$\mathfrak{a} \supset \mathfrak{b} \iff \text{existe um ideal ordinário } \mathfrak{c} \text{ de } \mathcal{O}_K \text{ tal que } \mathfrak{b} = \mathfrak{a}\mathfrak{c}.$$

DEMONSTRAÇÃO: A implicação \Leftarrow é clara. Para a outra implicação, faremos uma indução no número n de fatores primos de \mathfrak{a} . Se $n = 0$, então $\mathfrak{a} = (1)$ e podemos tomar $\mathfrak{c} = \mathfrak{b}$. Agora suponha $n > 0$ e seja \mathfrak{p} um fator primo de \mathfrak{a} . Então $\mathfrak{a} \supset \mathfrak{b} \implies \mathcal{O}_K \supset \mathfrak{p}^{-1}\mathfrak{a} \supset \mathfrak{p}^{-1}\mathfrak{b}$. Como $\mathfrak{p}^{-1}\mathfrak{a}$ tem $n - 1$ fatores primos, temos que existe um ideal \mathfrak{c} tal que $\mathfrak{p}^{-1}\mathfrak{b} = \mathfrak{p}^{-1}\mathfrak{a}\mathfrak{c} \implies \mathfrak{b} = \mathfrak{a}\mathfrak{c}$. \square

Obtemos ainda o seguinte corolário para ideais fracionários:

Corolário 6.68. *Qualquer ideal fracionário $\mathfrak{f} \neq 0$ de \mathcal{O}_K se escreve, de maneira única, como*

$$\mathfrak{f} = \prod_{1 \leq i \leq n} \mathfrak{p}_i^{e_i} \quad e_i \in \mathbb{Z}$$

onde $\mathfrak{p}_i \subset \mathcal{O}_K$ são ideais primos distintos.

Vamos encerrar esta seção com uma discussão sobre normas de ideais. Lembre-se de que o anel quociente $\mathcal{O}_K/\mathfrak{a}$ é sempre finito para um ideal $\mathfrak{a} \neq 0$ (lema 6.60).

Definição 6.69. *Seja \mathfrak{a} um ideal não nulo de \mathcal{O}_K . A norma $N(\mathfrak{a})$ de \mathfrak{a} é definida como o número de elementos do anel quociente $\mathcal{O}_K/\mathfrak{a}$.*

Proposição 6.70. *Sejam \mathfrak{a} e \mathfrak{b} ideais ordinários de \mathcal{O}_K . Então*

1. $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$;
2. $N((\alpha)) = |N(\alpha)|$ para todo $\alpha \in \mathcal{O}_K$.
3. $N(\mathfrak{a}) \in \mathfrak{a}$

DEMONSTRAÇÃO: Pela fatoração única, para mostrar (1) é suficiente mostrar que $N(\mathfrak{a})N(\mathfrak{p}) = N(\mathfrak{a}\mathfrak{p})$ para um ideal primo \mathfrak{p} e um ideal \mathfrak{a} qualquer. E como $|\mathcal{O}_K/\mathfrak{a}\mathfrak{p}| = |\mathcal{O}_K/\mathfrak{a}| \cdot |\mathfrak{a}/\mathfrak{a}\mathfrak{p}|$ basta mostrar o isomorfismo de grupos abelianos $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{p}$. Pela fatoração única, temos $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}$ e assim existe um elemento $\omega \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}$. Em outras palavras, ω é um elemento de \mathfrak{a} tal que (ω) é divisível pela mesma potência de \mathfrak{p} que divide \mathfrak{a} . Note que isto implica (pense no mdc de (ω) e $\mathfrak{a}\mathfrak{p}$)

$$\mathfrak{a} = (\omega) + \mathfrak{a}\mathfrak{p}.$$

De fato, a inclusão \supset é clara, de modo que $\mathfrak{a} \mid (\omega) + \mathfrak{a}\mathfrak{p}$. Por outro lado, $(\omega) + \mathfrak{a}\mathfrak{p} \supset \mathfrak{a}\mathfrak{p} \iff (\omega) + \mathfrak{a}\mathfrak{p} \mid \mathfrak{a}\mathfrak{p}$. Das duas relações de divisibilidade, concluímos que $(\omega) + \mathfrak{a}\mathfrak{p} = \mathfrak{a}$ ou $(\omega) + \mathfrak{a}\mathfrak{p} = \mathfrak{a}\mathfrak{p}$, mas a última possibilidade não ocorre pela escolha de ω .

Agora considere o mapa $\phi: \mathcal{O}_K/\mathfrak{p} \rightarrow \mathfrak{a}/\mathfrak{a}\mathfrak{p}$ dado por $a \bmod \mathfrak{p} \mapsto a\omega \bmod \mathfrak{a}\mathfrak{p}$, $a \in \mathcal{O}_K$, que está bem definido pois se $a \in \mathfrak{p}$ então $a\omega \in \mathfrak{a}\mathfrak{p}$.

Pelo provado acima, ϕ é sobrejetor, assim para mostrar que ϕ é um isomorfismo basta mostrar que ele é injetor. Mas se $\phi(a + \mathfrak{p})$ é zero, isto é, $a\omega \in \mathfrak{a}\mathfrak{p}$, então como (ω) é divisível pela mesma potência de \mathfrak{p} que divide \mathfrak{a} , devemos ter $\mathfrak{p} \mid (a) \iff a \in \mathfrak{p}$. Isto completa a prova de (1).

Para provar (2), seja $\omega_1, \dots, \omega_n$ uma base integral de \mathcal{O}_K . Temos então que $\alpha\omega_1, \dots, \alpha\omega_n$ é uma base integral do ideal principal (α) , e escrevendo $\alpha\omega_i$ em função dos ω_j , temos $\alpha\omega_i = \sum_{1 \leq j \leq n} a_{ij}\omega_j$ com $a_{ij} \in \mathbb{Z}$. Mas a matriz (a_{ij}) é a matriz da transformação linear T_α com relação à base ω_i , na notação da proposição 6.38. Assim, por esta última proposição e pelo lema 6.60, temos

$$N((\alpha)) = |\mathcal{O}_K/(\alpha)| = |\det(a_{ij})| = |\det T_\alpha| = |N(\alpha)|.$$

Finalmente, para (3) basta notar que como $N(\mathfrak{a})$ é a quantidade de elementos em $\mathcal{O}_K/\mathfrak{a}$, temos que $N(\mathfrak{a}) \cdot x \equiv 0 \pmod{\mathfrak{a}}$ para qualquer $x \in \mathcal{O}_K$ pelo teorema de Lagrange, em particular para $x = 1$ obtemos $N(\mathfrak{a}) \in \mathfrak{a}$. \square

6.6 Grupo de Classe e Unidades

Começamos com uma

Definição 6.71. *Seja K uma extensão finita de \mathbb{Q} de grau $n = [K : \mathbb{Q}]$. Uma imersão $\sigma: K \hookrightarrow \mathbb{C}$ é dita real se a imagem de K está contida em \mathbb{R} , caso contrário σ é dita complexa. Imersões complexas sempre vêm aos pares $\sigma, \bar{\sigma}$, pois podemos compor σ com a conjugação complexa para obter uma nova imersão complexa.*

De agora em diante, utilizaremos r para denotar o número de imersões reais de K e $2s$ para o número de imersões complexas, de modo que $r + 2s = n = [K : \mathbb{Q}]$. Convencionaremos a seguinte enumeração destas imersões

$$\underbrace{\sigma_1, \sigma_2, \dots, \sigma_r}_{\text{imersões reais}}, \quad \underbrace{\sigma_{r+1}, \bar{\sigma}_{r+1}, \sigma_{r+2}, \bar{\sigma}_{r+2}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+s}}_{\text{pares de imersões complexas conjugadas}}.$$

Por exemplo, para $K = \mathbb{Q}(\sqrt[3]{2})$, temos três imersões em \mathbb{C} , sendo $r = 1$ real e $2s = 2$ complexas, dadas por $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_2(\sqrt[3]{2}) = \omega\sqrt[3]{2}$

e $\bar{\sigma}_2(\sqrt[3]{2}) = \bar{\omega}\sqrt[3]{2}$, onde $\omega = \frac{-1+i\sqrt{3}}{2}$ é uma raiz cúbica primitiva da unidade.

Vamos agora definir um mapa

$$\psi: K \rightarrow \mathbb{R}^n$$

$$a \mapsto (\sigma_1(a), \dots, \sigma_r(a), \Re\sigma_{r+1}(a), \Im\sigma_{r+1}(a), \dots, \Re\sigma_{r+s}(a), \Im\sigma_{r+s}(a))$$

onde $\Re z$ e $\Im z$ denotam a parte real e imaginária do número complexo z . Observe que ψ é injetor e é um morfismo de grupos abelianos, isto é, $\psi(a+b) = \psi(a) + \psi(b)$ para quaisquer $a, b \in K$. Afirmamos que a imagem de \mathcal{O}_K por ψ é um reticulado em \mathbb{R}^n . De fato, seja $\omega_1, \dots, \omega_n$ uma base integral de \mathcal{O}_K , vamos mostrar que os vetores coluna $\psi(\omega_i)$ são linearmente independentes sobre \mathbb{R} , ou seja, que $\det(\psi(\omega_1), \dots, \psi(\omega_n)) \neq 0$. Recombinamos $\Re\sigma_{r+j}$ com $\Im\sigma_{r+j}$ para reobter σ_{r+j} : multiplicando a $(r+j+1)$ -ésima linha por i e somando com a $(r+j)$ -ésima linha e, em seguida, multiplicando a $(r+j)$ -ésima linha por $-\frac{1}{2}$ e somando com a $(r+j+1)$ -ésima linha, para $j = 1, 3, \dots, 2s-1$, obtemos, na notação da prova do lema 6.50,

$$\det(\psi(\omega_1), \dots, \psi(\omega_n)) = \left(-\frac{1}{2}\right)^s \cdot \det \delta(\omega_1, \dots, \omega_n) \neq 0.$$

De quebra, obtemos que

$$\text{vol}(\psi(\mathcal{O}_K)) = 2^{-s} \sqrt{|\Delta(\omega_1, \dots, \omega_n)|}$$

é o volume deste reticulado. Como aplicação, vamos mostrar o seguinte

Lema 6.72. *Seja \mathfrak{a} um ideal de \mathcal{O}_K . Então existe um elemento $a \in \mathfrak{a}$, $a \neq 0$, tal que*

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s N_{K/\mathbb{Q}}(\mathfrak{a}) \sqrt{|\Delta(\omega_1, \dots, \omega_n)|}.$$

DEMONSTRAÇÃO: Observe que $\psi(\mathfrak{a})$ também é um reticulado, cujo volume é $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ vezes maior do que o do reticulado $\psi(\mathcal{O}_K)$. Queremos aplicar o teorema de Minkowski 4.18 com o reticulado $\psi(\mathfrak{a})$ e o conjunto convexo e simétrico $V \subset \mathbb{R}^n$ definido pelas desigualdades

$$|x_1| \leq c, \dots, |x_r| \leq c, \quad x_{r+1}^2 + x_{r+2}^2 \leq c^2, \dots, x_{r+2s-1}^2 + x_{r+2s}^2 \leq c^2$$

onde $c^n = (2/\pi)^s N_{K/\mathbb{Q}}(\mathfrak{a}) \sqrt{|\Delta(\omega_1, \dots, \omega_n)|}$. O volume de V é

$$\begin{aligned} & \int_{|x_1| \leq c} \dots \int_{|x_r| \leq c} \int_{x_{r+1}^2 + x_{r+2}^2 \leq c^2} \int_{x_{r+1}^2 + x_{r+2}^2 \leq c^2} dx_1 \dots dx_n \\ &= \left(\int_{-c}^c dx \right)^r \left(\int_{x^2 + y^2 \leq c^2} dx dy \right)^s \\ &= (2c)^r (\pi c^2)^s = 2^r \pi^s c^n \end{aligned}$$

Como $2^r \pi^s c^n \geq 2^n \cdot N_{K/\mathbb{Q}}(\mathfrak{a}) 2^{-s} \sqrt{|\Delta(\omega_1, \dots, \omega_n)|} = 2^n \text{vol}(\psi(\mathfrak{a}))$ pela escolha de c , pelo teorema de Minkowski existe $a \in \mathfrak{a}$ tal que $a \neq 0$ e $\psi(a) \in V$, isto é, $|\sigma_i(a)| \leq c$ para $i = 1, \dots, r$ e $\sigma_{r+j}(a) \cdot \bar{\sigma}_{r+j}(a) = |\sigma_{r+j}(a)|^2 \leq c^2$ para $j = 1, \dots, s$. Logo

$$|N_{K/\mathbb{Q}}(a)| = |\sigma_1(a) \cdots \sigma_r(a) \cdot \sigma_{r+1}(a) \bar{\sigma}_{r+1}(a) \cdots \sigma_{r+s}(a) \bar{\sigma}_{r+s}(a)| \leq c^n$$

o que termina a prova. \square

Definição 6.73. O grupo de classe de \mathcal{O}_K é o grupo cujos elementos são classes de equivalência $[\mathfrak{a}]$ de ideais fracionários $\mathfrak{a} \neq (0)$ de \mathcal{O}_K , sendo dois ideais \mathfrak{a} e \mathfrak{b} equivalentes se eles diferem entre si por um ideal principal:

$$[\mathfrak{a}] = [\mathfrak{b}] \iff \mathfrak{a} = \mathfrak{b} \cdot (c) \quad \text{para algum } c \in K^\times.$$

É fácil checar que a relação acima é uma relação de equivalência no grupo multiplicativo dos ideais fracionários, compatível com o produto deste último grupo, de modo que podemos definir

$$[\mathfrak{a}] \cdot [\mathfrak{b}] \stackrel{\text{def}}{=} [\mathfrak{a} \cdot \mathfrak{b}].$$

Esta operação nas classes de ideais torna este conjunto um grupo; a identidade é a classe $[(1)]$ (ou de qualquer ideal principal) e $[\mathfrak{a}]^{-1} = [\mathfrak{a}^{-1}]$.

O grupo de classe é uma medida da “falha da fatoração única” em elementos irredutíveis. Por exemplo, para \mathbb{Z} e $\mathbb{Z}[i]$, o grupo de classe é trivial, pois todos os ideais são principais. Um resultado importante é que para o anel de inteiros \mathcal{O}_K esta “falha” é limitada:

Teorema 6.74 (Finitude do Grupo de Classe). *O grupo de classe do anel de inteiros \mathcal{O}_K é finito.*

DEMONSTRAÇÃO: Há uma quantidade finita de ideais com norma menor ou igual a $C = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\omega_1, \dots, \omega_n)|}$, pois há apenas um número finito de inteiros m entre 1 e C e se um ideal tem norma m , pela proposição 6.70 ele divide o ideal principal (m) , que possui um número finito de divisores.

Seja S este conjunto de ideais com norma menor ou igual a C . Basta mostrar que qualquer ideal \mathfrak{a} de \mathcal{O}_K é equivalente ao inverso de um ideal em S . Porém pelo lema anterior existe $a \neq 0$ em \mathfrak{a} tal que $|N(a)| \leq C \cdot N(\mathfrak{a})$. Como $a \in \mathfrak{a} \iff \mathfrak{a} \mid (a)$, existe um ideal \mathfrak{b} de \mathcal{O}_K tal que $\mathfrak{a}\mathfrak{b} = (a)$, isto é, $[\mathfrak{a}] = [\mathfrak{b}^{-1}]$. Por outro lado, $N(\mathfrak{a})N(\mathfrak{b}) = |N(a)| \implies N(\mathfrak{b}) \leq C$, ou seja, $\mathfrak{b} \in S$, como queríamos mostrar. \square

Exemplo 6.75. *Mostre que o grupo de classe do anel $\mathbb{Z}[i\sqrt{5}]$ possui dois elementos.*

DEMONSTRAÇÃO: O discriminante da base integral 1 e $i\sqrt{5}$ é

$$\Delta(1, i\sqrt{5}) = \begin{vmatrix} \text{Tr}(1) & \text{Tr}(i\sqrt{5}) \\ \text{Tr}(i\sqrt{5}) & \text{Tr}(-5) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & -10 \end{vmatrix} = -20.$$

Como há apenas $s = 1$ par de imersões complexas, pela demonstração acima, basta olhar para os ideais com norma menor ou igual a $C = \frac{2}{\pi}\sqrt{20} < 2.85$, ou seja, com norma menor ou igual a 2. Temos que $(2) = (2, 1+i\sqrt{5})^2$, logo $[(2, 1+i\sqrt{5})]^2 = [(1)]$ e $[(2, 1+i\sqrt{5})]$ é possivelmente o único elemento não trivial do grupo de classe de $\mathbb{Z}[i\sqrt{5}]$. Para terminar, devemos mostrar que $(2, 1+i\sqrt{5})$ não é principal. Mas se $(2, 1+i\sqrt{5}) = (d)$, teríamos que $d \mid 2 \implies N(d) \mid N(2) = 4$ e $d \mid 1+i\sqrt{5} \implies N(d) \mid N(1+i\sqrt{5}) = 6$, ou seja, $N(d) = 2$. Porém, $N(a+bi\sqrt{5}) = a^2 + 5b^2 = 2$ não possui solução com $a, b \in \mathbb{Z}$. Assim, o grupo de classe de $\mathbb{Z}[i\sqrt{5}]$ é constituído das classes $[(1)]$ e $[(2, 1+i\sqrt{5})]$. \square

Vejamos como aplicar os conceitos acima na resolução de equações diofantinas:

Exemplo 6.76. *Resolva a equação diofantina $y^3 = x^2 + 5$.*

DEMONSTRAÇÃO: Trabalhamos em $\mathbb{Z}[i\sqrt{5}]$, pois neste anel temos a fatoração $y^3 = (x + i\sqrt{5})(x - i\sqrt{5})$. Já vimos que o grupo de classe deste anel possui apenas dois elementos. Além disso, temos que $\mathbb{Z}[i\sqrt{5}]^\times = \pm 1$, pois se $a + bi\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]^\times$, $a, b \in \mathbb{Z}$, temos que $N(a + bi\sqrt{5}) = a^2 + 5b^2 = 1$, logo $a = \pm 1$ e $b = 0$. Observe ainda que x deve ser par e y , ímpar, pois caso contrário teríamos y par, logo $y^3 \equiv 0 \pmod{8}$, e x ímpar, logo $x^2 \equiv 1 \pmod{8} \implies x^2 + 5 \equiv 6 \pmod{8}$, um absurdo. Da mesma forma, é fácil mostrar que y não é um múltiplo de 5 também.

Sejam $\mathfrak{a} = (x + i\sqrt{5})$ e $\mathfrak{b} = (x - i\sqrt{5})$ os ideais principais gerados por $x \pm i\sqrt{5}$. Reescrevendo a fatoração acima em termos de ideais, temos

$$(y)^3 = \mathfrak{a}\mathfrak{b}. \quad (*)$$

Se \mathfrak{p} é um ideal primo que divide \mathfrak{a} e \mathfrak{b} , então \mathfrak{p} divide $x + i\sqrt{5} - (x - i\sqrt{5}) = 2i\sqrt{5}$ e temos a fatoração em ideais primos $(2i\sqrt{5}) = (2, 1 + i\sqrt{5})^2(i\sqrt{5})$. Logo $\mathfrak{p} = (2, 1 + i\sqrt{5})$ ou $\mathfrak{p} = (i\sqrt{5})$. Mas o primeiro caso não pode ocorrer, pois caso contrário de $(*)$ temos $\mathfrak{p} \mid (y) \implies 2 = N(\mathfrak{p}) \mid N(y) = y^2$ e y é ímpar; analogamente o segundo caso não ocorre pois $5 \nmid y$.

Assim, \mathfrak{a} e \mathfrak{b} são primos entre si, de $(*)$ temos pela fatoração única em ideais primos que $\mathfrak{a} = \mathfrak{c}^3$ e $\mathfrak{b} = \mathfrak{d}^3$ para ideais $\mathfrak{c}, \mathfrak{d}$ de $\mathbb{Z}[i\sqrt{5}]$. Como o grupo de classe só possui dois elementos, o quadrado de qualquer classe é trivial, e como \mathfrak{a} é principal, temos que $\mathfrak{a} = \mathfrak{c}^3 \implies [(1)] = [\mathfrak{c}]$, isto é, \mathfrak{c} é principal. Analogamente \mathfrak{d} é principal também. Resumindo, existem $a, b \in \mathbb{Z}$ tais que temos a igualdade de ideais

$$\mathfrak{a} = (a + bi\sqrt{5})^3 \iff (x + i\sqrt{5}) = (a + bi\sqrt{5})^3.$$

Como dois elementos geram o mesmo ideal principal se, e somente se, eles diferem de uma unidade, temos que $x + i\sqrt{5} = \pm((a^3 - 15ab^2) + (3a^2b - 5b^3)i\sqrt{5})$. Daqui temos $3a^2b - 5b^3 = \pm 1 \implies b = \pm 1$. Testando os valores, vemos que não há solução inteira para a . Logo a equação $y^3 = x^2 + 5$ não possui soluções inteiras. \square

Exemplo 6.77. *Mostre que os anéis de inteiros \mathcal{O}_K de $K = \mathbb{Q}(\sqrt{-n})$ para $n = 19, 43, 67, 163$ são domínio de ideais principais.*

SOLUÇÃO: Devemos mostrar que o grupo de classe é trivial para estes anéis. Temos, pelo exercício 6.27, que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ onde $\omega = \frac{1+\sqrt{-n}}{2}$, de modo que o discriminante é dado por $\Delta(1, \omega) = -n$. Assim, como há apenas $s = 1$ par de imersões complexas, pela demonstração do teorema de finitude do grupo de classe, basta mostrar que os ideais primos \mathfrak{p} com norma menor que $C = \frac{2}{\pi}\sqrt{n}$ são principais. Note que $\mathfrak{p} \mid N(\mathfrak{p})$ (proposição 6.70) e como $\mathcal{O}_K/\mathfrak{p}$ é um corpo finito, então $N(\mathfrak{p})$ é potência de algum número primo, assim \mathfrak{p} deve dividir (p) para algum número primo $p < C$. Assim, basta mostrar que os ideais (p) são maximais, o que pode ser feito exatamente como na proposição 6.21 utilizando o fato que $\left(\frac{p}{n}\right) = -1$. \square

Os anéis acima são exemplos de domínios de ideais principais que não são euclidianos. Para mostrar isto, seja D um domínio e denotemos por \tilde{D} o conjunto das unidades de D juntamente com o elemento zero. Um elemento $u \in D \setminus \tilde{D}$ é chamado um *divisor universal* se para todo $x \in D$ existe $z \in \tilde{D}$ tal que $u \mid x - z$. Por exemplo, 2 e 3 são divisores universais em \mathbb{Z} .

Lema 6.78. *Seja D um domínio que não é um corpo e tal que D não possui divisores universais. Então D não é um domínio euclidiano.*

DEMONSTRAÇÃO: Suponhamos por contradição que D é euclidiano com função euclidiana d (isto é, $d: D \setminus \{0\} \rightarrow \mathbb{N}$ e para todo $a, b \in D$, $b \neq 0$, existem q e r com $a = bq + r$ e $r = 0$ ou $d(r) < d(b)$). Definamos

$$S = \{d(v) \mid v \in D \setminus \tilde{D}\} \subset \mathbb{N}.$$

Como D não é um corpo, $D \neq \tilde{D}$ e S é não vazio, logo possui mínimo. Seja $u \in D \setminus \tilde{D}$ tal que $d(u)$ é mínimo em S . Para cada $x \in D$ existem $q, r \in D$ tais que $x = uq + r$ onde $r = 0$ ou $d(r) < d(u)$. Pela minimalidade de $d(u)$ sabemos que $r \in \tilde{D}$ e como $u \mid x - r$, u é um divisor universal, o que é absurdo. \square

O seguinte teorema completa a prova da afirmação de que os anéis do exemplo anterior são principais mas não euclidianos.

Teorema 6.79. *Os anéis de inteiros de $\mathbb{Q}(\sqrt{-n})$ onde $n \equiv -5 \pmod{24}$ não são euclidianos.*

DEMONSTRAÇÃO: Como $-n \equiv 1 \pmod{4}$, temos que o anel de inteiros de $K = \mathbb{Q}(\sqrt{-n})$ é $D_n = \mathbb{Z} + \mathbb{Z}\omega$ onde $\omega = \frac{1+\sqrt{-n}}{2}$. Suponhamos que D_n possui um divisor universal u . Como $\tilde{D}_n = \{-1, 0, 1\}$, segue que u que divide um dos números $2-1$, $2+0$ ou $2+1$, isto é, u divide 2 ou 3. Mas 2 e 3 são irredutíveis em D_n (verifique!), logo $u = \pm 2$ ou $u = \pm 3$. Porém, nenhum destes números divide quaisquer dos números

$$\omega + 1 = \frac{3 + \sqrt{-n}}{2}, \quad \omega = \frac{1 + \sqrt{-n}}{2}, \quad \omega - 1 = \frac{-1 + \sqrt{-n}}{2}$$

já que nem 2 nem 3 dividem as normas

$$\left| \frac{3 + \sqrt{-n}}{2} \right|^2 = \frac{9 + n}{4} \equiv 1 \pmod{6}$$

e

$$\left| \frac{\pm 1 + \sqrt{-n}}{2} \right|^2 = \frac{1 + n}{4} \equiv -1 \pmod{6},$$

logo tal divisor universal não pode existir, assim pelo lema D_n não é euclidiano. \square

Queremos utilizar os métodos geométricos acima para estudar o grupo de unidades de \mathcal{O}_K . Vamos agora definir uma versão “multiplicativa” do mapa ψ anterior. Seja

$$\begin{aligned} \mu: \mathcal{O}_K^\times &\rightarrow \mathbb{R}^{r+s} \\ a &\mapsto (\log |\sigma_1(a)|, \dots, \log |\sigma_r(a)|, 2 \log |\sigma_{r+1}(a)|, \dots, 2 \log |\sigma_{r+s}(a)|) \end{aligned}$$

Temos que μ é um morfismo de grupos: $\mu(ab) = \mu(a) + \mu(b)$ para todo $a, b \in \mathcal{O}_K^\times$. Além disso, a imagem de μ está contida no hiperplano $x_1 + x_2 + \dots + x_{r+s} = 0$ pois $N_{K/\mathbb{Q}}(a) = \pm 1$ (a é unidade) e assim

$$\begin{aligned} &\log |\sigma_1(a)| + \dots + \log |\sigma_r(a)| + 2 \log |\sigma_{r+1}(a)| + \dots + 2 \log |\sigma_{r+s}(a)| \\ &= \log |\sigma_1(a) \cdots \sigma_r(a) \sigma_{r+1}(a) \bar{\sigma}_{r+1}(a) \cdots \sigma_{r+s}(a) \bar{\sigma}_{r+s}(a)| \\ &= \log |N_{K/\mathbb{Q}}(a)| = \log 1 = 0 \end{aligned}$$

O mapa μ não é injetivo como ψ , porém o seu kernel é finito:

Proposição 6.80 (Kronecker). *Seja $a \in \mathcal{O}_K^\times$ tal que $\mu(a) = 0$, isto é, $|\sigma(a)| = 1$ para toda imersão $\sigma: K \hookrightarrow \mathbb{C}$. Então a é uma raiz da unidade.*

DEMONSTRAÇÃO: Para $m \geq 1$, a^m satisfaz o polinômio

$$\prod_{\sigma} (x - \sigma(a)^m) = x^n + c_1 x^{n-1} + \cdots + c_n$$

onde σ percorre todas as imersões de K em \mathbb{C} . Note que como os coeficientes c_i deste polinômio são funções simétricas elementares em $\sigma(a^m)$, que são todos inteiros algébricos de módulo 1, temos que os coeficientes c_i são todos inteiros (c.f. demonstração da proposição 6.38) e satisfazem a desigualdade $|c_i| \leq \binom{n}{i}$. Portanto só há um número finito de tais polinômios! Assim, pelo princípio da casa dos pombos, existem $m_1 > m_2$ tais que $a^{m_1} = a^{m_2} \iff a^{m_1-m_2} = 1$, isto é, a é uma raiz da unidade. \square

Note que só há um número finito de raízes da unidade em uma extensão finita K de \mathbb{Q} pois como $\psi(\mathcal{O}_K)$ é um reticulado, há apenas um número finito de elementos $a \in \mathcal{O}_K$ com $|\sigma_i(a)| = 1$ para todo i . Note ainda que o grupo de todas as raízes da unidade contidas em K é *cíclico*, isto é, existe uma raiz da unidade ζ_t em K tal que todas as demais se escrevem como potências ζ_t^i desta; a demonstração deste fato é idêntica à demonstração da existência de raízes primitivas para um primo p , e é deixada como exercício para o leitor.

Vamos agora mostrar que $\mu(\mathcal{O}_K^\times)$ é um reticulado no hiperplano

$$H \stackrel{\text{def}}{=} \{(x_1, \dots, x_{r+s}) \in \mathbb{R}^{r+s} \mid x_1 + \cdots + x_{r+s} = 0\}.$$

Como já sabemos que $\mu(\mathcal{O}_K^\times)$ é um subgrupo de H , é suficiente mostrar que a imagem de μ é discreta e que existe um conjunto limitado $B \subset H$ tal que os translados $\mu(u) + B$, $u \in \mathcal{O}_K^\times$, cobrem todo o H .

O fato de que $\mu(\mathcal{O}_K^\times)$ é discreto é simples: se $\|\mu(u)\| < R$, então $|\sigma_i(u)|$ é limitado para todo i . Como $\psi(\mathcal{O}_K)$ é um reticulado, temos que há apenas um número finito de tais u 's, logo a intersecção da imagem de μ com cada bola aberta é finita e portanto $\mu(\mathcal{O}_K^\times)$ é um conjunto discreto.

Para mostrar a existência de B , utilizaremos a seguinte notação: para $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{R}^n$, denotaremos pelo mesmo símbolo a transformação linear dada por

$$\begin{aligned} \mathbf{a}: \mathbb{R}^n \rightarrow \mathbb{R}^n \\ (x_1, \dots, x_n) \mapsto (a_1 x_1, \dots, a_r x_r, a_{r+1} x_{r+1} - a_{r+2} x_{r+2}, a_{r+2} x_{r+1} + \\ + a_{r+1} x_{r+2}, \dots, a_{r+2s-1} x_{r+2s-1} - a_{r+2s} x_{r+2s}, \\ a_{r+2s} x_{r+2s-1} + a_{r+2s-1} x_{r+2s}) \end{aligned}$$

de modo que $\psi(ab) = \psi(a)\psi(b) = \psi(b)\psi(a)$ (vistos como transformações lineares) para todo $a, b \in K$. Note que quando $\mathbf{a} = \psi(a)$, o determinante desta transformação linear é exatamente $N(a)$, de modo que se $a \in \mathcal{O}_K^\times$, esta transformação preserva volumes.

Vamos reescrever nosso problema em notação “multiplicativa”. Seja

$$H' = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid x_1 \dots x_r (x_{r+1}^2 + x_{r+2}^2) \dots (x_{r+2s-1}^2 + x_{r+2s}^2) = \pm 1\}$$

a “hiperfície dos elementos de norma ± 1 ”. Note que $\psi(u) \in H'$ e $\psi(u)H' \subset H'$ para todo $u \in \mathcal{O}_K^\times$. Para mostrar a existência do conjunto B é suficiente mostrar a existência de um conjunto limitado $B' \subset H'$ tal que

$$H' = \bigcup_{u \in \mathcal{O}_K^\times} \psi(u)B'.$$

Precisamos de um

Lema 6.81. *Dado $C > 0$, existem elementos $\alpha_1, \dots, \alpha_h$ em \mathcal{O}_K tais que se $N_{K/\mathbb{Q}}(\alpha) \leq C$ então α é associado a algum α_i , isto é, existe $u \in \mathcal{O}_K^\times$ para o qual $\alpha = u\alpha_i$.*

DEMONSTRAÇÃO: Há um número finito de ideais com norma menor ou igual a C , em particular há um número finito de ideais principais com norma igual a C , digamos $(\alpha_1), \dots, (\alpha_h)$. Assim, dado α com $N(\alpha) \leq C$, temos que $(\alpha) = (\alpha_i)$ para algum i e portanto $\alpha = u\alpha_i$ para alguma unidade u . \square

Já sabemos como produzir elementos de norma pequena pelo lema 6.72. Na notação da prova daquele lema, aplicado ao ideal $\mathfrak{a} = (1)$,

considere o conjunto $V \subset \mathbb{R}^n$ lá definido e seja $C = (\frac{2}{\pi})^s \sqrt{|\Delta(\omega_1, \dots, \omega_n)|}$. Sejam α_i como no lema anterior. Definimos

$$B' = H' \cap \bigcup_{1 \leq i \leq h} \psi(\alpha_i^{-1})V.$$

Vamos agora mostrar que os conjuntos $\psi(u)B'$, $u \in \mathcal{O}_K^\times$, cobrem H' . Tome $\mathbf{x} \in H'$. Considere o conjunto $\mathbf{x}^{-1}V$, que possui mesmo volume que V e ainda é convexo e simétrico. Assim, existe $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, tal que $\psi(\alpha) \in \mathbf{x}^{-1}V$. Isto implica que $N(\alpha) \leq C$ e portanto existem $u \in \mathcal{O}_K^\times$ e α_i tais que $\alpha = u\alpha_i$. Assim, $\psi(u\alpha_i) \in \mathbf{x}^{-1}V \iff \mathbf{x} \in \psi(u^{-1})\psi(\alpha_i^{-1})V \subset \psi(u^{-1})B'$.

Agora podemos dar a caracterização completa do grupo de unidades do anel de inteiros de uma extensão finita de \mathbb{Q} :

Teorema 6.82 (Dirichlet). *Seja K uma extensão finita de \mathbb{Q} , r o número de imersões reais de K e s igual à metade do número de imersões complexas de K . Então o grupo de unidades \mathcal{O}_K^\times é finitamente gerado de posto $r + s - 1$, isto é, existem unidades u_1, \dots, u_{r+s-1} e uma raiz da unidade $\zeta_t \in K$ tal que toda unidade de \mathcal{O}_K se escreve de maneira única como*

$$\zeta_t^a u_1^{e_1} \dots u_{r+s-1}^{e_{r+s-1}} \quad a \in \mathbb{Z}/t \text{ e } e_i \in \mathbb{Z}.$$

DEMONSTRAÇÃO: Temos que $\mu(\mathcal{O}_K^\times)$ é um reticulado de H , logo existem unidades u_1, \dots, u_{r+s-1} tais que

$$\mu(\mathcal{O}_K^\times) = \mathbb{Z} \cdot \mu(u_1) + \dots + \mathbb{Z} \cdot \mu(u_{r+s-1}).$$

Além disso, existe uma t -ésima raiz da unidade ζ_t que gera o kernel de μ . Assim, dada uma unidade $u \in \mathcal{O}_K^\times$, existem inteiros $e_i \in \mathbb{Z}$, unicamente determinados, tais que

$$\mu(u) = e_1 \mu(u_1) + \dots + e_{r+s-1} \mu(u_{r+s-1}) \iff \mu(u u_1^{-e_1} \dots u_{r+s-1}^{-e_{r+s-1}}) = 1$$

e agora existe um único $a \in \mathbb{Z}/t$ tal que $u u_1^{-e_1} \dots u_{r+s-1}^{-e_{r+s-1}} = \zeta_t^a$, e o resultado segue. \square

Por exemplo, como há duas imersões reais de $\mathbb{Q}(\sqrt{2})$ em \mathbb{C} , temos que o grupo de unidades de $\mathbb{Z}[\sqrt{2}]$ tem posto $r - 1 = 1$. E de fato, temos que $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$ pois as unidades correspondem às soluções da equação de Pell $N(x + y\sqrt{2}) = x^2 - 2y^2 = \pm 1$.

Problemas Propostos

6.27. *Seja d um inteiro livre de quadrados. Mostre que o anel de inteiros de $\mathbb{Q}(\sqrt{d})$ é $\mathbb{Z} + \mathbb{Z}\omega$, onde*

$$\omega = \begin{cases} \sqrt{d} & \text{se } d \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{se } d \equiv 1 \pmod{4} \end{cases}.$$

6.28. *Determine o anel de inteiros de $\mathbb{Q}(\sqrt[3]{2})$.*

6.29. *Fatore os seguintes ideais de $\mathbb{Z}[i\sqrt{5}]$ em produto de ideais primos: (2), (3), (5), (7), (11), (23), $(7 + 3i\sqrt{5})$.*

6.30. *Seja ζ_5 uma raiz quinta primitiva da unidade.*

(a) *Mostre que $1 + \zeta_5$, $1 + \zeta_5 + \zeta_5^2$ e $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3$ são unidades em $\mathbb{Z}[\zeta_5]$. Mostre que $(1 - \zeta_5)$ é um ideal maximal em $\mathbb{Z}[\zeta_5]$ e que $(5) = (1 - \zeta_5)^4$.*

(b) *Mostre que o anel de inteiros algébricos de $\mathbb{Q}(\zeta_5)$ é $\mathbb{Z}[\zeta_5] = \mathbb{Z} + \mathbb{Z}\zeta_5 + \mathbb{Z}\zeta_5^2 + \mathbb{Z}\zeta_5^3$.*

Dica: Utilize a base $(1 - \zeta_5)^i$ e analise módulo $(1 - \zeta_5)$.

(c) *Fatore em ideais primos de $\mathbb{Z}[\zeta_5]$: (2), (3) e $(7 + \zeta_5)$.*

(d) *Determine o grupo de classe de $\mathbb{Z}[\zeta_5]$.*

6.31 (Teorema Chinês dos Restos). *Seja A um anel comutativo qualquer e sejam $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideais dois a dois coprimos, isto é, $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ para $i \neq j$ (esta condição é por exemplo satisfeita se os \mathfrak{a}_i são todos maximais distintos). Mostre que*

(a) $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n$

(b) *Temos um isomorfismo*

$$\frac{A}{\mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n} = \frac{A}{\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n} \rightarrow \frac{A}{\mathfrak{a}_1} \times \dots \times \frac{A}{\mathfrak{a}_n}$$

dado pelo mapa natural $a \bmod \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n \mapsto (a \bmod \mathfrak{a}_1, \dots, a \bmod \mathfrak{a}_n)$.

6.32. Mostre que qualquer ideal \mathfrak{a} no anel de inteiros \mathcal{O}_K de uma extensão finita K de \mathbb{Q} pode ser gerado por 2 elementos.

6.33. Determine o grupo de unidades e o grupo de classe do anel de inteiros de $\mathbb{Q}(\sqrt[3]{14})$. Encontre todas as soluções da equação diofantina $x^2 - 14y^2 = 22$.

6.34. Determine todas as soluções inteiras (x, y, n) da equação $5x^2 + 1 = y^{2n+1}$ com $n \geq 1$.

6.35. Neste exercício, mostraremos que

$$\mathbb{Z}[\sqrt[3]{2}]^\times = \{\pm(\sqrt[3]{2} - 1)^n \mid n \in \mathbb{Z}\}$$

Para isto, seja $\omega = e^{2\pi i/3}$ (uma raiz cúbica primitiva da unidade) e sejam $\sigma_j: \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$ as três imersões de $\mathbb{Q}(\sqrt[3]{2})$ em \mathbb{C} dadas por $\sigma_j(\sqrt[3]{2}) = \omega^j \sqrt[3]{2}$ para $j = 0, 1, 2$.

(a) Verifique que $\sqrt[3]{2} - 1 \in \mathbb{Z}[\sqrt[3]{2}]^\times$.

(b) Seja $u \in \mathbb{Z}[\sqrt[3]{2}]^\times$. Mostre que existe $k \in \mathbb{Z}$ de modo que uma das seguintes unidades

$$\begin{array}{ll} u \cdot (\sqrt[3]{2} - 1)^k & u^{-1} \cdot (\sqrt[3]{2} - 1)^k \\ -u \cdot (\sqrt[3]{2} - 1)^k & -u^{-1} \cdot (\sqrt[3]{2} - 1)^k \end{array}$$

pertença ao intervalo aberto $(\frac{1}{2}, 1)$.

(c) Defina o “tamanho” $\|\alpha\| \in \mathbb{R}_{\geq 0}$ de um elemento $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ por

$$\|\alpha\|^2 \stackrel{\text{def}}{=} |\sigma_0(\alpha)|^2 + |\sigma_1(\alpha)|^2 + |\sigma_2(\alpha)|^2 = |\alpha|^2 + 2|\sigma_1(\alpha)|^2$$

Verifique que, para $a, b, c \in \mathbb{Q}$, temos

$$\|a + b\sqrt[3]{2} + c\sqrt[3]{4}\|^2 = 3 \cdot (a^2 + (b\sqrt[3]{2})^2 + (c\sqrt[3]{4})^2)$$

(d) Utilize o fato que, para todo $u \in \mathbb{Z}[\sqrt[3]{2}]^\times$,

$$1 = |N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(u)| = |u| \cdot |\sigma_1(u)|^2$$

para mostrar que se $\frac{1}{2} < u < 1$ então $\|u\|^2 < 5$. Conclua que $u = \pm 1$.

(e) Conclua que $\mathbb{Z}[\sqrt[3]{2}]^\times = \{\pm(\sqrt[3]{2} - 1)^n \mid n \in \mathbb{Z}\}$.

Capítulo 7

Primos

Desde tempos remotos, problemas concernentes a números primos têm fascinado os matemáticos. De fato, Karl Friedrich Gauß (1777–1855) chegou a afirmar em seu *Disquisitiones Arithmeticae* (1801): “O problema de distinguir números primos de compostos e de decompor esses últimos em seus fatores primos é conhecido como sendo um dos mais importantes e úteis na aritmética. . . . a dignidade da própria ciência parece requerer que todos os meios possíveis sejam explorados para a solução de um problema tão elegante e tão celebrado” (traduzido de Knuth [83]).

Este capítulo aborda primos sob diversos aspectos: o analítico, o algébrico e até mesmo o computacional. Veremos algumas conjecturas e problemas em aberto sobre primos que ainda hoje desafiam os matemáticos profissionais.

7.1 Sobre a Distribuição dos Números Primos

Nesta seção estudaremos alguns resultados sobre a distribuição dos números primos.

7.1.1 O Teorema dos Números Primos

Já vimos que existem infinitos primos; o teorema dos números primos dá uma estimativa de quantos primos existem até um inteiro x , ou seja, descreve a distribuição dos primos. Defina $\pi(x)$ como sendo o número de primos p com $2 \leq p \leq x$. Já sabemos pelo teorema de Chebyshev 5.15

que $\pi(x)$ está entre $cx/\log x$ e $Cx/\log x$ para duas constantes $c < C$. Na verdade, temos um resultado muito mais preciso:

Teorema 7.1 (Teorema dos Números Primos).

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Este resultado foi conjecturado por vários matemáticos, inclusive por Legendre e Gauß, mas a demonstração completa só foi encontrada em 1896, por de la Vallée Poussin e Hadamard (independentemente). Não demonstraremos este teorema aqui: as demonstrações elementares conhecidas são todas bastante difíceis (lembramos que uma demonstração é dita *elementar* quando não usa ferramentas avançadas: muitas demonstrações elementares são longas e sofisticadas). Uma demonstração deste teorema, que utiliza ferramentas de Análise Complexa, encontra-se no apêndice A deste livro, que reproduz, com pequenas modificações, a dissertação de mestrado de Jorge Aarão.

Uma aproximação mais precisa para $\pi(x)$ é dada por

$$\text{Li}(x) = \int_0^x \frac{dt}{\log t},$$

onde tomamos o valor principal desta integral, ou seja,

$$\text{Li}(x) = \lim_{\varepsilon \rightarrow 0} \int_{\varepsilon}^{1-\varepsilon} \frac{dt}{\log t} + \int_{1+\varepsilon}^x \frac{dt}{\log t};$$

claramente

$$\lim_{x \rightarrow \infty} \frac{\text{Li}(x)}{\log(x)/x} = 1.$$

Sabe-se entretanto que

$$|\pi(x) - \text{Li}(x)| \leq Cxe^{-a(\log x)^{3/5}(\log \log x)^{-1/5}}$$

para algum valor das constantes a e C (independente de x). Em particular, para qualquer $k > 0$ existe $C > 0$ tal que, para todo x ,

$$|\pi(x) - \text{Li}(x)| \leq C \frac{x}{(\log x)^k},$$

o que mostra que $\text{Li}(x)$ (e mesmo $x/(\log x - 1)$) é uma aproximação de $\pi(x)$ bem melhor do que $x/\log x$.

Em 1901 von Koch mostrou que a hipótese de Riemann, já mencionada, equivale a dizer que para todo $\varepsilon > 0$ existe C com

$$|\pi(x) - \text{Li}(x)| \leq Cx^{1/2+\varepsilon};$$

ninguém sabe demonstrar que esta estimativa seja correta sequer para algum valor de $\varepsilon < 1/2$. A hipótese de Riemann também implica que existe C com

$$|\pi(x) - \text{Li}(x)| \leq Cx^{1/2} \log x,$$

o que daria uma estimativa para o tamanho deste erro muito melhor do que as que se sabe demonstrar. Por outro lado, sabe-se demonstrar que não pode existir nenhuma estimativa muito melhor do que esta para $|\pi(x) - \text{Li}(x)|$: Littlewood provou em 1914 que, para todo $M > 0$, existem inteiros $x_1 > M$ e $x_2 > M$ com

$$\begin{aligned} \pi(x_1) - \text{Li}(x_1) &< -\frac{1}{3} \frac{\sqrt{x_1} \log \log x_1}{\log x_1}, \\ \pi(x_2) - \text{Li}(x_2) &> \frac{1}{3} \frac{\sqrt{x_2} \log \log x_2}{\log x_2}. \end{aligned}$$

7.1.2 Primos Gêmeos e Primos de Sophie Germain

Dizemos que p e q são *primos gêmeos* se p e q são primos e $|p - q| = 2$. Conjetura-se, mas não se sabe demonstrar, que existem infinitos pares de primos gêmeos. São conhecidos pares de primos gêmeos bastante grandes, como $65516468355 \cdot 2^{333333} \pm 1$, que têm 100355 dígitos cada. Brun, por outro lado, provou em [23] que primos gêmeos são escassos no seguinte sentido: se

$$\pi_2(x) = \#\{p \leq x \mid p \text{ e } p+2 \text{ são primos}\}$$

é o número de pares de primos gêmeos até x então

$$\pi_2(x) = O\left(\frac{x(\log \log x)^2}{(\log x)^2}\right).$$

Em particular, isto implica que

$$\sum_{p \text{ primo gêmeo}} \frac{1}{p} < +\infty,$$

enquanto sabemos que a soma sobre todos os primos $\sum_{p \text{ primo}} \frac{1}{p}$ diverge (teorema 5.24). Brun provou posteriormente em [24] que

$$\pi_2(x) < \frac{100x}{(\log x)^2}$$

para x suficientemente grande. Acredita-se, mas não se sabe demonstrar, que $\pi_2(x)$ seja assintótico a $Cx/(\log x)^2$ para alguma constante positiva C . Deixamos como exercício provar a seguinte caracterização de primos gêmeos devida a Clement. Seja $n \geq 2$; os inteiros n e $n+2$ são ambos primos se, e somente se,

$$4((n-1)! + 1) + n \equiv 0 \pmod{n(n+2)}.$$

Os primos p para os quais $2p+1$ é primo são chamados de *primos de Sophie Germain*. Este nome é usado porque Sophie Germain provou o chamado primeiro caso do Último teorema de Fermat (demonstrado completamente por Wiles e Taylor) para primos p desta forma.

Proposição 7.2 (Sophie Germain). *Se p e $2p+1$ são primos com $p > 2$, então não existem inteiros x, y, z com $\text{mdc}(x, y, z) = 1$ e $p \nmid xyz$ tais que $x^p + y^p + z^p = 0$.*

DEMONSTRAÇÃO: Observe inicialmente que $2p+1 \mid xyz$: caso contrário, pelo pequeno teorema de Fermat, $x^{2p} \equiv 1 \pmod{2p+1}$, o que equivale a $(x^p - 1)(x^p + 1) \equiv 0 \pmod{2p+1}$. Assim, temos que $x^p \equiv \pm 1 \pmod{2p+1}$ e analogamente $y^p \equiv \pm 1 \pmod{2p+1}$ e $z^p \equiv \pm 1 \pmod{2p+1}$. Mas $x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{2p+1}$, um absurdo.

Por outro lado, temos

$$(-x)^p = (y+z)(y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1})$$

Vamos mostrar que os dois fatores da direita são primos entre si. Se q é um primo que divide ambos os termos, então $y \equiv -z \pmod{q}$ e portanto $0 \equiv y^{p-1} - y^{p-2}z + \cdots + z^{p-1} \equiv py^{p-1} \pmod{q}$; temos $q \neq p$ pois $q \mid x$, assim $q \mid py^{p-1} \implies q \mid y$, mas então $z \equiv -y \equiv 0 \pmod{q}$ e q dividiria simultaneamente x, y, z , contrariando a hipótese $\text{mdc}(x, y, z) = 1$. Assim, pela fatoração única em primos existem inteiros a, d tais que

$$a^p = y + z \quad \text{e} \quad d^p = y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}$$

e analogamente

$$\begin{aligned} b^p &= x + z & \text{e} & & e^p &= x^{p-1} - x^{p-2}z + \cdots - xz^{p-2} + z^{p-1} \\ c^p &= x + y & \text{e} & & f^p &= x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1} \end{aligned}$$

para b, c, e, f inteiros.

Como $2p + 1 \mid xyz$, podemos supor sem perda de generalidade que $2p + 1 \mid x$. Assim, de $2x = b^p + c^p - a^p$, temos que $2p + 1 \mid b^p + c^p - a^p$ e o mesmo argumento no início da demonstração mostra que $2p + 1 \mid abc$ também. Mas se $2p + 1 \mid b = x + z$ ou $2p + 1 \mid c = x + y$, como $2p + 1 \mid x$ e $x^p + y^p + z^p = 0$ teríamos que $2p + 1 \mid \text{mdc}(x, y, z) = 1$, um absurdo. Por outro lado, temos $f^p \equiv y^{p-1} \pmod{2p+1}$ e se $2p + 1 \mid a$, então $2p + 1 \nmid d$ e $y \equiv -z \pmod{2p+1} \implies d^p \equiv py^{p-1} \pmod{2p+1}$. Assim, $2p + 1 \mid f$, pois caso contrário teríamos $\pm p \equiv pf^p \equiv py^{p-1} \equiv d^p \equiv \pm 1 \pmod{2p+1}$, um absurdo. Mas neste caso, $2p + 1 \mid z$ também, o que é impossível já que $\text{mdc}(x, y, z) = 1$, completando a prova. \square

Alguns primos de Sophie Germain bastante grandes são conhecidos, como $183027 \cdot 2^{265440} - 1$, que tem 79911 dígitos. Sabe-se também que se $\pi_{\text{SG}}(x)$ denota o número de primos de Sophie Germain menores do que x então existe C tal que para todo x

$$\pi_{\text{SG}}(x) < C \frac{x}{(\log x)^2}.$$

Acredita-se que $\pi_{\text{SG}}(x)$ seja assintótico a $cx/(\log x)^2$ para algum $c > 0$, mas não se sabe demonstrar sequer que existem infinitos primos de Sophie Germain.

Em geral, dados a, b, c números inteiros positivos, dois a dois primos entre si e com exatamente um de tais números par, denotamos por $\pi_{a,b,c}(x)$ a quantidade de pares de números primos (p, q) que satisfazem a condição $aq - bp = c$ com $p \leq x$. Hardy e Littlewood conjecturaram em [69] a seguinte estimativa assintótica para $\pi_{a,b,c}(x)$:

Conjetura 7.3 (Hardy, Littlewood).

$$\pi_{a,b,c}(x) \sim \frac{2C}{a} \frac{x}{(\log x)^2} \prod_{\substack{p \mid abc \\ p \text{ primo} > 2}} \left(\frac{p-1}{p-2} \right),$$

onde $C = \prod_{\substack{p \text{ primo} \\ p > 2}} \left(1 - \frac{1}{(p-1)^2} \right).$

Em particular, se $a = 1$, $b = 1$ e $c = 2$ temos que $\pi_{1,1,2} = \pi_2$, e se $a = 1$, $b = 2$ e $c = 1$ temos que $\pi_{1,2,1}(x)$ é o número de primos de Sophie Germain menores do que ou iguais a x .

Nesta seção, provaremos o corolário do teorema de Brun, segundo o qual a série dos inversos dos primos gêmeos converge. Pelo mesmo argumento se prova que a soma dos inversos dos primos de Sophie Germain converge, o que mostra que os primos gêmeos, assim como os primos de Sophie Germain, são bem mais raros que os primos.

Antes de enunciar a proposição fundamental desta seção, precisamos dos seguintes lemas.

Lema 7.4. *Sejam m e l números naturais com $l \geq 1$. Então*

$$\sum_{\substack{d|m \\ \omega(d) \leq 2l-1}} \mu(d) \leq \sum_{d|m} \mu(d) \leq \sum_{\substack{d|m \\ \omega(d) \leq 2l}} \mu(d),$$

onde $\omega(d)$ denota o número de fatores primos distintos de d .

DEMONSTRAÇÃO: Se $m = 1$, os três termos são iguais a 1. Se $m > 1$, o termo do meio é igual a 0 pelo lema 5.8. Agora seja $k = \omega(m)$. Como $\mu(d) \neq 0$ implica que d é produto de primos distintos, para todo s temos que

$$\sum_{\substack{d|m \\ \omega(d) \leq s}} \mu(d) = \sum_{j=0}^s \sum_{\substack{d|m \\ \omega(d)=j}} \mu(d) = \sum_{j=0}^s \binom{k}{j} (-1)^j$$

pois se d é produto de j primos distintos então $\mu(d) = (-1)^j$ e existem $\binom{k}{j}$ produtos de j primos distintos que dividem m . Por outro lado,

$$\sum_{j=0}^s \binom{k}{j} (-1)^j = 1 + \sum_{j=1}^s \left[\binom{k-1}{j} + \binom{k-1}{j-1} \right] (-1)^j = (-1)^s \binom{k-1}{s},$$

em particular, se s é par $\sum_{j=0}^s \binom{k}{j} (-1)^j \geq 0$, e se s é ímpar $\sum_{j=0}^s \binom{k}{j} (-1)^j \leq 0$, como queríamos demonstrar. \square

Lema 7.5. *Sejam m um produto de primos distintos e b, c inteiros primos entre si. O número de soluções de $x(bx + c) \equiv 0 \pmod{m}$ contadas módulo m é*

$$f_{bc}(m) \stackrel{\text{def}}{=} \frac{d(m)}{d(\text{mdc}(m, bc))} = 2^{\omega(m) - \omega(\text{mdc}(m, bc))}$$

onde $d(n)$ e $\omega(n)$ denotam o número de divisores de n e o número de fatores primos distintos de n , respectivamente.

DEMONSTRAÇÃO: Note que toda solução de $x(bx + c) \equiv 0 \pmod{m}$ é solução do sistema de congruências

$$\begin{aligned} x &\equiv 0 \pmod{r} \\ bx &\equiv -c \pmod{\frac{m}{r}} \end{aligned}$$

para algum $r \mid m$. Por outro lado, para cada $r \mid m$, temos que $\text{mdc}(r, \frac{m}{r}) = 1$ pois m é um produto de primos distintos, assim pelo teorema chinês dos restos o sistema acima possui uma única solução x_r módulo m se $\text{mdc}(b, \frac{m}{r}) = 1 \iff \text{mdc}(m, b) \mid r$, ou nenhuma caso contrário, uma vez que $\text{mdc}(b, c) = 1$. Assim, devemos contar o número de soluções x_r distintas módulo m quando r percorre os divisores de m tais que $\text{mdc}(m, b) \mid r$.

Sejam r e s dois divisores de m que são múltiplos de $\text{mdc}(m, b)$ e suponha $x_s \equiv x_r \pmod{m}$. Temos que $t = \frac{\text{mmc}(r, s)}{\text{mdc}(r, s)}$ (a “diferença simétrica” dos primos que dividem r e s) divide simultaneamente x_s e $bx_s + c$, logo $t \mid c$ e como $r, s \mid m$ temos que $t \mid \text{mdc}(c, m)$. Reciprocamente, dado r como antes e um divisor t de $\text{mdc}(m, c)$, podemos definir $s = \frac{\text{mmc}(r, t)}{\text{mdc}(r, t)}$, de modo que $\text{mdc}(m, b) \mid s \mid m$; a solução correspondente x_s é tal que $x_s \equiv x_r \pmod{p}$ para todo primo $p \mid m$, ou seja, temos $x_s \equiv x_r \pmod{m}$. Assim, utilizando a multiplicatividade de $d(n)$, temos que o número de soluções é

$$\frac{d(m / \text{mdc}(m, b))}{d(\text{mdc}(m, c))} = \frac{d(m)}{d(\text{mdc}(m, bc))} = \frac{2^{\omega(m)}}{2^{\omega(\text{mdc}(m, bc))}} = 2^{\omega(m) - \omega(\text{mdc}(m, bc))}$$

□

A seguinte proposição é baseada na exposição de Y. Motohashi [109] sobre o chamado *método do crivo*. Ela implica que $\pi_2(x) = O\left(x \left(\frac{\log \log x}{\log x}\right)^2\right)$;

Brun provou um resultado mais forte para primos gêmeos, a saber $\pi_2(x) = O\left(\frac{x}{(\log x)^2}\right)$. A proposição seguinte, no entanto, tem uma prova mais simples, e já é suficiente para garantir que a série dos inversos dos primos gêmeos converge, como veremos no final desta seção.

Proposição 7.6. *Sejam a, b, c inteiros positivos, primos relativos dois a dois e com exatamente um deles par. Então*

$$\pi_{a,b,c}(x) = O\left(x \left(\frac{\log \log x}{\log x}\right)^2\right)$$

DEMONSTRAÇÃO: Seja $z \leq \sqrt{\frac{x}{b}}$ e defina

$P_a(z) \stackrel{\text{def}}{=} \text{produto dos primos menores ou iguais a } z \text{ que não dividem } a$
e

$$A \stackrel{\text{def}}{=} \{k(bk + c) \mid 1 \leq k \leq x\}.$$

Observemos que se $y = k(bk + c) \in A$ com k e $\frac{bk + c}{a}$ primos e $k > \frac{a}{b}z$ então $\frac{bk + c}{a} > \frac{b}{a}k > z$ e portanto $\text{mdc}(y, P_a(z)) = 1$. Assim, temos que

$$\begin{aligned} \pi_{a,b,c}(x) &\leq \#\{y \in A \mid \text{mdc}(y, P_a(z)) = 1\} + \pi_{a,b,c}\left(\frac{a}{b}z\right) \\ &< \#\{y \in A \mid \text{mdc}(y, P_a(z)) = 1\} + \frac{a}{b}z. \end{aligned}$$

De fato, esta última parcela $z \leq \frac{a}{b}\sqrt{\frac{x}{b}}$ não afeta nossa estimativa, logo basta limitar o tamanho da primeira parcela. Para isso, observemos que pelos lemas 5.8 e 7.4, temos, para todo $l \geq 1$,

$$\begin{aligned} \#\{y \in A \mid \text{mdc}(y, P_a(z)) = 1\} &= \sum_{y \in A} \sum_{m \mid \text{mdc}(y, P_a(z))} \mu(m) \\ &\leq \sum_{y \in A} \sum_{\substack{m \mid \text{mdc}(y, P_a(z)) \\ \omega(m) \leq 2l}} \mu(m) \\ &= \sum_{\substack{m \mid P_a(z) \\ \omega(m) \leq 2l}} \mu(m) |A_m|, \end{aligned}$$

onde $A_m \stackrel{\text{def}}{=} \{y \in A \mid m \text{ divide } y\}$. Mas do lema 7.5 segue que

$$\left| A_m - \frac{x}{m} f_{bc}(m) \right| < f_{bc}(m),$$

pois de cada conjunto de m inteiros consecutivos k , exatamente $f_{bc}(m)$ deles são tais que $m \mid k(bk + c)$. Assim

$$\begin{aligned} & \#\{y \in A \mid \text{mdc}(y, P_a(z)) = 1\} \leq \\ & \leq x \sum_{\substack{m \mid P_a(z) \\ \omega(m) \leq 2l}} \frac{\mu(m) f_{bc}(m)}{m} + O\left(\sum_{\substack{m \mid P_a(z) \\ \omega(m) \leq 2l}} f_{bc}(m) \right). \end{aligned}$$

Como $m \mid P_a(z)$ e $\omega(m) \leq 2l$ implica que m é produto de no máximo $2l$ primos distintos menores ou iguais a z , segue que $m \leq z^{2l}$ e o último somando pode ser limitado como

$$\begin{aligned} \sum_{\substack{m \mid P_a(z) \\ \omega(m) \leq 2l}} f_{bc}(m) & \leq \sum_{1 \leq r \leq z^{2l}} d(r) = \sum_{1 \leq r \leq z^{2l}} \sum_{d \mid r} 1 \\ & = \sum_{d=1}^{z^{2l}} \left\lfloor \frac{z^{2l}}{d} \right\rfloor \leq z^{2l} \sum_{d=1}^{z^{2l}} \frac{1}{d} \\ & = O(z^{2l} \log(z^{2l})) \end{aligned}$$

Portanto, o propósito é escolher z e l adequados, de tal forma que o termo limitado por $z^{2l} \log(z^{2l})$ seja pequeno comparado com o outro. Tal escolha será feita mais para frente e dependerá também da limitação do somando principal

$$\sum_{\substack{m \mid P_a(z) \\ \omega(m) \leq 2l}} \frac{\mu(m) f_{bc}(m)}{m} = \sum_{m \mid P_a(z)} \frac{\mu(m) f_{bc}(m)}{m} - \sum_{\substack{m \mid P_a(z) \\ \omega(m) \geq 2l+1}} \frac{\mu(m) f_{bc}(m)}{m},$$

assim, temos que dar valores a z e l de tal forma que cada um destes termos seja dominado por $O\left(\left(\frac{\log \log x}{\log x}\right)^2\right)$.

Para isto, observemos que a função $\frac{\mu(n) f_{bc}(n)}{n}$ é multiplicativa, e assim $\sum_{m \mid n} \frac{\mu(m) f_{bc}(m)}{m}$ também é multiplicativa (teorema 5.4), logo podemos

utilizar o teorema 5.24 de onde temos que

$$\begin{aligned}
 \sum_{m|P_a(z)} \frac{\mu(m)f_{bc}(m)}{m} &= \prod_{\substack{q \text{ primo} \\ q|P_a(z)}} \left(1 + \frac{\mu(q)f_{bc}(q)}{q}\right) = A \prod_{\substack{q \text{ primo} \\ 3 \leq q \leq z}} \left(1 - \frac{2}{q}\right) \\
 &= A \exp\left(\sum_{\substack{q \text{ primo} \\ 3 \leq q \leq z}} \log\left(1 - \frac{2}{q}\right)\right) \\
 &= \exp\left(O(1) - 2 \sum_{\substack{q \text{ primo} \\ q \leq z}} \frac{1}{q}\right) \\
 &= \exp(O(1) - 2 \log \log z) = O((\log z)^{-2})
 \end{aligned}$$

onde

$$A = \begin{cases} \frac{1}{2} \prod_{\substack{q \text{ primo} \\ 3 \leq q \leq z, q|bc}} \left(1 - \frac{1}{q}\right) \left(1 - \frac{2}{q}\right)^{-1} & \text{se } A \text{ é ímpar} \\ \prod_{\substack{q \text{ primo} \\ 3 \leq q \leq z, q|bc}} \left(1 - \frac{1}{q}\right) \left(1 - \frac{2}{q}\right)^{-1} & \text{se } A \text{ é par.} \end{cases}$$

Para estimar o termo restante, observe que $\omega(m) \geq 2l + 1$ implica $f_{bc}(m) \geq \frac{2^{2l+1}}{bc}$, donde $f_{bc}(m) \leq \frac{bc}{2} 2^{-2l} f_{bc}(m)^2$. Assim,

$$\left| \sum_{\substack{m|P_a(z) \\ \omega(m) \geq 2l+1}} \frac{\mu(m)f_{bc}(m)}{m} \right| \leq \frac{bc}{2} 2^{-2l} \sum_{m|P_a(z)} \frac{(f_{bc}(m))^2}{m}.$$

Como $\frac{(f_{bc}(n))^2}{n}$ é multiplicativa, segue que $\sum_{m|n} \frac{(f_{bc}(n))^2}{n}$ é multiplicativa e

portanto

$$\begin{aligned}
 \sum_{m|P_a(z)} \frac{(f_{bc}(m))^2}{m} &= \prod_{\substack{q \text{ primo} \\ q|P_a(z)}} \left(1 + \frac{(f_{bc}(q))^2}{q} \right) = B \prod_{\substack{q \text{ primo} \\ 3 \leq q \leq z}} \left(1 + \frac{4}{q} \right) \\
 &= B \exp \left(\sum_{\substack{q \text{ primo} \\ 3 \leq q \leq z}} \log \left(1 + \frac{4}{q} \right) \right) \\
 &= \exp \left(O(1) + 4 \sum_{\substack{q \text{ primo} \\ q \leq z}} \frac{1}{q} \right) = \exp(O(1) + 4 \log \log z) \\
 &= O(\log^4 z),
 \end{aligned}$$

onde

$$B = \begin{cases} \frac{3}{2} \prod_{\substack{q \text{ primo} \\ 3 \leq q \leq z, q|bc}} \left(1 + \frac{1}{q} \right) \left(1 + \frac{4}{q} \right)^{-1} & \text{se } a \text{ é ímpar} \\ \prod_{\substack{q \text{ primo} \\ 3 \leq q \leq z, q|bc}} \left(1 + \frac{1}{q} \right) \left(1 + \frac{4}{q} \right)^{-1} & \text{se } a \text{ é par.} \end{cases}$$

Desta forma obtemos que

$$\begin{aligned}
 &\#\{y \in A \mid \text{mdc}(y, P_a(z)) = 1\} = \\
 &= O(x(\log z)^{-2}) + O(x2^{-2l} \log^4 z) + O(z^{2l} \log(z^{2l})).
 \end{aligned}$$

Precisamos escolher z e l de tal forma que a ordem de grandeza dos somandos à direita sejam simultaneamente “pequenos”. De fato, fazendo

$$z = \exp\left(\frac{\log x}{20 \log \log x}\right) \quad \text{e} \quad l = \left\lfloor \frac{\log x}{4 \log z} \right\rfloor = \lfloor 5 \log \log x \rfloor,$$

temos que

$$z^{2l} \log(z^{2l}) = O(\sqrt{x} \log x), \quad x(\log z)^{-2} = O\left(x \left(\frac{\log \log x}{\log x}\right)^2\right)$$

e

$$\begin{aligned}
O(x2^{-2l} \log^4 z) &= O(x \exp(-10 \log 2 \log \log x) \cdot \log^4 z) \\
&= O\left(x \log^{-6} x \cdot \left(\frac{\log x}{\log \log x}\right)^4\right) \\
&= O\left(\frac{x}{(\log \log x)^4 \log^2 x}\right),
\end{aligned}$$

pois $10 \log 2 > 6$. Isto completa a prova, pois as funções $\sqrt{x} \log x$ e $\frac{x}{(\log \log x)^4 \log^2 x}$ são dominadas pela função $x \left(\frac{\log \log x}{\log x}\right)^2$. \square

Corolário 7.7. $\sum_{p, p+2 \text{ primos}} \frac{1}{p} < \infty$.

DEMONSTRAÇÃO:

$$\begin{aligned}
\sum_{p, p+2 \text{ primos}} \frac{1}{p} &= \sum_{n=0}^{\infty} \sum_{\substack{p, p+2 \text{ primos} \\ 2^n \leq p < 2^{n+1}}} \frac{1}{p} \leq \sum_{n=0}^{\infty} \frac{\pi_2(2^{n+1})}{2^n} \\
&= O\left(\sum_{n=0}^{\infty} \frac{2^{n+1} \left(\frac{\log(n+1)}{n+1}\right)^2}{2^n}\right) \\
&= O\left(\sum_{n=0}^{\infty} \left(\frac{\log(n+1)}{n+1}\right)^2\right) < \infty.
\end{aligned}$$

□

7.1.3 Outros Resultados e Conjeturas sobre Primos

Nesta seção veremos o enunciado de alguns resultados clássicos sobre números primos. Também veremos vários problemas em aberto famosos.

Teorema 7.8 (Dirichlet). *Dados naturais a, d com $\text{mdc}(a, d) = 1$, existem infinitos primos da forma $a + dn$ (com n natural).*

A demonstração usual deste teorema, dada no apêndice A, usa variáveis complexas. Muitos casos particulares admitem demonstrações

elementares mais ou menos simples. O leitor não deve ter dificuldade em demonstrar, por exemplo, que existem infinitos primos da forma $4n + 3$ ou $6n + 5$.

A seguir mostramos um caso particular do teorema de Dirichlet, no qual usaremos ferramentas elementares para sua prova. Usaremos o *polinômio ciclotômico* $\phi_m(x)$ definido indutivamente pela fórmula

$$\prod_{\ell|m} \phi_\ell(x) = x^m - 1.$$

Verifica-se facilmente que $\phi_m(x)$ é o polinômio mônico de grau $\phi(m)$ cujas raízes são $\exp(2k\pi i/m)$, $0 \leq k < m$, $\text{mdc}(k, m) = 1$. Além disso, $\phi_m(x) \in \mathbb{Z}[x]$.

Teorema 7.9. *Para todo inteiro positivo d , existem infinitos primos na progressão aritmética $S = \{dn + 1\}_{n \in \mathbb{N}}$.*

DEMONSTRAÇÃO: Suponhamos que em S existe apenas um número finito de primos p_1, \dots, p_l e definamos $a = 2dp_1 \cdots p_l$. Seja q um divisor primo de $\phi_d(a)$. Dado que $q \mid \phi_d(a) \mid a^d - 1$, temos que $a^d \equiv 1 \pmod{q}$. Mostremos que $d = \text{ord}_q a$. De fato, se $e = \text{ord}_q a$ é um divisor próprio de d , como o polinômio $(x^e - 1)\phi_d(x)$ divide $x^d - 1$ então $a \pmod{q}$ será raiz dupla de $x^d - 1 \in \mathbb{Z}/(q)[x]$. Mas $q \mid a^d - 1$ e $d \mid a$ implica $q \nmid d$, assim todas as raízes de $x^d - 1$ são simples porque sua derivada dx^{d-1} só é nula em $x \equiv 0 \pmod{q}$, que não é raiz de $x^d - 1$. Portanto $d = \text{ord}_q a$ e assim $d \mid q - 1$, isto é, $q = nd + 1 \in S$, mas $q \neq p_j$ pois $q \mid a^d - 1 \implies q \nmid a$, logo $q \notin S$, o que é uma contradição. \square

Existem vários refinamentos conhecidos do teorema de Dirichlet. Definimos $\pi_{d,a}(x)$ como sendo o número de primos da forma $a + dn$ no intervalo $[2, x]$. De la Vallée Poussin provou que

$$\lim_{x \rightarrow +\infty} \frac{\pi_{d,a}(x)}{\pi(x)} = \frac{1}{\varphi(d)},$$

isto é, todas as possíveis classes módulo d têm aproximadamente a mesma proporção de primos. Uma prova deste resultado, utilizando variáveis complexas, encontra-se no apêndice.

Por outro lado, Tchebychev observou que para valores pequenos de x , $\pi_{3,2}(x) - \pi_{3,1}(x)$ e $\pi_{4,3}(x) - \pi_{4,1}(x)$ são positivos. Um teorema de

Littlewood, entretanto, demonstra que estas funções mudam de sinal infinitas vezes. Em 1957, Leech demonstrou que o menor valor de x para o qual $\pi_{4,3}(x) - \pi_{4,1}(x) = -1$ é 26861 e em 1978 Bays e Hudson demonstraram que o menor valor de x para o qual $\pi_{3,2}(x) - \pi_{3,1}(x) = -1$ é 608981813029.

Seja $p(d, a)$ o menor primo da forma $a + dn$, n inteiro e

$$p(d) = \max\{p(d, a) \mid 0 < a < d, \text{mdc}(a, d) = 1\}.$$

Linnik (1944) provou que existe $L > 1$ com $p(d) < d^L$ para todo d suficientemente grande. A melhor estimativa conhecida para L é $L \leq 5,5$, devida a Heath-Brown (1992), que também conjecturou que

$$p(d) \leq Cd(\log d)^2.$$

Por outro lado, não se sabe demonstrar que existam infinitos primos da forma $n^2 + 1$; aliás, não existe nenhum polinômio P em uma variável e de grau maior que 1 para o qual se saiba demonstrar que existem infinitos primos da forma $P(n)$, $n \in \mathbb{Z}$. Mas, existem muitos polinômios em mais de uma variável que assumem infinitos valores primos: por exemplo, prova-se facilmente que todo primo da forma $4n + 1$ pode ser escrito também na forma $a^2 + b^2$, $a, b \in \mathbb{Z}$ (ver teoremas 4.6, 4.19 e 6.12). Recentemente, Friedlander e Iwaniec provaram um resultado muito mais difícil: que existem infinitos primos da forma $a^2 + b^4$.

Um dos problemas em aberto mais famosos da Matemática é a conjectura de Goldbach: todo número par maior ou igual a 4 é a soma de dois primos. Chen demonstrou que todo número par suficientemente grande é a soma de um primo com um número com no máximo dois fatores primos. Vinogradov demonstrou que todo ímpar suficientemente grande (por exemplo, maior do que $3^{3^{15}}$) é uma soma de três primos. Mais recentemente, H. Helfgott anunciou ([68]) uma demonstração de que todo ímpar maior do que 5 é soma de três primos.

Seja p_n o n -ésimo número primo. O teorema dos números primos equivale a dizer que (c.f. corolário 5.16)

$$\lim_{n \rightarrow \infty} \frac{p_n}{n \log n} = 1.$$

Por outro lado, sabe-se muito pouco sobre o comportamento da função $d_n = p_{n+1} - p_n$. Por exemplo, a conjectura de que existem infinitos

primos gêmeos equivale a dizer que $\liminf d_n = 2$. Seja

$$L = \liminf \frac{d_n}{\log p_n};$$

Erdős provou que $L < 1$ e Maier que $L \leq 0,248$. Apenas em 2005, D. A. Goldston, J. Pintz e C. Y. Yıldırım provaram que $L = 0$ (ver [57]). De fato eles provaram bem mais (ver [58]): por exemplo, temos

$$\liminf \frac{d_n}{\sqrt{\log p_n}(\log \log p_n)^2} < \infty.$$

E, em 2013, Y. Zhang realizou um avanço muito importante, provando que $\liminf d_n < 70000000$ (ver [155]). Erdős também provou que o conjunto dos pontos de acumulação de $d_n/\log p_n$ tem medida positiva. Por outro lado, pelo postulado de Bertrand, sempre existe pelo menos um primo entre m e $2m$, ou seja, $d_n < p_n$. Em 1931, Westzynthius provou que

$$\limsup \frac{d_n}{\log p_n} = \infty,$$

e em 1963 Rankin, completando um trabalho de Erdős, mostrou que

$$\limsup \frac{d_n(\log \log \log p_n)^2}{\log p_n \cdot \log \log p_n \cdot \log \log \log p_n} \geq e^\gamma \approx 1,78107$$

onde γ é a já mencionada constante de Euler-Mascheroni. Este resultado foi melhorado por Pomerance e posteriormente por Pintz, que provou que o lado esquerdo é maior do que ou igual a $2e^\gamma$ (ver [115]). Conjetura-se que

$$\limsup \frac{d_n}{(\log p_n)^2} = C$$

para alguma constante positiva C . Observamos que a primeira vez que $d_n > 1000$ ocorre para $p_n = 1693182318746371$, quando $d_n = 1132$, o que foi descoberto recentemente por T. Nicely e D. Nyman.

Outra conjectura famosa é que sempre há pelo menos um primo entre n^2 e $(n+1)^2$. Por outro lado, sabe-se que existe um primo entre n^3 e $(n+1)^3$ para todo $n > e^{e^{15}}$ (ver [33]). Mais ainda, para x suficientemente grande, sempre existe um primo no intervalo $(x, x+x^w)$ onde $w = 0.525$ (ver [11]).

Ben Green e Terence Tao provaram em [62] que existem progressões aritméticas arbitrariamente grandes formadas exclusivamente por

números primos (veja [7] para um texto expositório sobre este teorema e outros resultados relacionados). A maior progressão aritmética conhecida formada exclusivamente por números primos, que tem 26 termos, é

$$43142746595714191 + 5283234035979900 \cdot n = \\ 43142746595714191 + 23681770 \cdot 23\# \cdot n,$$

para $n = 0, 1, \dots, 25$, onde $n\#$ denota o produto dos primos menores do que ou iguais a n . Esta progressão aritmética foi descoberta em 12 de abril de 2010 por Benoît Perichon usando um programa desenvolvido por Jaroslaw Wroblewski em Geoff Reynolds, em um projeto distribuído do *PrimeGrid*, que é um projeto cooperativo para procurar primos grandes de diversos tipos - veja <http://www.primegrid.com/> para mais informações.

Sierpinski provou que existem infinitos números naturais k tais que $k \cdot 2^n + 1$ é composto para todo natural n e Riesel provou o mesmo resultado para $k \cdot 2^n - 1$. Conjetura-se que os menores valores de k com as propriedades acima são respectivamente 78557 e 509203. Há um projeto cooperativo, que consiste em procurar primos grandes, para demonstrar estas conjecturas (veja observação a seguir).

Também existem infinitos naturais ímpares k que são simultaneamente números de Sierpinski e de Riesel, os chamados *números de Brier*. O menor número de Brier conhecido é 143665583045350793098657. Veja

<http://oeis.org/A076335>

e as páginas e referências lá mencionadas para mais informações.

O leitor interessado em aprender mais sobre problemas em aberto em teoria dos números pode consultar [63].

Observação 7.10. *Um sumário de vários projetos cooperativos para encontrar primos grandes pode ser visto em <http://www.prothsearch.net/> Projetos ativos que pretendem provar que 78557 e 509203 são os menores números de Sierpinski e Riesel podem ser encontrados respectivamente em*

<http://www.seventeenorbust.com/> e <http://www.rieselsieve.com/>.

O projeto Seventeen or Bust tem obtido resultados particularmente bons nos últimos anos. O fato de que 78557 é um número de Sierpinski foi

provado em 1962 por John Selfridge (veja o exercício 7.4). Quando o projeto começou, em 2002, havia 17 números menores que 78557 sobre os quais não se sabia se eram números de Sierpinski ou não: 4847, 5359, 10223, 19249, 21181, 22699, 24737, 27653, 28433, 33661, 44131, 46157, 54767, 55459, 65567, 67607 e 69109.

Desde então, os participantes do projeto encontraram os seguintes primos

Primo	Descubridor	Data
$46157 \cdot 2^{698207} + 1$	S. Gibson	27/11/2002
$65567 \cdot 2^{1013803} + 1$	J. Burt	3/12/2002
$44131 \cdot 2^{995972} + 1$	equipe <i>deviced</i>	6/12/2002
$69109 \cdot 2^{1157446} + 1$	S. DiMichele	7/12/2002
$54767 \cdot 2^{1337287} + 1$	P. Coels	22/12/2002
$5359 \cdot 2^{5054502} + 1$	R. Sundquist	6/12/2003
$28433 \cdot 2^{7830457} + 1$	equipe <i>TeamPrimeRib</i>	30/11/2004
$27653 \cdot 2^{9167433} + 1$	D. Gordon	8/06/2005
$4847 \cdot 2^{3321063} + 1$	R. Hassler	15/10/2005
$19249 \cdot 2^{13018586} + 1$	K. Agafonov	5/05/2007
$33661 \cdot 2^{7031232} + 1$	S. Sunde	17/10/2007

Sobram portanto os 6 números 10223, 21181, 22699, 24737, 55459 e 67607. Veja <http://www.seventeenorbust.com/> para mais informações (em particular sobre como participar do projeto).

7.2 Fórmulas para Primos

Não se conhece nenhuma fórmula simples para gerar primos arbitrariamente grandes. Uma palavra imprecisa mas importante nesta frase é “simples”. Existem fórmulas que geram números primos, mas que são tão complicadas que não ajudam muito nem a gerar números primos explicitamente nem a responder perguntas teóricas sobre a distribuição dos primos. Um exemplo de fórmula para p_n , o n -ésimo primo, é

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor,$$

onde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$; deixamos a demonstração a cargo do leitor. Outra fórmula é

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

onde

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0.0203000500000007 \dots$$

A inutilidade desta última fórmula vem do fato que para calcular c devemos encontrar todos os primos; a fórmula se tornaria mais interessante se existisse outra interpretação para o número real c , o que parece muito improvável.

Por outro lado, Mills provou que existem números reais $A > 1$ tal que $\lfloor A^{3^n} \rfloor$ é primo para todo $n \in \mathbb{N}$. Mais geral ainda,

Teorema 7.11. *Se $S = \{a_n\} \subset \mathbb{N}$ é uma sequência com a propriedade que: existem números reais x_0 e w com $0 < w < 1$, tais que para todo $x > x_0$ o intervalo aberto $(x, x + x^w)$ contém um elemento de S . Então para todo número real $c > \min\{1/(1-w), 2\}$, existe um número A tal que $\lfloor A^{c^n} \rfloor$ é uma subsequência de S .*

DEMONSTRAÇÃO: Definamos uma subsequência $\{b_n\}$ de S recursivamente por

1. b_1 o menor elemento de S tal que $b_1^c \geq x_0$.
2. b_{n+1} o menor elemento de S que satisfaz $b_n^c < b_{n+1} < b_n^c + b_n^{wc}$.

Como $c \geq \frac{1}{1-w}$ e $c \geq 2$, segue que

$$b_n^c < b_{n+1} < 1 + b_{n+1} < 1 + b_n^c + b_n^{wc} < 1 + b_n^c + b_n^{c-1} \leq (1 + b_n)^c.$$

tomando a $c^{-(n+1)}$ -ésima potência na desigualdade anterior temos que

$$b_n^{c^{-n}} < b_{n+1}^{c^{-(n+1)}} < (1 + b_{n+1})^{c^{-(n+1)}} \leq (1 + b_n)^{c^{-n}},$$

o que mostra que a sequência $\{b_n^{c^{-n}}\}$ converge para um número real A . Segue que $b_n < A^{c^n} < 1 + b_n$ e portanto $b_n = \lfloor A^{c^n} \rfloor$. \square

Corolário 7.12 (Mills). *Existe uma constante A tal que $\lfloor A^{3^n} \rfloor$ é primo para todo $n \in \mathbb{N}$.*

DEMONSTRAÇÃO: Pelo teorema anterior tomando S a sequência de primos, é conhecido (ver [11]) que entre $(x, x + x^w)$ sempre existe um primo com x suficientemente grande e $w = 0.525$. \square

Um tipo de fórmula para primos, de certa forma mais intrigante, são polinômios de coeficientes inteiros em S variáveis com a seguinte propriedade quase mágica: a intersecção da imagem de \mathbb{N}^S com \mathbb{N} é exatamente o conjunto dos números primos. Note que se tomarmos um ponto de \mathbb{N}^S “ao acaso”, o valor do polinômio neste ponto quase certamente será negativo; assim, é difícil usar o polinômio para gerar primos. A título de curiosidade, vejamos um exemplo de polinômio com estas propriedades; aqui $S = 26$, o valor do polinômio é P , as variáveis chamam-se a, b, \dots, z e A, B, \dots, N são expressões auxiliares:

$$P = (k + 2)(1 - A^2 - B^2 - C^2 - \dots - N^2),$$

$$A = wz + h + j - q,$$

$$B = (gk + 2g + k + 1)(h + j) + h - z,$$

$$C = 16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2,$$

$$D = 2n + p + q + z - e,$$

$$E = e^3(e + 2)(a + 1)^2 + 1 - o^2,$$

$$F = (a^2 - 1)y^2 + 1 - x^2,$$

$$G = 16r^2y^4(a^2 - 1) + 1 - u^2,$$

$$H = ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2,$$

$$I = (a^2 - 1)l^2 + 1 - m^2,$$

$$J = ai + k + 1 - l - i,$$

$$K = n + l + v - y,$$

$$L = p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m,$$

$$M = q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x,$$

$$N = z + pl(a - p) + t(2ap - p^2 - 1) - pm.$$

Algumas observações simples: a única forma de P ser positivo é se $A = B = \dots = N = 0$; neste caso seu valor será $k + 2$. Vemos assim que para

produzir um número primo P com este polinômio devemos antes de mais nada tomar $k = P - 2$. As expressões auxiliares viram equações: como $A = 0$ temos $q = wz + h + j$. Assim, dado k para o qual $k + 2$ é primo, precisamos procurar valores para as outras letras que satisfaçam estas equações. Estes valores de certa forma *codificam* uma demonstração de que $P = k + 2$ é primo.

Problemas Propostos

7.1. a) *Sejam x inteiro e p um divisor primo de $20x^2 - 1$. Prove que $p \equiv \pm 1 \pmod{10}$.*

b) *Mostrar que existem infinitos primos que terminam no dígito 9.*

7.2. *Mostrar que existe um intervalo de 1000 números inteiros positivos consecutivos contendo exatamente cinco números primos.*

7.3. *Mostrar que não existem polinômios P e Q tais que $\pi(x) = \frac{P(x)}{Q(x)}$ para todo $x \in \mathbb{N}$.*

7.4. *Prove que 78557 é um número de Sierpinski, e que existem infinitos números de Sierpinski a partir das congruências*

$$78557 \cdot 2^0 + 1 \equiv 0 \pmod{3}$$

$$78557 \cdot 2^1 + 1 \equiv 0 \pmod{5}$$

$$78557 \cdot 2^7 + 1 \equiv 0 \pmod{7}$$

$$78557 \cdot 2^{11} + 1 \equiv 0 \pmod{13}$$

$$78557 \cdot 2^3 + 1 \equiv 78557 \cdot 2^{39} + 1 \equiv 0 \pmod{73}$$

$$78557 \cdot 2^{15} + 1 \equiv 0 \pmod{19}$$

$$78557 \cdot 2^{27} + 1 \equiv 0 \pmod{37}.$$

7.5. *Mostre que o teorema do número primo é de fato equivalente a*

$$\lim_{n \rightarrow \infty} \frac{p_n}{n \log n} = 1.$$

onde p_n denota o n -ésimo número primo.

7.6. *Mostrar que se p é um número primo, então $p^p - 1$ tem um fator primo que é congruente a 1 módulo p .*

7.7. *Seja p_n o n -ésimo número primo. Mostrar que para todo $n \geq 6$*

$$\pi(\sqrt{p_1 p_2 \cdots p_n}) > 2n.$$

7.8. *Mostrar que o número de primos entre n e $2n$ é menor do que $\frac{2n}{\log_2 n}$.*

7.9. *Seja t_n a soma dos primeiros n primos. Mostrar que para cada $n > 1$ o intervalo $[t_n, t_{n+1}]$ contém quadrados perfeitos.*

7.10. *Mostrar que existem dois quadrados consecutivos tais que existem ao menos 1000 primos entre eles.*

7.11. *Mostrar que para todo $n \geq 9$ entre n e $2n - 7$ sempre existe um número primo.*

7.12. *Seja $\Phi(x, y) = \#\{n \leq x \mid \text{todo divisor primo de } n \text{ é maior que } y\}$. Prove que, se $y \leq \exp(\log x / 10 \log \log x)$ então*

$$\Phi(x, y) = O\left(\frac{x}{\log y}\right).$$

Sugestão: *Adapte a prova da proposição 7.6.*

7.13. *Mostrar que não existem 11 primos, todos menores que 20000 e em progressão aritmética.*

7.14. *Prove que numa progressão aritmética formada por n primos, a razão deve ser um múltiplo de $(n - 1)\#$, e, a menos que n seja primo e o menor termo da progressão seja n , sua razão deve ser um múltiplo de $n\#$.*

Obs.: *Lembramos que $m\#$ denota o produto dos primos menores do que ou iguais a m .*

7.15. *Mostrar que, salvo os números 1, 4, e 6, todo número natural pode ser escrito como uma soma de primos distintos.*

7.16. *Mostrar que para cada primo p no intervalo $(n, \frac{4n}{3}]$, p divide*

$$\sum_{j=0}^n \binom{n}{j}^4.$$

7.3 Testes de Primalidade

Uma questão relacionada com a de *gerar* números primos é a de *testar* se um determinado número é primo. Com o advento dos computadores, a partir da década de 60, surgiram inúmeras tentativas de se obter um algoritmo eficiente para o teste de primalidade de um número. A relevância desse problema tem crescido imensamente em anos recentes devido à utilização intensa de números primos em algoritmos de criptografia, como os algoritmos RSA e El Gamal para criptografia pública. Dessa forma o problema do teste de primalidade se tornou um importante problema para a ciência da computação teórica. Sobre esse ponto de vista duas coisas são requeridas: um certificado de prova de que o algoritmo realmente produz a resposta correta; e uma medida da eficiência do algoritmo, isto é, quão bem o algoritmo faz uso dos recursos computacionais (como o tempo ou número de passos executados, espaço ou memória utilizada) em função do tamanho da entrada do problema para a obtenção da solução.

Existe um algoritmo bastante simples para testar se qualquer inteiro positivo n é primo, devido ao matemático grego Eratóstenes (ca. 240 A.C.): calcule o resto da divisão de n por cada inteiro m com $2 \leq m \leq \sqrt{n}$. Se o resto for 0 em algum caso então n é composto e encontramos um divisor; se isto nunca ocorrer, n é primo. O inconveniente deste algoritmo é que ele é muito lento. O tamanho da entrada do algoritmo para um dado número n é o tamanho da sua codificação em bits, que é aproximadamente $k = \log_2 n$ pois $2^k \leq n < 2^{k+1}$. Portanto, em termos do tamanho da entrada k , temos que o número de operações é $O(\sqrt{n}) = O(2^{k/2})$, ou seja, o algoritmo tem complexidade de tempo exponencial no tamanho da entrada. Assim, mesmo para um inteiro de 200 dígitos, teríamos que fazer aproximadamente 10^{100} divisões, o que não só está fora do alcance da tecnologia atual mas fora do alcance de qualquer tecnologia plausível de acordo com o que se conhece de Física¹.

¹Bem, esta frase parecia verdadeira há uns dez anos atrás mas hoje suspeita-se que alguns aspectos da Física quântica possam ser explorados para colocar um computador especial em um estado de superposição em que ele faz várias contas diferentes em paralelo. Desta forma seria possível não apenas testar primalidade rapidamente mas até fatorar rapidamente inteiros muito grandes. Alguns *computadores quânticos* (é assim que são chamadas estas máquinas) extremamente rudimentares (com uns poucos q -bits de memória) já foram construídos mas não se sabe com certeza se é realmente possível construir computadores quânticos capazes, por exemplo, de fatorar

Alguns teoremas de Teoria dos Números podem ser usados para testar a primalidade de um inteiro positivo n . Pelo teorema de Wilson, por exemplo, podemos testar a primalidade de n calculando $(n-1)! \bmod n$; infelizmente, esta conta parece ser tão difícil de efetuar quanto a busca de divisores pelo algoritmo anterior. Observe que dizemos apenas que a conta *parece* difícil: não está excluída a possibilidade de alguém inventar um algoritmo rápido para calcular $(n-1)! \bmod n$.

Uma ideia mais bem sucedida é a de usar o pequeno teorema de Fermat: tomamos a , $1 < a < n$, e calculamos $a^{n-1} \bmod n$. Se n for primo teremos $a^{n-1} \equiv 1 \pmod{n}$; qualquer outro resultado indica que n é composto mesmo sem termos encontrado um fator de n . Observe que para calcular $a^{n-1} \bmod n$ não precisamos calcular $a \cdot a \cdots a$, $n-1$ vezes. Podemos fazer esta conta com menos de $4 \log_2 n$ operações envolvendo inteiros menores do que n^2 : se $n-1 = \sum_{0 \leq i < N} b_i 2^i$, $N = \lfloor \log_2(n-1) \rfloor$, então definimos

$$p_k = a^{\sum_{0 \leq i < k} b_i 2^i} \bmod n$$

e temos $p_0 = 1$, $p_N = a^{n-1} \bmod n$, e podemos calcular p_{k+1} a partir de p_k com uma operação de elevar ao quadrado, tomar o resto da divisão por n , possivelmente multiplicar por a e novamente de tomar o resto da divisão por n .

Se $a^{n-1} \equiv 1 \pmod{n}$, por outro lado, não demonstramos que n é primo; se n for composto satisfazendo $a^{n-1} \equiv 1 \pmod{n}$ dizemos que n é um *pseudoprimo* na base a . Pseudoprimos existem mas são raros (ver [34]): o menor pseudoprimo na base 2 é $341 = 11 \cdot 31$ e existem apenas 21 853 pseudoprimos na base 2 menores do que $2,5 \cdot 10^{10}$ (contra 1 091 987 405 primos). Pomerance (melhorando um resultado anterior de Erdős) provou que se $P\pi_a(x)$ é o número de pseudoprimos até x na base a temos

$$P\pi_a(x) \leq x \cdot e^{-\frac{\log x \log \log \log x}{2 \log \log x}}$$

para x suficientemente grande. A proposição abaixo exhibe uma família infinita de pseudoprimos na base a (para qualquer $a > 1$ dado); assim a simples verificação $a^{n-1} \equiv 1 \pmod{n}$ não *demonstra* a primalidade de n .

rapidamente inteiros grandes; se isto for possível, o impacto científico e tecnológico será imenso. Por outro lado, não se sabe exatamente quais tarefas seriam rápidas para um computador quântico; suspeita-se que alguns problemas, como o de verificar se um grafo pode ser pintado com três cores de modo que não haja vértices adjacentes de mesma cor, seriam difíceis mesmo para este novo tipo de equipamento.

Proposição 7.13. *Seja $a > 1$ e p primo, $p > 2$, p não divide $a^2 - 1$. Então*

$$n = \frac{a^{2p} - 1}{a^2 - 1} = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}$$

é um pseudoprimo na base a .

DEMONSTRAÇÃO: Como $a \pm 1$ são inversíveis módulo p e $a^p \equiv a \pmod{p}$ pelo pequeno teorema de Fermat,

$$\frac{a^p - 1}{a - 1} \equiv \frac{a^p + 1}{a + 1} \equiv 1 \pmod{p}$$

e verifica-se facilmente que estes números são ímpares (considere a maior potência de 2 que divide $a \pm 1$ e proceda como na prova da proposição 1.75), donde $n \equiv 1 \pmod{2p}$, ou $n = 2kp + 1$ para k inteiro. Assim, como $a^{2p} \equiv 1 \pmod{n}$ temos $a^n = a^{2kp+1} = (a^{2p})^k \cdot a \equiv a \pmod{n}$. \square

Uma ideia natural é a de testar vários valores de a . Claramente, se $\text{mdc}(a, n) > 1$, teremos $a^{n-1} \not\equiv 1 \pmod{n}$; entretanto, se n for um produto de uns poucos primos grandes os valores de a para os quais $\text{mdc}(a, n) > 1$ são raros e se formos obrigados a encontrar um tal valor de a teremos feito muito pouco progresso em relação aos primeiros algoritmos. Aliás, uma vez encontrado a com $\text{mdc}(a, n) > 1$ é fácil encontrar $\text{mdc}(a, n)$ pelo algoritmo de Euclides, o que nos dá uma fatoração (parcial) de n . É um fato interessante que existam alguns raros números compostos n , chamados *números de Carmichael*, com a propriedade de que se $0 < a < n$ e $\text{mdc}(a, n) = 1$ então $a^{n-1} \equiv 1 \pmod{n}$. Foi até demonstrado recentemente por Alford, Granville e Pomerance que se $CN(x)$ é a quantidade de números de Carmichael menores do que x então

$$CN(x) \geq x^{2/7}$$

para x suficientemente grande, o que implica na existência de infinitos números de Carmichael. Há apenas 2163 números de Carmichael menores do que $2,5 \cdot 10^{10}$ e os primeiros são 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 e 75361².

²Veja <ftp://ftp.dpmms.cam.ac.uk/pub/Carmichael> para a lista dos números de Carmichael menores do que 10^{16} .

7.3.1 O teste probabilístico de Miller-Rabin

Podemos refinar o conceito de pseudoprimo para definir *pseudoprimos fortes* na base a . Para definir quando n é um pseudoprimo forte na base a inicialmente escrevemos $n - 1 = 2^k \cdot b$, com b ímpar. Se $n > 2$ é primo deve existir um menor valor de j para o qual $(a^b)^{2^j} \equiv 1 \pmod{n}$ (observe que por Fermat $(a^b)^{2^k} \equiv 1 \pmod{n}$). Se $j = 0$ isto significa que $a^b \equiv 1 \pmod{n}$; caso contrário temos $(a^b)^{2^{j-1}} \equiv -1 \pmod{n}$ já que -1 é o único valor de x diferente de 1 (módulo n) para o qual $x^2 \equiv 1 \pmod{n}$. Assim, dizemos que n composto ímpar é um pseudoprimo forte na base a se *ou* $a^b \equiv 1 \pmod{n}$ *ou* existe $j' < k$ com $(a^b)^{2^{j'}} \equiv -1 \pmod{n}$. Claramente todo pseudoprimo forte na base a é um pseudoprimo na base a mas pseudoprimos fortes são mais raros do que pseudoprimos.

Observe que se n for pseudoprimo mas não pseudoprimo forte na base a , então o teste acima não apenas demonstra que n é composto mas produz uma fatoração parcial de n . De fato, seja $c = (a^b)^{2^{j-1}}$; temos $c - 1 \not\equiv 0 \pmod{n}$, $c + 1 \not\equiv 0 \pmod{n}$ mas $(c - 1)(c + 1) = c^2 - 1 \equiv 0 \pmod{n}$. Assim, $n = \text{mdc}(n, c - 1) \cdot \text{mdc}(n, c + 1)$.

Existem infinitos pseudoprimos fortes em qualquer base $a > 1$: Pomerance provou que, se $SP\pi_a(x)$ é o número de pseudoprimos fortes na base a menores ou iguais a x então

$$SP\pi_a(x) \geq e^{(\log x)^{5/14}}$$

para todo x suficientemente grande (ver [118]). Não existem “números de Carmichael fortes”: para todo número composto ímpar n existe $0 < a < n$ com $\text{mdc}(a, n) = 1$ e tal que n não é um pseudoprimo forte na base a . Melhor ainda, os valores de a que servem de testemunha para a não-primalidade de n são sempre relativamente frequentes.

Teorema 7.14. *Seja*

$$\alpha(n) = \frac{1}{\varphi(n)} \{a \mid 0 < a < n, n \text{ é um pseudoprimo forte na base } a\}.$$

Então para todo número composto ímpar $n > 9$ temos $\alpha(n) \leq 1/4$. A igualdade vale exatamente para os compostos n das seguintes formas:

$$n = p_1 p_2, \quad p_1, p_2 \text{ primos}, \quad p_1 \equiv 3 \pmod{4}, \quad p_2 = 2p_1 - 1;$$

$$n = p_1 p_2 p_3, \quad p_1, p_2, p_3 \text{ primos}, \quad p_i \equiv 3 \pmod{4}, \quad n \text{ número de Carmichael.}$$

DEMONSTRAÇÃO: Como acima, escreve $n - 1 = 2^k b$, b ímpar. Seja $n = p_1^{e_1} \dots p_m^{e_m}$ a fatoração canônica de n . Escreva $p_i - 1 = 2^{k_i} b_i$, b_i ímpar. Pelo teorema chinês dos restos e pela existência de raízes primitivas módulo $p_i^{e_i}$, temos um isomorfismos de grupos abelianos $(\mathbb{Z}/(n))^* = G = G_2 \oplus G_b \oplus G_p$ onde

$$\begin{aligned} G_2 &= \mathbb{Z}/(2^{k_1}) \oplus \dots \oplus \mathbb{Z}/(2^{k_m}), \\ G_b &= \mathbb{Z}/(b_1) \oplus \dots \oplus \mathbb{Z}/(b_m), \\ G_p &= \mathbb{Z}/(p_1^{e_1-1}) \oplus \dots \oplus \mathbb{Z}/(p_m^{e_m-1}). \end{aligned}$$

Dado $a \in (\mathbb{Z}/(n))^*$, seja $(a_{2,1}, \dots, a_{2,m}, a_{b_1}, \dots, a_{b_m}, a_{p_1}, \dots, a_{p_m})$ a imagem de a em $G_2 \oplus G_b \oplus G_p$. Assim, a imagem de $a^{(2^j b)}$ nesta soma direta é $(2^j b a_{2,1}, \dots, 2^j b a_{2,m}, 2^j b a_{b_1}, \dots, 2^j b a_{b_m}, 2^j b a_{p_1}, \dots, 2^j b a_{p_m})$ e n é pseudoprimo forte na base a se e somente se

$$\begin{aligned} (b a_{2,1}, \dots, b a_{2,m}, b a_{b_1}, \dots, b a_{b_m}, b a_{p_1}, \dots, b a_{p_m}) \\ = (s_1, \dots, s_m, 0, \dots, 0, 0, \dots, 0) \end{aligned}$$

onde $\text{ord}(s_1) = \dots = \text{ord}(s_m) = 2^j$, $j \leq k$. Em outras palavras, n é pseudoprimo forte na base a se e somente se $\text{ord}(a_{2,1}) = \dots = \text{ord}(a_{2,m}) = 2^j$, $j \leq k$, $\text{ord}(a_{b_1})|b, \dots, \text{ord}(a_{b_m})|b$, $\text{ord}(a_{p_1})|b, \dots, \text{ord}(a_{p_m})|b$. Devemos contar para quantos $a \in (\mathbb{Z}/(n))^*$ valem as condições acima.

Convem usar a linguagem de probabilidades: $\alpha(n)$ é a probabilidade de que n seja pseudoprimo forte na base a . Os eventos

$$\text{ord}(a_{b_1})|b, \dots, \text{ord}(a_{b_m})|b, \text{ord}(a_{p_1})|b, \dots, \text{ord}(a_{p_m})|b$$

são independentes e têm probabilidades

$$\text{mdc}(b, b_1)/b_1, \dots, \text{mdc}(b, b_m)/b_m, 1/p_1^{e_1-1}, \dots, 1/p_m^{e_m-1}$$

(note que $\text{mdc}(b, p_i) = 1$). Seja $k_{\min} = \min(k_1, \dots, k_m, k)$, $K = k_1 + \dots + k_m$. A probabilidade de que $\text{ord}(a_{2,1}) = \dots = \text{ord}(a_{2,m}) = 1$ é igual a 2^{-K} ; a probabilidade de que $\text{ord}(a_{2,1}) = \dots = \text{ord}(a_{2,m}) = 2^j$ é igual a $2^{-K+m(j-1)}$ se $0 < j \leq k_{\min}$; assim, a probabilidade de que $\text{ord}(a_{2,1}) = \dots = \text{ord}(a_{2,m})$ é igual a

$$\begin{aligned} 2^{-K}(1 + 1 + 2^m + 2^{(2m)} + \dots + 2^{((k_{\min}-1)m)}) &\leq 2^{-(m-1)} 2^{-(K-mk_{\min})} \\ &\leq 2^{-(m-1)}. \end{aligned}$$

Resumindo,

$$\alpha(n) \leq 2^{-(m-1)} 2^{-(K-mk_{\min})} \frac{\text{mdc}(b, b_1)}{b_1} \dots \frac{\text{mdc}(b, b_m)}{b_m} \frac{1}{p_1^{e_1-1}} \dots \frac{1}{p_m^{e_m-1}}.$$

Vamos agora considerar vários casos de n composto e verificar em quais deles vale $\alpha(n) \geq 1/4$.

Se $m = 1$ e $n = p_1^{e_1}$ então $\alpha(n) \leq 1/p_1^{(e_1-1)}$. O único caso em que esta estimativa não implica $\alpha < 1/4$ é para $n = 9$.

Se $m \geq 2$ e $e_i > 1$ temos $\alpha(n) \leq 1/(2p_i) < 1/4$; podemos portanto nos restringir ao caso em que n é livre de quadrados. Se $m \geq 4$ temos $\alpha(n) \leq 1/8$; podemos portanto nos restringir aos casos $n = p_1 p_2$ e $n = p_1 p_2 p_3$.

Se $n = p_1 p_2 p_3$ temos

$$\alpha(n) \leq \frac{1}{4} \frac{\text{mdc}(b, b_1)}{b_1} \frac{\text{mdc}(b, b_2)}{b_2} \frac{\text{mdc}(b, b_3)}{b_3};$$

temos portanto $\alpha(n) \leq 1/4$. Para que $\alpha(n) = 1/4$ devemos ter $k_1 = k_2 = k_3 = 1$ e $b_1|b$, $b_2|b$, $b_3|b$ donde $(p_1 - 1)|(n - 1)$, $(p_2 - 1)|(n - 1)$, $(p_3 - 1)|(n - 1)$ e $n = p_1 p_2 p_3$ é um número de Carmichael com $p_1 \equiv p_2 \equiv p_3 \equiv 3 \pmod{4}$.

Finalmente, considere $n = p_1 p_2$, $p_1 < p_2$. Observe que

$$\begin{aligned} \text{mdc}(p_1 - 1, n - 1) &= \text{mdc}(p_1 - 1, (p_1 - 1)p_2 + p_2 - 1) \\ &= \text{mdc}(p_1 - 1, p_2 - 1) \\ &= \text{mdc}(p_2 - 1, n - 1). \end{aligned}$$

Em particular, $(p_2 - 1)/\text{mdc}(p_2 - 1, n - 1) > 1$. Se existir um primo ímpar q com $q|(p_2 - 1)/\text{mdc}(p_2 - 1, n - 1)$ temos $\alpha(n) \leq 1/2q < 1/4$. Podemos portanto supor que $(p_2 - 1)/\text{mdc}(p_2 - 1, n - 1) = 2^{k_2 - k}$. Analogamente, podemos supor que $(p_1 - 1)/\text{mdc}(p_1 - 1, n - 1) = 2^{k_1 - k}$ e portanto que $k = k_1 < k_2$ donde $p_2 - 1 = 2^l(p_1 - 1)$, $l = k_2 - k_1 > 0$. Neste caso temos $\alpha(n) = 2^{-2k_1 - l}(1 + 1 + 4 + \dots + 4^{(k_1 - 1)}) = 1/2^l(1/4 + 1/16 + \dots + 1/4^{k_1} + 1/4^{k_1})$ que é menor ou igual a $1/4$, com igualdade apenas no caso $l = 1$, $k_1 = 1$ que equivale a $p_1 \equiv 3 \pmod{4}$, $p_2 = 2p_1 - 1$. \square

Os menores exemplos de números compostos n da primeira forma para a qual $\alpha(n) = 1/4$ são $n = 15 = 3 \cdot 5$, $n = 91 = 7 \cdot 13$ e $n = 703 = 19 \cdot 37$. O menor exemplo de número composto da segunda forma

é $n = 8911 = 7 \cdot 19 \cdot 67$. Sabe-se que existem menos do que $CN^{(1/2+\epsilon)}$ números compostos n destas formas menores do que N ; conjectura-se que o número de compostos n da primeira forma seja maior do que $CN^{(1/2-\epsilon)}$. Na maioria dos casos $\alpha(n)$ é muito menor.

O teorema acima serve de base para certos testes de primalidade *probabilísticos*, como o chamado o *algoritmo Miller-Rabin*, que agora descrevemos. Dado n , tomamos t valores de a ao acaso no intervalo $1 < a < n$ e verificamos para cada a se n passa no teste de primalidade na base a . Se n for ímpar composto, a probabilidade de que um dado a acuse a não-primalidade de a é maior do que $3/4$ (pelo teorema); assim, a probabilidade de que n escape a t testes é menor do que 4^{-t} .

Um problema relacionado é aquele em que escolhemos um inteiro ímpar com k bits ao acaso e aplicamos o teste de Miller-Rabin t vezes: se o inteiro falhar descartamos e sorteamos outro até obtermos um inteiro n que tenha passado em t testes. Queremos estimar a probabilidade $p_{k,t}$ de que n seja composto: a idéia é que esta probabilidade seja pequena e que possamos declarar que n é “provavelmente primo”(ver [47]). O teorema dos números primos nos diz que há pelo menos $C_1 2^k/k$ primos na faixa acima (onde C_1 é uma constante positiva). Como vimos no parágrafo anterior, a probabilidade de que um n composto passe por t testes é menor do que 4^{-t} . Podemos daí estimar que $p_{k,t} < C_2 k 4^{-t}$ (para algum $C_2 > 0$), o que já é bem pequeno. Na verdade, $p_{k,t}$ é muito menor do que este valor e tende a decrescer quando k cresce. Isto se deve ao fato de pseudoprimos serem muito mais raros do que primos e $\alpha(n)$ ser em geral muito menor do que $1/4$.

Este tipo de teste é extremamente útil em aplicações (como em criptografia) onde é importante criar primos relativamente grandes mas não existe a preocupação com demonstrações ou com perfeição absoluta. Trataremos de testes de primalidade determinísticos (i.e., que demonstram matematicamente a primalidade) na próxima seção.

Existe uma variação do conceito de pseudoprimalidade forte. Suponhamos que $n - 1 = p^k \cdot b$, $p \nmid b$. Seja a um inteiro, $0 < a < n$. O pequeno teorema de Fermat diz que se n é primo devemos ter $(a^b)^{p^k} \equiv 1 \pmod{n}$. Suponhamos que isto ocorra: nosso teste refinado consiste em considerar o último termo não côngruo a 1 módulo n da sequência $a^b, (a^b)^p, (a^b)^{p^2}, \dots, (a^b)^{p^k}$: chamemos este termo de c (se ocorrer $a^b \equiv 1 \pmod{n}$ não podemos aplicar o teste). Temos claramente $c^p - 1 = (c^{p-1} + \dots + c + 1)(c - 1) \equiv 0 \pmod{n}$ e $c - 1 \not\equiv 0 \pmod{n}$; se n for

primo devemos obrigatoriamente ter $c^{p-1} + \dots + c + 1 \equiv 0 \pmod{n}$. Em outras palavras, se $c^{p-1} + \dots + c + 1 \not\equiv 0 \pmod{n}$ sabemos que n é composto. Assim como no caso de pseudoprimos fortes, se n for pseudo-primo na base a mas falhar este teste para algum primo p acabamos de obter uma fatoração para n : $n = \text{mdc}(n, c-1) \cdot \text{mdc}(n, c^{p-1} + \dots + c + 1)$.

Em [144], Solovay e Strassen obtiveram um outro algoritmo probabilístico em tempo polinomial utilizando resíduos quadráticos. Desde então, vários algoritmos probabilísticos têm sido propostos.

7.4 Testes determinísticos

Nosso principal ponto de vista neste livro é o de um matemático: queremos não apenas um teste probabilístico mas uma demonstração da primalidade de n .

O teste de Miller-Rabin apresentado na seção anterior é uma variação probabilística, devida a Rabin ([121]), de um teste determinístico criado anteriormente por Miller que dependia de uma famosa generalização da hipótese de Riemann. Uma maneira de modificar o algoritmo de Miller-Rabin para torná-lo determinístico é testar todos os valores da base a em um intervalo suficientemente grande: essa generalização da hipótese de Riemann implica que o intervalo de 1 até $2(\log n)^2$ já é grande o bastante ([8]). Este algoritmo é rápido e geral, mas infelizmente depende de uma conjectura.

Um grande avanço ocorreu em 1983 com o trabalho de Adleman, Pomerance e Rumely [1], que obtiveram um algoritmo determinístico e incondicional em tempo sub-exponencial $(\log n)^{O(\log \log \log n)}$ (enquanto todos os outros algoritmos determinísticos e incondicionais anteriores requeriam tempo exponencial), apesar de ser muito menos eficiente que o algoritmo de Miller-Rabin. Em 1986, Goldwasser e Kilian [59] propuseram um algoritmo probabilístico baseado em curvas elípticas com tempo esperado polinomial em quase qualquer entrada (ou qualquer entrada assumindo uma hipótese que se acredita ser verdadeira) e que produz um certificado de primalidade (até então, todos os algoritmos probabilísticos produziam certificados apenas de que o número era composto). Adleman e Huang [2] modificaram o algoritmo de Goldwasser-Kilian obtendo um algoritmo probabilístico em tempo polinomial que sempre produz um certificado de primalidade.

Mas foi somente em agosto de 2002 que um grupo de pesquisadores

do Indian Institute of Technology, formado por um professor (Manindra Agrawal) e dois alunos de graduação (Neeraj Kayal e Nitin Saxena), provou que o problema de teste de primalidade pertence à classe \mathcal{P} ao obterem o primeiro algoritmo determinístico polinomial para tal problema: o algoritmo decide se N é ou não primo em tempo que é da ordem de um polinômio com relação ao número de bits $k = \log_2 N$ da entrada. Em particular o algoritmo não executa nenhuma escolha aleatória como fazem todos os algoritmos eficientes conhecidos até então. Esta descoberta deixou a comunidade de cientistas da área surpresos pelo fato de que, não apenas esse algoritmo resolve um problema de longa data, ele também o faz de uma maneira brilhantemente simples. Fica no ar a pergunta sobre o que mais tem sido deixado passar de forma semelhante.

A partir de então, esforços têm sido feitos para implementar o algoritmo de forma eficiente, acarretando no surgimento de diversas variantes, que agora são mencionados como pertencentes à classe AKS. Dentre essas variantes, pode-se destacar as de Lenstra [88], Pomerance [119], Berrizbeitia [16], Cheng [32], Bernstein [14] e Lenstra e Pomerance [89]. A tendência geral é a redução do expoente de complexidade k , cujo valor rigoroso é atualmente $k = 6 + \epsilon$, resultado obtido por [89], embora valores de até $k = 4 + \epsilon$ tenham sido obtidos para determinados valores de entrada, ou para qualquer valor de entrada assumindo hipóteses como a HGR e/ou heurísticas.

O algoritmo AKS será explicado mais tarde nesta seção.

7.4.1 Testes de Primalidade Baseados em Fatorações de $n - 1$

Veremos inicialmente alguns algoritmos determinísticos que funcionam para valores especiais de n , para os quais uma fatoração (talvez incompleta) de $n - 1$ é conhecida.

Proposição 7.15. *Seja $n > 1$. Se para cada fator primo q de $n - 1$ existe um inteiro a_q tal que $a_q^{n-1} \equiv 1 \pmod{n}$ e $a_q^{(n-1)/q} \not\equiv 1 \pmod{n}$ então n é primo.*

DEMONSTRAÇÃO: Seja q^{k_q} a maior potência de q que divide $n - 1$. A ordem de a_q em $(\mathbb{Z}/(n))^\times$ é um múltiplo de q^{k_q} , donde $\varphi(n)$ é um

múltiplo de q^{kq} . Como isto vale para todo fator primo q de $n - 1$, $\varphi(n)$ é um múltiplo de $n - 1$ e n é primo. \square

Proposição 7.16 (Pocklington). *Se $n - 1 = q^k R$ onde q é primo e existe um inteiro a tal que $a^{n-1} \equiv 1 \pmod{n}$ e $\text{mdc}(a^{(n-1)/q} - 1, n) = 1$ então qualquer fator primo de n é côngruo a 1 módulo q^k .*

DEMONSTRAÇÃO: Se p é um fator primo de n então $a^{n-1} \equiv 1 \pmod{p}$ e p não divide $a^{(n-1)/q} - 1$, donde $\text{ord}_p a$, a ordem de a módulo p , divide $n - 1$ mas não divide $(n - 1)/q$. Assim, $q^k \mid \text{ord}_p a \mid p - 1$, donde $p \equiv 1 \pmod{q^k}$. \square

Corolário 7.17. *Se $n - 1 = FR$, com $F > R$ e para todo fator primo q de F existe $a > 1$ tal que $a^{n-1} \equiv 1 \pmod{n}$ e $\text{mdc}(a^{(n-1)/q} - 1, n) = 1$ então n é primo.*

DEMONSTRAÇÃO: Seja q um fator primo de F e q^k a maior potência de q que divide F ; pela proposição anterior, todo fator primo de n deve ser côngruo a 1 módulo q^k . Como isto vale para qualquer fator primo de F , segue que qualquer fator primo de n deve ser côngruo a 1 módulo F . Como $F > \sqrt{n}$, isto implica que n é primo. \square

De fato, basta conhecer um conjunto de fatores primos cujo produto seja maior do que $(n - 1)^{1/3}$ para, usando o resultado de Pocklington, tentar demonstrar a primalidade de n (o que deixamos como exercício). Os seguintes critérios clássicos são consequências diretas das proposições acima.

Fermat conjecturou que todo número da forma $F_n = 2^{2^n} + 1$ fosse primo e verificou a conjectura para $n \leq 4$. Observe que $2^n + 1$ (e em geral $a^n + 1$ com $a \geq 2$) não é primo se n não é uma potência de 2: se p é um fator primo ímpar de n , podemos escrever $a^n + 1 = b^p + 1 = (b + 1)(b^{p-1} - b^{p-2} + \dots + b^2 - b + 1)$ onde $b = a^{n/p}$. Euler mostraria mais tarde que F_5 não é primo (temos $F_5 = 4294967297 = 641 \cdot 6700417$) e já se demonstrou que F_n é composto para vários outros valores de n ; nenhum outro primo da forma $F_n = 2^{2^n} + 1$ é conhecido. Até outubro de 2011 o menor número de Fermat que se desconhece se é primo ou composto é F_{33} , mas se conhecem muitos primos (alguns bastante grandes) da forma

$a^{2^n} + 1$, que são conhecidos como *primos de Fermat generalizados*. O teste a seguir mostra como testar eficientemente a primalidade de F_n .

Corolário 7.18 (Teste de Pépin). *Seja $F_n = 2^{2^n} + 1$; F_n é primo se, e somente se, $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

DEMONSTRAÇÃO: Se $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ então a primalidade de F_n segue da Proposição 7.15. Por outro lado, se F_n é primo então pelo critério de Euler e a lei de reciprocidade quadrática temos

$$3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1 \pmod{F_n}$$

□

Teorema 7.19 (Proth (1878)). *Seja $n = h \cdot 2^k + 1$ com $2^k > h$. Então n é primo se, e somente se, existe um inteiro a com $a^{(n-1)/2} \equiv -1 \pmod{n}$.*

DEMONSTRAÇÃO: Se n é primo, podemos tomar a qualquer com $\left(\frac{a}{n}\right) = -1$; ou seja, metade dos inteiros entre 1 e $n-1$ serve como a . A recíproca segue do corolário 7.17 com $F = 2^k$. □

Corolário 7.20. *Se $n = h \cdot q^k + 1$ com q primo e $q^k > h$. Então n é primo se, e somente se, existe um inteiro a com $a^{n-1} \equiv 1 \pmod{n}$ e $\text{mdc}(a^{(n-1)/q} - 1, n) = 1$.*

DEMONSTRAÇÃO: Se n é primo, podemos tomar a qualquer que não seja da forma x^q módulo n (que existe pois n admite raiz primitiva); ou seja, uma proporção de $(q-1)/q$ dentre inteiros entre 1 e $n-1$ serve como a . A recíproca segue do corolário 7.17 com $F = q^k$. □

Muitos dentre os maiores primos conhecidos estão nas condições do teorema de Proth (ver tabelas). Isto se deve ao fato de primos desta forma serem frequentes (mais frequentes do que, por exemplo, primos de Mersenne) e que sua primalidade é facilmente demonstrada usando este resultado.

7.4.2 Teste de Agrawal, Kayal e Saxena

Todos os algoritmos eficientes conhecidos até o momento, sejam determinísticos ou probabilísticos, baseiam-se no pequeno teorema de Fermat: um número p é um número primo se, e somente se, para todo número natural $1 \leq a < p$ temos que $a^{p-1} - 1$ é divisível por p , isto é,

$$p \text{ é primo} \iff a^{p-1} \equiv 1 \pmod{p} \text{ para todo } 1 \leq a < p.$$

Para a recíproca, basta observar que se p é composto, então a congruência acima é falsa para todo divisor a de p com $1 < a < p$.

No algoritmo AKS, o fundamento matemático de fato não é diferente: Suponhamos que x é uma variável, a um inteiro e p um número primo. Usando o binômio de Newton temos que

$$(x + a)^p = \sum_{j=0}^p \binom{p}{j} x^{p-j} a^j,$$

mas nos casos em que j é diferente de 1 e p , o coeficiente binomial $\binom{p}{j}$ é divisível por p , logo todos os termos intermediários desta expansão são divisíveis por p , assim

$$(x + a)^p \equiv x^p + a^p \equiv x^p + a \pmod{p}$$

onde na última igualdade usamos o teorema de Fermat. Reciprocamente, se $(x + a)^N \equiv x^N + a \pmod{N}$ para todo $a < N$, então tomando $a = 1$ vemos que N divide todos os coeficientes binomiais $\binom{N}{j}$ com $0 < j < N$. Se N fosse composto e q é um fator primo de N , então

$$\binom{N}{q} = \frac{N(N-1) \dots (N-q+1)}{q(q-1) \dots 1}.$$

Vemos que os únicos termos que são múltiplos de q nesta expressão são o N no numerador e o q no denominador, assim se q^k é a maior potência de q que divide N , temos que $q^k \nmid \binom{N}{q}$, logo $N \nmid \binom{N}{q}$, absurdo. Assim, N é primo. Desta forma obtemos o seguinte critério de primalidade:

$$N \text{ é primo} \iff (x + a)^N \equiv x^N + a \pmod{N}, \text{ para todo } a < N$$

$$\iff (x+a)^N \equiv x^N + a \pmod{N}, \text{ para algum } a < N, \text{ com } \text{mdc}(a, N) = 1.$$

Este critério, por enquanto, é ineficiente, porque temos que calcular todos os coeficientes de $(x + a)^N$ e mostrar que todos os coeficientes intermediários são divisíveis por N . Outra observação importante é que se os polinômios $(x+a)^N$ e $x^N + a$ são iguais módulo N , então eles deixam o mesmo resto módulo N quando divididos por qualquer polinômio. Em particular, se dividimos por $x^r - 1$ temos que

$$N \text{ é primo} \implies \begin{array}{l} (x+a)^N \equiv x^N + a \pmod{x^r - 1, N} \\ \text{para todo } a < N, r \in \mathbb{N} \end{array}$$

O fato importante, mostrado por Agrawal, Kayal e Saxena, é que para garantir a primalidade de N só precisamos testar que esta congruência é válida para um valor especial de r (na versão original um r primo para o qual $r - 1$ tem um fator primo $q \geq 4\sqrt{r} \log N$, o qual divide a ordem de n módulo r) que depende polinomialmente de $\log N$ e alguns poucos valores de a . Assim, na versão original do AKS [3] se mostra, usando um teorema não elementar devido a Fouvry (ver [54]), a existência de um tal r da ordem $O((\log_2 N)^6)$.

Mostraremos o seguinte resultado (o qual aparece na versão final [3] do artigo de Agrawal, Kayal e Saxena), que é uma simplificação do AKS obtida por H. Lenstra, no qual não é preciso usar o teorema de Fouvry.

Teorema 7.21 (Agrawal, Kayal, Saxena, Lenstra). *Sejam N , r e v inteiros maiores que 1, com r potência de primo. Seja S um conjunto finito com s elementos. Suponhamos que*

1. *N e r são primos relativos e a ordem de N módulo r é v , i.e., v é o mínimo tal que $N^v \equiv 1 \pmod{r}$.*
2. *$\text{mdc}(N, a - b) = 1$ para quaisquer elementos $a, b \in S$, $a \neq b$.*
3. *$\binom{s+t-1}{s} \geq N^{\sqrt{t/2}}$ para todo t divisor de $\varphi(r)$ que seja múltiplo de v .*
4. *$(x + a)^N \equiv x^N + a \pmod{x^r - 1, N}$ para todo $a \in S$.*

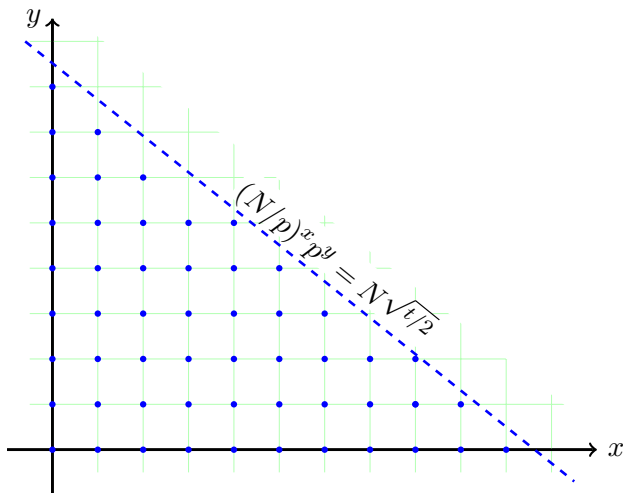
Então N é potência de um primo.

DEMONSTRAÇÃO: Pela condição 1, podemos escolher um divisor primo p de N tal que $\text{ord}_r p > 1$. Por hipótese, $(x + a)^N = x^N + a$ no anel $\mathbb{F}_p[x]/(x^r - 1)$ para todo $a \in S$ (aqui $\mathbb{F}_p = \mathbb{Z}/(p)$ denota o corpo com

p elementos). Substituindo x por x^{N^i} temos que $(x^{N^i} + a)^N = x^{N^{i+1}} + a$ no anel $\mathbb{F}_p[x]/(x^{rN^i} - 1)$ para todo $a \in S$, e logo também no anel $\mathbb{F}_p[x]/(x^r - 1)$. Assim, indutivamente obtemos que $(x + a)^{N^i} = x^{N^i} + a$ no anel $\mathbb{F}_p[x]/(x^r - 1)$ para todo $a \in S$. Pelo teorema de Fermat obtemos $(x + a)^{N^i p^j} = (x^{N^i} + a)^{p^j} = x^{N^i p^j} + a$ no anel $\mathbb{F}_p[x]/(x^r - 1)$ para todo $a \in S$. Daí segue que temos também $(x + a)^{(N/p)^i p^j} = x^{(N/p)^i p^j} + a$ no anel $\mathbb{F}_p[x]/(x^r - 1)$; de fato, elevando os dois lados a p^i temos igualdade, e elevar um polinômio em $\mathbb{F}_p[x]$ a p^i é uma função injetora.

Seja G o subgrupo multiplicativo de $(\mathbb{Z}/(r))^\times$ gerado pelas classes de congruência de N e de p módulo r , e seja $t = |G|$. Note que $t \mid \varphi(r)$ e que $v \mid t$ (pois G contém o grupo gerado pela classe de congruência módulo r de N em $\mathbb{Z}/(r)$, que, por definição, tem v elementos).

Mostraremos que existem mais do que t pares $i, j \geq 0$ tais que $(N/p)^i p^j \leq N^{\sqrt{t/2}}$. Considere o triângulo T formado pelos pontos (x, y) com $x, y \in \mathbb{R}, x, y, \geq 0$ tais que $(N/p)^x p^y \leq N^{\sqrt{t/2}}$. A área de T , que é $\frac{t \log^2(N)}{4 \log(N/p) \log p} \geq t$, é menor que o número de quadrados da forma $[i, i+1] \times [j, j+1]$ com $i, j \geq 0$ inteiros tais que $(N/p)^i p^j \leq N^{\sqrt{t/2}}$, pois esses quadrados cobrem T . Isso prova a nossa afirmação.



Como temos mais do que $|G|$ tais pares (i, j) e $G = \langle N, p \rangle_{(\text{mod } r)} = \langle N/p, p \rangle_{(\text{mod } r)}$, existem pares $(i, j) \neq (k, l)$ tais que $(N/p)^i p^j \equiv (N/p)^k p^l \pmod{r}$. Escrevendo $w = (N/p)^i p^j$ e $u = (N/p)^k p^l$ temos que $|w - u| <$

$N^{\sqrt{t/2}}$ e $x^w = x^u$ em $\mathbb{F}_p[x]/(x^r - 1)$, logo $(x + a)^w = x^w + a = x^u + a = (x + a)^u$ em $\mathbb{F}_p[x]/(x^r - 1)$.

Seja $r = q^d$, q primo. Seja $h(x)$ um polinômio irreduzível em $\mathbb{F}_p[x]$ que divide

$$x^{q^d - q^{d-1}} + x^{q^d - 2q^{d-1}} + \cdots + x^{2q^{d-1}} + x^{q^{d-1}} + 1 = \frac{x^{q^d} - 1}{x^{q^{d-1}} - 1}.$$

O corpo $K = \mathbb{F}_p[x]/(h(x))$ possui $p^{\deg h(x)}$ elementos, e em seu grupo multiplicativo x tem ordem $r = q^d$ pois $x^{q^{d-1}} = 1$ implica em $q = 0$ em \mathbb{F}_p , uma contradição. Assim, $r \mid p^{\deg h(x)} - 1$ pelo teorema de Lagrange e portanto $\text{ord}_r p \mid \deg h(x)$. Concluimos que $\deg h > 1$.

Seja \mathcal{G} o subgrupo de K^\times gerado pelos elementos $x + a$, $a \in S$. A condição 2 acima garante que os elementos $x + a$ são todos distintos em K . Dizemos que um polinômio $f \in \mathbb{F}_p[y]$ é *introspectivo* se valerem em $\mathbb{F}_p[y]$ as congruências $f(y^p) \equiv (f(y))^p \pmod{y^r - 1}$ e $f(y^{(N/p)}) \equiv (f(y))^{N/p} \pmod{y^r - 1}$. Como discutido acima, temos $f(y^m) \equiv (f(y))^m$ para todo $m \in G$, onde $G \subseteq (\mathbb{Z}/(r))^\times$ é gerado por N/p e p . O produto de polinômios introspectivos é introspectivo e já vimos que $y + a$ é introspectivo para $a \in S$. Considere os multi-índices $E = (e_a)_{a \in S}$, com $e_a \in \mathbb{N}$ para todo $a \in S$, satisfazendo $\sum_{a \in S} e_a \leq t - 1$; para cada tal E seja $P_E(y) = \prod_{a \in S} (y + a)^{e_a} \in \mathbb{F}_p[y]$; estes polinômios também são introspectivos. Pela fatoração única em irreduzíveis temos que os polinômios P_E são todos distintos: afirmamos que os elementos $P_E(x) \in K$ também são todos distintos. De fato, suponha $P_{E_1}(x) = P_{E_2}(x)$; seja $H(y) = P_{E_1}(y) - P_{E_2}(y) \in \mathbb{F}_p[y] \subset K[y]$: o grau de H é menor do que t e para $m \in G$ temos $H(x^m) = P_{E_1}(x^m) - P_{E_2}(x^m) = (P_{E_1}(x))^m - (P_{E_2}(x))^m = 0$ e portanto H tem t raízes distintas em K , logo $H = 0$ e $E_1 = E_2$. Assim, \mathcal{G} tem no mínimo $\binom{s+t-1}{s} \geq N^{\sqrt{t/2}} > |w - u|$ elementos. Por outro lado, já vimos que para todo $g \in \mathcal{G}$ temos que $g^w = g^u$, mas se $w \neq u$ esta equação pode ter no máximo $|w - u|$ soluções não nulas num corpo. Logo $w = u$, isto é, $(N/p)^i p^j = (N/p)^k p^l$, mas $i = k \implies j = l$, e como (i, j) e (k, l) são diferentes, temos $i \neq k$ e portanto de $(N/p)^i p^j = (N/p)^k p^l$ concluimos que N tem que ser uma potência de p . \square

Note que se a condição 2 é falsa, significa que foi encontrado um fator de N , que portanto não seria primo.

Observemos que, se $v > \frac{1}{2}(\log_2 N)^2$, tomando $S = \{0, 1, \dots, \ell\}$, onde $\ell := \lfloor \sqrt{\varphi(r)/2} \log_2 N \rfloor$ elementos, temos que r e s satisfazem a condição 3 do teorema. De fato, tomando $\tilde{\ell} := \lfloor \sqrt{t/2} \log_2 N \rfloor \leq \ell$, temos

$$\begin{aligned} \binom{s+t-1}{s} &= \binom{\ell+t}{t-1} \geq \binom{\tilde{\ell}+t}{t-1} = \binom{\tilde{\ell}+t}{\tilde{\ell}+1} \\ &\geq \binom{2\tilde{\ell}+1}{\tilde{\ell}+1} > 2^{\tilde{\ell}+1} \\ &> N^{\sqrt{t/2}}. \end{aligned}$$

Note que, como $t \geq v > \frac{1}{2}(\log_2 N)^2$, temos $\tilde{\ell} = \lfloor \sqrt{t/2} \log_2 N \rfloor < t$.

Lema 7.22. *Seja $N \geq 9$ um inteiro. Existe uma potência de primo r menor do que $(\log_2 N)^5$ tal que $v = \text{ord}_r N > \frac{1}{2}(\log_2 N)^2$.*

DEMONSTRAÇÃO: Considere o número

$$M = N^{\lfloor 5 \log_2 \log_2 N \rfloor} (N-1)(N^2-1) \cdots (N^{\lfloor \frac{\log_2^2 N}{2} \rfloor} - 1)$$

e tome r como o menor número que não divide M . Note que r é uma potência de primo. Temos

$$M < N^{(5 \log_2 \log_2 N + 1 + 2 + \cdots + \lfloor \frac{\log_2^2 N}{2} \rfloor)} < 2^{\frac{\log_2^5 N}{2}}.$$

Pelo corolário 5.14, sabemos que, para todo $k \geq 2$, o mínimo múltiplo comum dos números menores que $2k$ é maior que 2^k . Portanto $r < (\log_2 N)^5$. Temos $\text{mdc}(r, N) = 1$, pois, se r é uma potência de um primo que divide N , o expoente deve ser maior que $5 \log_2 \log_2 N$ (senão r dividiria M), e então $r > 2^{5 \log_2 \log_2 N} = (\log_2 N)^5$, absurdo. Como r não divide $N^j - 1$ para todo j com $1 \leq j \leq \lfloor \frac{\log_2^2 N}{2} \rfloor$, temos $\text{ord}_r N > \frac{1}{2}(\log_2 N)^2$. \square

O pseudo-código associado a este teorema com estas escolhas de r e S fica da seguinte forma.

Algoritmo AKSL

1. Entrada $N > 6$.
2. Se $N = a^b$ com $b > 1$, retorna COMPOSTO.
3. Encontrar o menor r tal que $\text{ord}_r N > \frac{1}{2}(\log_2 N)^2$.
4. Se $\text{mdc}(a, N) > 1$ para algum primo $a \leq r$, retorna COMPOSTO.
5. Se $\sqrt{N} < r$, retorna PRIMO.
6. Para $a = 1$ até $\lfloor \sqrt{\varphi(r)/2 \log_2 N} \rfloor$ faça
 Se $(x+a)^N \not\equiv x^N + a \pmod{x^r - 1, N}$, retorna COMPOSTO;
7. Retorna PRIMO.

Observação 7.23. Em relação ao passo 3, o lema anterior garante que, para todo $N \geq 9$, encontraremos um inteiro positivo r menor do que $(\log_2 N)^5$ com $\text{mdc}(r, N) = 1$ tal que $\text{ord}_r N > \frac{1}{2}(\log_2 N)^2$. Pode ser que antes disso encontremos um divisor primo próprio de n , e nesse caso podemos encerrar a busca e retornar COMPOSTO.

Implementação e Complexidade

Nesta seção mostraremos uma possível implementação de cada passo do algoritmo anterior, assim como analisaremos a complexidade de cada passo. No que segue $\tilde{O}(k^n)$ significa $O(k^n P(\log k))$, onde P é um polinômio. Observe que para todo $\epsilon > 0$, $\tilde{O}(k^n) < O(k^{n+\epsilon})$.

Determinar se $N = a^b$

Observemos que se N é uma potência perfeita, isto é $N = a^b$ com $b > 2$, como $a \geq 2$ então $N = a^b \geq 2^b$, portanto $b \leq \log N$, o que gera o seguinte algoritmo que retorna 1 caso seja potência perfeita e 0 caso contrário.

Algoritmo PotenciaPerfeita

Entrada N

1. Para $b = 2$ até $\log N$ faça {
2. $S \leftarrow \lfloor N^{1/b} \rfloor$
3. Se $S^b = N$ retorna 1}
4. Retorna 0.

Existem várias formas de implementar o passo 2. Uma das mas simples é usando o método de Newton encontrado em qualquer livro de Cál-

culo elementar: “a sequência $\{x_n\}$ definida recorrentemente por $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ converge para uma raiz de $f(x) = 0$ para todo ponto inicial suficientemente próximo dessa raiz”, além disso a velocidade de convergência é quadrática. Em nosso caso $f(x) = x^b - N$, e nosso ponto inicial é um valor à direita da raiz. Dado que estamos interessados somente em raízes inteiras, o algoritmo fica da seguinte forma:

Algoritmo RaizInteira

Entrada N, b

1. $P = 2^{\lceil B(N)/b \rceil}$ // aqui $B(N)$ denota o número de bits de N

2. Faça{

3. $Q \leftarrow \left\lfloor \frac{(b-1)P + \lfloor N/P^{b-1} \rfloor}{b} \right\rfloor$

4. Se $Q \geq P$ retorne P

5. $P \leftarrow Q$ }

Dada que a convergência do método de Newton é quadrática, em cada passo do loop obtemos o dobro de dígitos (em base dois) significativos, e no segundo passo já temos no mínimo um dígito significativo. Isso significa que tal loop se repete no máximo $\log(\lceil B(N)/b \rceil) = O(\log(\log N))$ vezes para obter a raiz. Dado que para calcular A^B preciso no máximo de $2 \log B$ multiplicações e uma divisão inteira tem complexidade equivalente à multiplicação, o algoritmo anterior tem complexidade $O(\log N \log \log N)$. Portanto podemos determinar se um número N é potência perfeita com complexidade $O((\log N)^2 \log \log N)$ no número de multiplicações de inteiros com no máximo $\log N$ dígitos. Como a multiplicação de inteiros com k bits, tem complexidade (k^2) usando o método clássico, ou $(k \log k)$ usando Transformada Rápida de Fourier (FFT), temos que a complexidade de determinar se um número é raiz perfeita é $O((\log N)^3 (\log \log N)^2) = \tilde{O}((\log N)^3)$. Este valor está longe do ótimo. De fato, em [15], Bernstein mostra um algoritmo não elementar, usando aritmética de ponto flutuante, mas com complexidade

$$\log N \exp(O(\sqrt{\log \log N \log \log \log N})) = \tilde{O}(\log N),$$

isto é, quase linear.

Ordem N módulo r

O seguinte é um algoritmo simples para determinar a ordem de N módulo r , que verifica passo a passo qual é o menor inteiro j tal que

$$N^j \equiv 1 \pmod{r}.$$

Algoritmo Ordemmódulo

Entrada N, r

1. Se $\text{mdc}(N, r) \neq 1$ retorna -1 .
2. $A \leftarrow N \pmod{r}$
3. $B \leftarrow A$
4. $i \leftarrow 1$
5. Enquanto $B \neq 1$ faça{
 6. $B \leftarrow A \cdot B \pmod{r}$
 7. $i \leftarrow i + 1$
8. Retorna i

Pelo teorema de Euler-Fermat sabemos que a ordem de N módulo r é um divisor de $\varphi(r) < r$, assim o passo 5 se repete no máximo r vezes. No passo 6 temos que fazer um produto de números com $\log r$ dígitos e reduzir módulo r , logo a complexidade do algoritmo **Ordemmódulo** usando FFT para multiplicar é $O(r \log r \log \log r) = \tilde{O}(r)$. Assim como no passo 3 do algoritmo **AKSL** testamos todos os valores desde $\frac{1}{2}(\log N)^2$ até o menor r que cumpre a condição. Temos que a complexidade é no máximo $O(r^2 \log r \log \log r) = \tilde{O}(r^2)$ para determinar r , que mostramos ser menor do que $(\log_2 N)^5$.

Cálculo de MDC

O seguinte algoritmo é clássico, e está baseado no algoritmo de Euclides do capítulo 1: “seja r o resto ao dividir A por B , então $\text{mdc}(A, B) = \text{mdc}(B, r)$ ”. Usando iterativamente este algoritmo até obter resto 0, obtemos o seguinte algoritmo.

Algoritmo MDC

Entrada A, B

1. $R \leftarrow A - B \lfloor \frac{A}{B} \rfloor$
2. Enquanto $R \neq 0$ faça {
 3. $A \leftarrow B$
 4. $B \leftarrow R$
 5. $R \leftarrow A - B \lfloor \frac{A}{B} \rfloor$
6. Retorna B .

É fácil provar que o ciclo do algoritmo tem no máximo $\log_\phi \min\{A, B\}$ passos, onde $\phi = \frac{1+\sqrt{5}}{2}$ é a razão áurea, e este número é obtido exata-

mente quando tomamos dois termos consecutivos da sequência de Fibonacci (ver por exemplo [113]), assim a complexidade do passo 4 do algoritmo **AKSL** é $O(r \log r)$ em número de multiplicações de números com $\log r$ dígitos, logo a complexidade usando FFT para multiplicar é

$$O(r(\log r)^2 \log \log r) = \tilde{O}(r).$$

Cálculo de $(x + a)^N$ módulo $(x^r - 1, N)$

Este passo é, de fato, o mais complicado de implementar e também tem a maior complexidade algorítmica, que ilustramos no seguinte algoritmo.

Algoritmo PotenciaPolinomio

Entrada N, a, r onde $N = b_l b_{l-1} \dots b_0$ em base 2

1. $P[x] \leftarrow 1$
2. Para $i = l$ até 0 faça{
 3. $P[x] \leftarrow P[x]^2$
 4. Se $b_i = 1$ faça
 5. $P[x] \leftarrow P[x] \cdot (x + a)$.
 6. $P[x] \leftarrow P[x] \pmod{x^r - 1, N}$
7. Retorna $P[x]$

Como estamos interessados em polinômios módulo $(x^r - 1, N)$ cada polinômio pode ser implementado como um vetor com r entradas menores do que N . Assim, se $P(x)$ é um polinômio de grau menor ou igual a $r - 1$ então $(P(x))^2$ é um polinômio de grau menor ou igual $2r - 2$, isto é, $(P(x))^2 = \sum_{j=0}^{2r-2} a_j x^j$. Observemos que

$$(P(x))^2 = \sum_{j=0}^{r-1} (a_j + a_{j+r}) x^j + (x^r - 1) \sum_{j=0}^{r-1} a_{j+r} x^j$$

logo $(P(x))^2 \equiv \sum_{j=0}^{r-1} (a_j + a_{j+r}) x^j \pmod{x^r - 1}$, assim aplicar módulo $x^r - 1$ é uma operação com complexidade linear com relação a r . Agora, a multiplicação de polinômios de grau r pode ser feita usando o método clássico com r^2 multiplicações e r somas, ou $r \log r$ multiplicações usando FFT, onde estamos multiplicando números com $\log N$ bits. Assim a complexidade dos passos 3, 4, 5 e 6 do algoritmo é $O(r \log r \log N \log \log N) = \tilde{O}(r \log N)$ e, portanto, a complexidade do

algoritmo **PotenciaPolinomio** é $O(r \log r (\log N)^2 \log \log N) = \tilde{O}(r (\log N)^2)$.

Com isto concluímos que a complexidade do passo 6 do algoritmo **AKSL** é

$$O(r^{3/2} \log r (\log N)^3 \log \log N) = \tilde{O}(r^{3/2} (\log N)^3).$$

Dado que a complexidade máxima do algoritmo **AKSL** ocorre no passo 6 temos que a complexidade do algoritmo é $\tilde{O}(r^{3/2} (\log N)^3) = \tilde{O}((\log N)^{21/2})$.

conjectura-se que na verdade $r = O((\log N)^2)$. Se esta conjectura estiver correta, a complexidade do algoritmo fica igual a $\tilde{O}((\log N)^6)$. Esta conjectura seguiria, por exemplo, da conjectura 7.3 (no caso particular de primos de Sophie Germain). De fato, se valer essa conjectura, teríamos, entre $\log^2 N$ e $2 \log^2 N$ (estritamente), da ordem de $\frac{C \log^2 N}{2(\log \log N)^2} \gg \log N$ primos q tais que $2q + 1$ também é primo. Para um tal primo q , temos que $\text{ord}_{2q+1}(N) \leq 2$ ou $\text{ord}_{2q+1}(N) \geq q > \log^2 N$. Como $\text{ord}_{2q+1}(N) \leq 2 \implies 2q+1 \mid N^2 - 1$, o número de tais primos $2q+1$ é $O(\log N) \ll \frac{C \log^2 N}{2(\log \log N)^2}$, e portanto existe um primo $r = O(\log^2 N)$ com $\text{ord}_r(N) > \log^2 N$ (r será um dos primos da forma $2q + 1$ que consideramos acima, para o qual $\text{ord}_{2q+1}(N) \geq q > \log^2 N$).

Posteriormente ao trabalho original de Agrawal, Kayal e Saxena, Lenstra e Pomerance obtiveram um algoritmo inspirado nas idéias do AKS que trabalha com polinômios mais gerais e tem complexidade $\tilde{O}((\log N)^6)$ (ver [89]).

O algoritmo AKS é interessante do ponto de vista teórico, já que mostrou que o problema de determinar a primalidade de um número está na classe P , mas na prática o tempo de processamento é muito inferior com relação aos algoritmos probabilísticos clássicos, tais como Miller-Rabin e Solovay-Strassen, que são altamente eficientes e amplamente usados nos métodos de criptografia. De fato, escolhendo aleatoriamente 20 primos que validam os testes, temos que a probabilidade do número escolhido não ser primo é menor do que $9 \cdot 10^{-13}$. Por outro lado, caso a Hipótese de Riemann Generalizada seja verdadeira, o teste de Miller-Rabin torna-se um teste determinístico, mas esta conjectura ainda está em aberto. Ela é uma generalização da Hipótese de Riemann clássica (cujo enunciado, em duas versões equivalentes, já foi apresentado nas seções 4.2 e 6.1.2), que é considerada um dos problemas mais difíceis e importantes da Matemática.

Vários dos resultados desta seção e diversos outros aspectos algorítmicos e computacionais de números primos são apresentados na referência [44].

7.5 Primos de Mersenne

Em abril de 2010, os nove maiores primos conhecidos são da forma $M_p = 2^p - 1$ para $p = 43112609, 42643801, 37156667, 32582657, 30402457, 25964951, 24036583, 20996011, 13466917$. Estes são os únicos primos conhecidos com mais de 4000000 de dígitos.

Primos da forma $2^p - 1$, com p primo, têm sido estudados há séculos e são conhecidos como *primos de Mersenne*; não é difícil demonstrar que $2^p - 1$ só pode ser primo quando p é primo. Parte do interesse em primos de Mersenne deve-se à sua estreita ligação com números perfeitos. Um número perfeito é um inteiro positivo que é igual à soma de seus divisores próprios (como $6 = 1 + 2 + 3$ e $28 = 1 + 2 + 4 + 7 + 14$); os números perfeitos pares são precisamente os números da forma $2^{p-1}(2^p - 1)$ onde $2^p - 1$ é primo (um primo de Mersenne).

Talvez o primeiro resultado não trivial sobre primos de Mersenne seja devido a Hudalricus Regius que em 1536 mostrou que $2^p - 1$ não precisa ser primo sempre que p for primo: $2^{11} - 1 = 2047 = 23 \cdot 89$. Em 1603, Pietro Cataldi tinha corretamente verificado a primalidade de $2^{17} - 1$ e $2^{19} - 1$ e afirmou (incorretamente) que $2^p - 1$ também era primo para $p = 23, 29, 31$ e 37 . Em 1640, Fermat mostrou que $2^{23} - 1$ e $2^{37} - 1$ são compostos. Em 1644, o monge Marin Mersenne (1588-1648) afirmou por sua vez (também incorretamente) que $2^p - 1$ era primo para

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ e } 257$$

e composto para os demais valores de $p \leq 257$. Esta afirmação demoraria séculos para ser completamente corrigida.

Em 1738, Euler mostrou que $2^{29} - 1$ é composto e em 1750, verificou que $2^{31} - 1$ é primo. Lucas desenvolveu um algoritmo para testar a primalidade de números de Mersenne e em 1876 verificou que $2^{127} - 1$ é primo; este número permaneceria por muito tempo como o maior primo conhecido (ver [94]). Só em 1947 a lista dos primos até 257 foi varrida: os valores de p nesta faixa para os quais $2^p - 1$ é primo são

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ e } 127.$$

O algoritmo de Lucas foi posteriormente melhorado por Lehmer para dar o seguinte critério: sejam $S_0 = 4$, $S_1 = 4^2 - 2 = 14$, \dots , $S_{k+1} = S_k^2 - 2$; dado $p > 2$, $2^p - 1$ é primo se e somente se S_{p-2} é múltiplo de $2^p - 1$. Esta sequência cresce muito rápido, mas basta fazer as contas módulo $2^p - 1$: temos assim o chamado critério de Lucas-Lehmer (ver [86]).

Em 1951, computadores eletrônicos começaram a ser usados para procurar grandes números primos. Desde então foram encontrados os seguintes valores de p para os quais M_p é primo:

521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937,
 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433,
 1257787, 1398269, 2976221, 3021377, 6972593, 13466917,
 20996011, 24036583, 25964951, 30402457, 32582657,
 37156667, 42643801, 43112609, 57885161.

Em todos os casos foi usado o critério de Lucas-Lehmer. Os últimos doze foram encontrados com a ajuda de computadores pessoais: se você tem um computador você também pode participar da busca do próximo número de Mersenne (veja as instruções em www.mersenne.org).

Note que um número de Mersenne M_p é escrito na base 2 como 111...111, com p dígitos. Uma generalização natural seriam os números escritos como 111...111 em outra base, isto é, números da forma $(B^p - 1)/(B - 1)$, onde B é a base. É fácil ver que um tal número só pode ser primo se p for primo. No caso $B = 10$ estes números são conhecidos como *repunits*. Não se conhece um critério análogo ao de Lucas-Lehmer para testar a primalidade de números deste tipo quando $B > 2$. O maior primo conhecido desta forma é $(28839^{8317} - 1)/28838$, que tem 37090 dígitos. Os únicos repunits (comprovadamente) primos conhecidos são para $p = 2, 19, 23, 317, 1031$. Recentemente (entre 1999 e 2007), foram descobertos os seguintes valores de p para os quais os repunits correspondentes são *provavelmente* primos, i.e., passam por diversos testes probabilísticos de primalidade: 49081, 86453, 109297 e 270343. De acordo com os testes já realizados, qualquer outro repunit primo deve ter mais de 400000 dígitos.

Um número de Mersenne é um número da forma $M_p = 2^p - 1$. Os maiores números primos conhecidos atualmente são primos de Mersenne. Uma tabela contendo os recordes atuais encontra-se no final deste capítulo. O critério de Lucas-Lehmer, que apresentaremos nesta seção, é um

dos fatores para que isso ocorra pois fornece um teste de primalidade bastante rápido para números de Mersenne. Vejamos primeiramente que $2^p - 1$ só tem chance de ser primo quando p é primo.

Proposição 7.24. *Se $2^n - 1$ é primo então n é primo.*

DEMONSTRAÇÃO: Se $n = ab$ com $a, b \geq 2$ então $1 < 2^a - 1 < 2^n - 1$ e $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$ e $2^n - 1$ é composto. \square

Por outro lado, não se sabe demonstrar nem que existam infinitos primos de Mersenne nem que existem infinitos primos p para os quais M_p é composto. conjectura-se, entretanto, que existam infinitos primos p para os quais M_p é primo e que, se p_n é o n -ésimo primo deste tipo, temos

$$0 < A < \frac{\log p_n}{n} < B < +\infty$$

para constantes A e B . Existem algumas conjecturas mais precisas quanto ao valor de

$$\lim_{n \rightarrow \infty} \sqrt[n]{p_n};$$

Eberhart conjectura que este limite exista e seja igual a $3/2$; Wagstaff por outro lado conjectura que o limite seja

$$2^{e^{-\gamma}} \approx 1,4757613971$$

onde γ é a já mencionada constante de Euler-Mascheroni.

Primos de Mersenne são interessantes também por causa de *números perfeitos*. Um inteiro positivo n é dito *perfeito* se $\sigma(n) = 2n$, onde $\sigma(n)$ é a soma dos divisores de n . Os primeiros números perfeitos são 6, 28 e 496. Nosso próximo resultado caracteriza os números perfeitos pares.

Proposição 7.25. *Se M_p é um primo de Mersenne então $2^{p-1}M_p$ é perfeito. Além disso, todo número perfeito par é da forma $2^{p-1}M_p$ para algum primo p , sendo M_p um primo de Mersenne.*

DEMONSTRAÇÃO: Se M_p é primo então

$$\sigma(2^{p-1}M_p) = \sigma(2^{p-1}) \cdot \sigma(M_p) = (2^p - 1)(M_p + 1) = 2 \cdot 2^{p-1}M_p.$$

Por outro lado seja $n = 2^k b$, com $k > 0$ e b ímpar, um número perfeito par. Temos $\sigma(n) = 2n = \sigma(2^k)\sigma(b)$ donde $2^{k+1}b = (2^{k+1} - 1)\sigma(b)$. Como $\text{mdc}(2^{k+1} - 1, 2^{k+1}) = 1$, temos $b = (2^{k+1} - 1)c$ para algum inteiro c e assim $\sigma(b) = 2^{k+1}c$. Mas $1, 2^{k+1} - 1, c, b$ são divisores de $b = (2^{k+1} - 1)c$; se $c > 1$ então $\sigma(b) = 2^{k+1}c \geq 1 + 2^{k+1} - 1 + b$, o que implica $c \geq 2^{k+1}$, mas neste caso $\sigma(b) = 2^{k+1}c \geq 1 + 2^{k+1} - 1 + b + c$, um absurdo. Logo $c = 1$ e $b = 2^{k+1} - 1$ é primo pois $\sigma(b) = 2^{k+1}$. Pela proposição 7.24, $p = k + 1$ é primo, $b = M_p$ e $n = 2^{p-1}M_p$. \square

Por outro lado, um dos problemas em aberto mais antigos da Matemática é o da existência de números perfeitos ímpares. Sabe-se apenas que um número perfeito ímpar, se existir, deve ser muito grande (mais de 300 dígitos) e satisfazer simultaneamente várias condições complicadas.

Conjetura 7.26. *Não existe nenhum número perfeito ímpar.*

Nosso próximo resultado é o critério de Lucas-Lehmer, a base dos algoritmos que testam para grandes valores de p se $2^p - 1$ é ou não primo:

Teorema 7.27. *Seja S_k a sequência definida por $S_0 = 4$, $S_{k+1} = S_k^2 - 2$ para todo natural k . Seja $n > 2$; $M_n = 2^n - 1$ é primo se, e somente se, S_{n-2} é múltiplo de M_n .*

DEMONSTRAÇÃO: Observemos inicialmente que

$$S_n = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$$

para todo natural n . A demonstração por indução é simples: claramente $S_0 = 4 = (2 + \sqrt{3})^{2^0} + (2 - \sqrt{3})^{2^0}$ e

$$\begin{aligned} S_{k+1} &= S_k^2 - 2 = ((2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k})^2 - 2 \\ &= ((2 + \sqrt{3})^{2^k})^2 + 2 \cdot (2 + \sqrt{3})^{2^k} \cdot (2 - \sqrt{3})^{2^k} + ((2 - \sqrt{3})^{2^k})^2 - 2 \\ &= (2 + \sqrt{3})^{2^{k+1}} + (2 - \sqrt{3})^{2^{k+1}}. \end{aligned}$$

Suponha por absurdo que $M_n \mid (2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}}$ e que M_n seja composto, com um fator primo q com $q^2 \leq M_n$. Teremos $(2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}} \equiv 0 \pmod{q}$ donde, no grupo multiplicativo

$G = (\mathbb{Z}[\sqrt{3}]/(q))^\times$, temos $(2 + \sqrt{3})^{2^{n-2}} = -(2 - \sqrt{3})^{2^{n-2}}$. Como $2 - \sqrt{3} = (2 + \sqrt{3})^{-1}$ esta equação pode ser reescrita como $(2 + \sqrt{3})^{2^{n-1}} = -1$ (ainda em G), o que significa que a ordem de $2 + \sqrt{3}$ em G é exatamente 2^n . Isto é um absurdo, pois o número de elementos de G é no máximo $q^2 - 1 < 2^n$. Fica portanto demonstrado que se S_{n-2} é múltiplo de M_n então M_n é primo.

Suponha agora M_n primo, $n > 2$. Lembramos que neste caso n é primo. Basta provar que, em $\mathbb{Z}[\sqrt{3}]$, M_n divide $S_{n-2} = (2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}}$, pois neste caso S_{n-2}/M_n será um inteiro algébrico racional, portanto inteiro pelo lema 6.40. Assim, devemos mostrar que

$$\begin{aligned} (2 + \sqrt{3})^{2^{n-2}} &\equiv -(2 - \sqrt{3})^{2^{n-2}} \pmod{M_n} \\ \iff (2 + \sqrt{3})^{2^{n-1}} &\equiv -1 \pmod{M_n} \end{aligned}$$

utilizando novamente o fato que $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$. Note ainda que $2 + \sqrt{3} = (1 + \sqrt{3})^2/2$ e que 2 é invertível módulo M_n , logo temos que provar que

$$(1 + \sqrt{3})^{M_n+1} \equiv -2^{2^{n-1}} \pmod{M_n}$$

Como M_n é primo, temos

$$\begin{aligned} (1 + \sqrt{3})^{M_n} &\equiv 1 + (\sqrt{3})^{M_n} \equiv 1 + 3^{(M_n-1)/2} \sqrt{3} \\ &\equiv 1 + \left(\frac{3}{M_n}\right) \sqrt{3} \equiv 1 - \sqrt{3} \pmod{M_n} \end{aligned}$$

já que por reciprocidade quadrática temos $\left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = -\left(\frac{-2}{3}\right) = -1$. Substituindo na expressão acima, devemos agora provar que

$$(1 - \sqrt{3})(1 + \sqrt{3}) \equiv -2^{2^{n-1}} \pmod{M_n} \iff 2^{2^{n-1}-1} \equiv 1 \pmod{M_n}$$

Como n é primo, $2^{n-1} - 1$ é um múltiplo de n pelo pequeno teorema de Fermat. Porém, como $2^n \equiv 1 \pmod{M_n}$, isto implica que $2^{2^{n-1}-1} \equiv 1 \pmod{M_n}$ também, o que encerra a prova. \square

Mesmo quando M_p não é primo, podemos garantir que seus fatores primos serão de certas formas especiais. Isto é muito útil quando procuramos primos de Mersenne pois podemos eliminar alguns expoentes encontrando fatores primos de M_p . Isto também pode ser útil para conjecturarmos quanto à “probabilidade” de M_p ser primo, ou, mais precisamente, quanto à distribuição dos primos de Mersenne.

Proposição 7.28. *Sejam $p > 2$ e q primos com q um divisor de M_p . Então $q \equiv 1 \pmod{p}$ e $q \equiv \pm 1 \pmod{8}$.*

DEMONSTRAÇÃO: Se q divide M_p então $2^p \equiv 1 \pmod{q}$, o que significa que a ordem de 2 módulo q é p (pois p é primo). Isto significa que p é um divisor de $q - 1$, ou seja, que $q \equiv 1 \pmod{p}$. Por outro lado, $2 \equiv 2^{p+1} = (2^{(p+1)/2})^2 \pmod{q}$, donde $(\frac{2}{q}) = 1$, o que significa que $q \equiv \pm 1 \pmod{8}$. \square

Os vários valores de p para os quais a primalidade de M_p foi testada sugerem que para a ampla maioria dos valores de p , M_p não é primo. Isto é apenas uma conjectura: não se sabe demonstrar sequer que existem infinitos primos p para os quais M_p seja composto. Vamos agora ver uma proposição que serve para garantir que para certos valores especiais de p , alguns muito grandes, M_p não é primo.

Proposição 7.29. *Seja p primo, $p \equiv 3 \pmod{4}$. Então $2p + 1$ é primo (i.e. p é primo de Sophie Germain) se, e somente se, $2p + 1$ divide M_p .*

DEMONSTRAÇÃO: Se $q = 2p + 1$ é primo então $M_p = 2^p - 1 = 2^{(q-1)/2} - 1 \equiv (\frac{2}{q}) - 1 \pmod{q}$. Mas $p \equiv 3 \pmod{4}$ significa que $q \equiv 7 \pmod{8}$, donde $(\frac{2}{q}) = 1$. Assim, $M_p \equiv 0 \pmod{q}$, o que demonstra uma das implicações da proposição.

Por outro lado, se $2p + 1$ não é primo, ele tem fatores primos r com $r \not\equiv 1 \pmod{p}$ (pois $r < p$). Se $2p + 1$ dividisse M_p , r seria um fator primo de M_p , contrariando a proposição anterior. \square

7.6 Sequências Recorrentes e Testes de Primalidade

Nesta seção veremos aplicações de certas sequências recorrentes lineares a testes de primalidade. Para uma exposição mais geral sobre sequências recorrentes lineares, veja o Apêndice B.

Suponha dados inteiros $n > 1$, P e Q tais que $D = P^2 - 4Q$ não é um quadrado módulo n . Seja

$$\alpha = \frac{P + \sqrt{D}}{2},$$

raiz da equação $X^2 - PX + Q = 0$. É fácil provar por indução que

$$\alpha^m = \frac{V_m + U_m \sqrt{D}}{2}$$

para todo natural m onde U_m e V_m são definidos recursivamente por

$$\begin{aligned} U_0 &= 0, & U_1 &= 1, & U_{m+2} &= PU_{m+1} - QU_m, \\ V_0 &= 2, & V_1 &= P, & V_{m+2} &= PV_{m+1} - QV_m. \end{aligned}$$

Tais sequências são denominadas *sequências de Lucas*. Se

$$\bar{\alpha} = \frac{P - \sqrt{D}}{2}$$

é a segunda raiz da equação $X^2 - PX + Q = 0$, podemos também escrever

$$U_m = \frac{\alpha^m - \bar{\alpha}^m}{\sqrt{D}}, \quad V_m = \alpha^m + \bar{\alpha}^m,$$

como se demonstra facilmente por indução. Segue destas fórmulas que

$$U_{m+1} = \frac{PU_m + V_m}{2}, \quad V_{m+1} = \frac{DU_m + PV_m}{2}$$

e

$$U_{2m} = U_m V_m, \quad V_{2m} = V_m^2 - 2Q^m.$$

Estas fórmulas nos permitem calcular U_m e V_m módulo n em $C \log m$ operações (para alguma constante positiva C): escrevemos $m = \sum_{0 \leq i < M} a_i 2^i$ com $a_i \in \{0, 1\}$, definimos

$$m_k = \sum_{0 \leq i < k} a_{i+M-k} 2^i$$

e calculamos sucessivamente $U_{m_1}, V_{m_1}, \dots, U_{m_k}, V_{m_k}, \dots, U_{m_M} = U_m, V_{m_M} = V_m$.

Lembramos (proposição 6.21) que se $p > 2$ é primo e d não é um quadrado módulo p então $K = \mathbb{Z}[\sqrt{d}]/(p)$ é um corpo com p^2 elementos. Além disso, em K temos pela fórmula do binômio que

$$(a + b)^p = a^p + b^p \quad a, b \in K$$

já que p divide todos os coeficientes binomiais $\binom{p}{j}$ com $0 < j < p$.

Proposição 7.30. *Se n é primo e D não é um quadrado módulo n então $\alpha^n = \bar{\alpha}$ em $K = \mathbb{Z}[\sqrt{D}]/(n)$.*

DEMONSTRAÇÃO: Temos em K

$$\alpha^n = \frac{P^n + D^{(n-1)/2}\sqrt{D}}{2^n} = \frac{P - \sqrt{D}}{2} = \bar{\alpha},$$

pois $P^n \equiv P \pmod{n}$, $2^n \equiv 2 \pmod{n}$ e $D^{(n-1)/2} \equiv \left(\frac{D}{n}\right) \equiv -1 \pmod{n}$. \square

Analogamente, temos $\bar{\alpha}^n = \alpha$ em K . Assim, ainda em K , $\alpha^{n+1} = \bar{\alpha}^{n+1} = \alpha\bar{\alpha}$. Segue da fórmula para U_m que $U_{n+1} \equiv 0 \pmod{n}$. Proclamamos este resultado como uma proposição:

Proposição 7.31. *Se n é primo ímpar, $\left(\frac{D}{n}\right) = -1$ e as sequências U_m e V_m são definidas pelas recorrências*

$$\begin{aligned} U_0 &= 0, & U_1 &= 1, & U_{m+2} &= PU_{m+1} - QU_m, \\ V_0 &= 2, & V_1 &= P, & V_{m+2} &= PV_{m+1} - QV_m. \end{aligned}$$

então $U_{n+1} \equiv 0 \pmod{n}$.

DEMONSTRAÇÃO: Acima. \square

Esta proposição nos dá mais um algoritmo para testar a primalidade de n .

Proposição 7.32. *Se $n \neq 2$ é primo, $n \nmid Q$, $n \nmid D$ e D é quadrado módulo n então $U_{n-1} \equiv 0 \pmod{n}$.*

DEMONSTRAÇÃO: No anel $K = \mathbb{Z}[\sqrt{D}]/(n)$, 2 é invertível, assim como D e \sqrt{D} . Em K temos, portanto,

$$\alpha^n = \frac{P^n + D^{\frac{n-1}{2}}\sqrt{D}}{2^n} = \frac{P + \sqrt{D}}{2} = \alpha$$

donde $\alpha^{n-1} = 1$ em K (pois α é invertível em K : de fato, $\alpha\bar{\alpha} = Q$, que é invertível em K). Do mesmo modo, $\bar{\alpha}^{n-1} = 1$ em K e portanto temos, em K ,

$$U_{n-1} = \frac{1}{\sqrt{D}}(\alpha^{n-1} - \bar{\alpha}^{n-1}) = 0,$$

ou seja, $U_{n-1} \equiv 0 \pmod{n}$. \square

Em suma, se $n \neq 2$ é primo, $n \nmid Q$, $n \nmid D$ então $U_{n - (\frac{D}{n})}$ é múltiplo de n , o que se deve ao fato de α^m ser igual a $\bar{\alpha}^m$ se $m = n - (\frac{D}{n})$ no anel $K = \mathbb{Z}[\sqrt{D}]/(n)$. Observemos agora que se $\alpha^m = \bar{\alpha}^m$ em K então existe um inteiro r tal que

$$\alpha^m = \bar{\alpha}^m + nr\sqrt{D}$$

pois $\frac{\alpha^m - \bar{\alpha}^m}{\sqrt{D}} \in \mathbb{Z}$. Vamos usar este fato para mostrar por indução o seguinte resultado.

Proposição 7.33. *Se $n \neq 2$ é primo, $n \nmid Q$ e $n \nmid D$ então, para todo natural $k \geq 1$, $U_{m \cdot n^{k-1}}$ é múltiplo de n^k , onde $m = n - (\frac{D}{n})$.*

DEMONSTRAÇÃO: Vamos supor, por indução, que $\alpha^{m \cdot n^{k-1}} = \bar{\alpha}^{m \cdot n^{k-1}} + n^k r_k \sqrt{D}$, $r_k \in \mathbb{Z}$. Elevando os dois lados da equação à n -ésima potência temos

$$\alpha^{m \cdot n^k} = (\bar{\alpha}^{m \cdot n^{k-1}} + n^k r_k \sqrt{D})^n = \bar{\alpha}^{m \cdot n^k} + n^{k+1} r_{k+1} \sqrt{D}$$

onde r_{k+1} pertence a $\mathbb{Z}[\sqrt{D}]$ por um lado, e por outro $n^{k+1} r_{k+1} = U_{m \cdot n^k}$ é um inteiro, o que implica que $r_{k+1} \in \mathbb{Q} \cap \mathbb{Z}[\sqrt{D}]$ pelo lema 6.40, e portanto é inteiro, o que conclui a prova da afirmação, que equivale ao enunciado. \square

Proposição 7.34. *Sejam $r \geq 1$ com $\text{mdc}(r, Q) = 1$. Se*

$$A_r = \{k \in \mathbb{N}^* \mid U_k \text{ é múltiplo de } r\}$$

é não vazio então existe $a \in \mathbb{N}^$ tal que $r \mid U_k$ se, e somente se, $a \mid k$. Tal a será denotado por $\text{ord}_r U$.*

DEMONSTRAÇÃO: Observemos inicialmente que para todo $m, n \in \mathbb{N}$, $n \neq 0$ temos $U_{m+n} = U_m U_{n+1} - Q U_{m-1} U_n$. De fato, considerando m fixo e n variável, os dois lados da igualdade satisfazem a mesma recorrência de segunda ordem $X_{k+2} = P X_{k+1} - Q X_k$, $\forall k \in \mathbb{N}$, e temos, para $n = 0$, $U_{m+0} = U_m \cdot U_1 - Q U_{m-1} \cdot U_0$ (pois $U_1 = 1$ e $U_0 = 0$), e, para $m = 1$, $U_{m+1} = U_m \cdot U_2 - Q U_{m-1} \cdot U_1$ (pois $U_2 = P$, $U_1 = 1$ e $U_{m+1} = P U_m - Q U_{n-1}$), o que implica a igualdade para todo $n \in \mathbb{N}$.

Como consequência, se $r \mid U_m$ e $r \mid U_n$ então $r \mid U_{m+n}$. Por outro lado, se $r \mid U_\ell$ e $r \mid U_s$, com $\ell < s$ então, como (fazendo $m = \ell$, $n = s - \ell$) $U_s = U_\ell U_{s-\ell+1} - QU_{\ell-1} U_{s-\ell}$ temos que r divide $QU_{\ell-1} U_{s-\ell}$, mas $\text{mdc}(Q, r) = 1$ e $\text{mdc}(U_{\ell-1}, U_\ell)$ divide $Q^{\ell-1}$ (o que pode ser facilmente provado por indução a partir de $U_{\ell+1} = PU_\ell - QU_{\ell-1}$), donde $\text{mdc}(r, U_{\ell-1})$ também é igual a 1, logo $r \mid U_{s-\ell}$. Assim, $m, n \in A_r \Rightarrow m + n \in A_r$, e $\ell, s \in A_r$, $\ell < s \Rightarrow s - \ell \in A_r$, o que implica que A_r é da forma descrita, com $a = \min A_r$ (de fato, se existe $k \in A_r$ que não seja múltiplo de a , existiriam b e c naturais com $k = ab + c$, $0 < c < a$, mas $k \in A_r$ e, como $a \in A_r$, $ab \in A_r$, logo $c = k - ab$ pertenceria a A_r , contradizendo a definição de a). \square

Teorema 7.35. *Seja $n > 1$ um inteiro ímpar. Se existe um inteiro d primo com n tal que para todo fator primo r de $n+1$ existem $P^{(r)}$, $Q^{(r)}$ e $m^{(r)}$ inteiros com $\text{mdc}(m^{(r)}, n) = 1$ e $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)} \equiv d(m^{(r)})^2 \pmod{n}$ tais que a sequência de Lucas associada $(U_k^{(r)})$ satisfaz $U_{n+1}^{(r)} \equiv 0 \pmod{n}$ e $U_{\frac{n+1}{r}}^{(r)} \not\equiv 0 \pmod{n}$ então n é primo.*

DEMONSTRAÇÃO: Seja $n+1 = r_1^{\alpha_1} r_2^{\alpha_2} \dots r_k^{\alpha_k}$ a fatoração prima de $n+1$. As hipóteses implicam que $r_i^{\alpha_i}$ divide $\text{ord}_n U^{(r_i)}$ para $i = 1, 2, \dots, k$. Por outro lado, se $n = \ell_1^{\beta_1} \ell_2^{\beta_2} \dots \ell_s^{\beta_s}$ é a fatoração prima de n , segue da Proposição 7.33 que $\text{ord}_{\ell_j^{\beta_j}} U^{(r_i)}$ divide $\ell_j^{\beta_j-1} (\ell_j - (\frac{d}{\ell_j}))$ (A hipótese $\ell_j \nmid Q^{(r_i)}$ é satisfeita. De fato, como $\text{mdc}(n, d) = 1$, ℓ_j não divide $D^{(r_i)}$, e, se ℓ_j dividisse $Q^{(r_i)}$, ℓ_j não dividiria $P^{(r_i)}$, e teríamos $U_k^{(r_i)} \equiv (P^{(r_i)})^{k-1} \pmod{\ell_j}$ para todo $k \geq 1$, e ℓ_j não dividiria $U_k^{(r_i)}$ para nenhum $k \geq 1$, contradizendo o fato de n dividir $U_{n+1}^{(r_i)}$). Assim, se $M = \text{mmc}\{\ell_j^{\beta_j-1} (\ell_j - (\frac{d}{\ell_j})), 1 \leq j \leq s\}$ temos que $\ell_j^{\beta_j}$ divide $U_M^{(r_i)}$, para $1 \leq j \leq s$, $1 \leq i \leq k$. Isso implica que $n = \ell_1^{\beta_1} \dots \ell_s^{\beta_s}$ divide $U_M^{(r_i)}$ para $1 \leq i \leq k$, e portanto $r_i^{\alpha_i} \mid \text{ord}_n U^{(r_i)} \mid M$ para $1 \leq i \leq k$, donde $n+1$ divide M . Temos agora duas possibilidades:

1. $s = 1$. Nesse caso temos que $n+1$ divide $M = \ell_1^{\beta_1-1} (\ell_1 - (\frac{d}{\ell_1}))$ o que é absurdo se $(\frac{d}{\ell_1}) = 1$, pois teríamos $M < \ell_1^{\beta_1} = n$, e se $(\frac{d}{\ell_1}) = -1$ temos que $\ell_1^{\beta_1} + 1$ divide $\ell_1^{\beta_1-1} (\ell_1 + 1)$, o que implica $\beta_1 = 1$, ou seja, n é primo.

2. $s \geq 2$. Nesse caso

$$\begin{aligned} M &= \text{mmc} \left\{ \ell_j^{\beta_j-1} \left(\ell_j - \left(\frac{d}{\ell_j} \right) \right), \quad 1 \leq j \leq s \right\} \\ &= 2 \text{mmc} \left\{ \frac{\ell_j^{\beta_j-1} \left(\ell_j - \left(\frac{d}{\ell_j} \right) \right)}{2}, \quad 1 \leq j \leq s \right\} \\ &\leq 2 \prod_{j=1}^s \frac{\ell_j^{\beta_j-1} \left(\ell_j - \left(\frac{d}{\ell_j} \right) \right)}{2} \leq 2n \prod_{j=1}^s \frac{\ell_j + 1}{2\ell_j}, \end{aligned}$$

que é sempre menor que n (pois $2 \cdot \frac{4}{6} \cdot \frac{6}{10} < 1$) e portanto é um absurdo que $n+1$ dividia M . □

A seguinte proposição, devida a Morrison, é análoga ao resultado de Pocklington:

Proposição 7.36. *Seja $N > 1$ um inteiro ímpar e $N+1 = FR$. Se existe um inteiro d primo com N tal que para todo fator primo r de F existe uma sequência de Lucas $U_n^{(r)}$ associada a inteiros $P^{(r)}, Q^{(r)}$ e um inteiro $m^{(r)}$ primo com N e $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)} \equiv d(m^{(r)})^2 \pmod{N}$ tal que $N \mid U_{\frac{N+1}{r}}^{(r)}$ e $\text{mdc}(U_{\frac{N+1}{r}}^{(r)}, N) = 1$ então cada fator primo ℓ de N satisfaz $\ell \equiv \left(\frac{d}{\ell} \right) \pmod{F}$.*

DEMONSTRAÇÃO: Se $F = r_1^{\alpha_1} r_2^{\alpha_2} \dots r_k^{\alpha_k}$ é a fatoração canônica de F então $\text{ord}_N U^{(r_i)} \mid N+1$ para $1 \leq i \leq k$. Se ℓ é um fator primo de N , também temos $\text{ord}_\ell U^{(r_i)} \mid N+1$. Como $\text{mdc}(N, U_{\frac{N+1}{r_i}}^{(r_i)}) = 1$ segue que $\ell \nmid U_{\frac{N+1}{r_i}}^{(r_i)}$, donde $\text{ord}_\ell U^{(r_i)} \nmid \frac{N+1}{r_i}$, e portanto $r_i^{\alpha_i}$ divide $\text{ord}_\ell U^{(r_i)}$ para $1 \leq i \leq k$. Por outro lado, $\text{ord}_\ell U^{(r_i)}$ divide $\ell - \left(\frac{d}{\ell} \right)$, donde $r_i^{\alpha_i}$ divide $\ell - \left(\frac{d}{\ell} \right)$ para $1 \leq i \leq k \implies F$ divide $\ell - \left(\frac{d}{\ell} \right) \implies \ell \equiv \left(\frac{d}{\ell} \right) \pmod{F}$. □

Corolário 7.37. *Nas condições da proposição, se $F > R$ então N é primo.*

DEMONSTRAÇÃO: Qualquer fator primo de N deve ser congruente a 1 ou a -1 módulo F , mas, se N é composto, deve ter um fator primo menor ou igual à sua raiz quadrada, que deve, pois, ser igual a $F - 1$. Como $F > \sqrt{N+1}$, $F^2 - 1 > N$, logo $\frac{N}{F-1} < F+1$, donde o outro fator primo de N também deve ser igual a $F - 1$, e teríamos $N = (F - 1)^2 \Rightarrow N + 1 = F^2 - 2F + 2$, que só seria múltiplo de F se F fosse igual a 2, e $F - 1$ igual a 1, absurdo. \square

Proposição 7.38. *Seja $n > 1$ um inteiro ímpar. Se para todo fator primo r de $n + 1$ existem $P^{(r)}, Q^{(r)}$ inteiros com $\text{mdc}(D^{(r)}, n) = 1$ onde $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)}$ tais que a sequência de Lucas associada $(U_k^{(r)})$ satisfaz $U_{n+1}^{(r)} \equiv 0 \pmod{n}$ e $\text{mdc}(U_{\frac{n+1}{r}}^{(r)}, n) = 1$ então n é primo.*

DEMONSTRAÇÃO: Seja ℓ um fator primo de n . Para cada fator primo r de $n + 1$ temos que $U_{n+1}^{(r)} \equiv 0 \pmod{\ell}$ e $U_{\frac{n+1}{r}}^{(r)} \not\equiv 0 \pmod{\ell}$. Assim, se r^{α_r} é a maior potência de r que divide $n + 1$, então r^{α_r} divide $\ell - \left(\frac{D^{(r)}}{\ell}\right)$, como acima. Em particular, r^{α_r} divide $\ell^2 - 1 = (\ell - 1)(\ell + 1)$, donde $n + 1$ divide $\ell^2 - 1$. Assim, $\ell^2 - 1 \geq n + 1$ donde $\ell > \sqrt{n}$, o que implica na primalidade de n pois n não tem nenhum fator primo menor ou igual à sua raiz quadrada. \square

Vamos agora dar outra prova do critério de Lucas-Lehmer usando os resultados anteriores.

DEMONSTRAÇÃO: A sequência de Lucas associada a $P = 2, Q = -2$, é dada pela fórmula $U_k = \frac{1}{2\sqrt{3}}((1 + \sqrt{3})^k - (1 - \sqrt{3})^k)$. Temos $(1 + \sqrt{3})^k = \frac{V_k}{2} + U_k\sqrt{3}$, onde $V_k = (1 + \sqrt{3})^k + (1 - \sqrt{3})^k$. Além disso, $U_{2k} = U_k V_k$ para todo $k \in \mathbb{N}$.

Para $r \geq 1$ temos

$$\begin{aligned} V_{2^r} &= (1 + \sqrt{3})^{2^r} + (1 - \sqrt{3})^{2^r} = (4 + 2\sqrt{3})^{2^{r-1}} + (4 - 2\sqrt{3})^{2^{r-1}} \\ &= 2^{2^{r-1}}((2 + \sqrt{3})^{2^{r-1}} + (2 - \sqrt{3})^{2^{r-1}}) = 2^{2^{r-1}} S_{r-1} \end{aligned}$$

(onde $S_0 = 4, S_{m+1} = S_m^2 - 2, \forall m \in \mathbb{N}$). Se $n > 2$ e $M_n = 2^n - 1$ divide S_{n-2} então M_n divide $V_{2^{n-1}}$, logo também divide $U_{M_n+1} = U_{2^n} = U_{2^{n-1}} V_{2^{n-1}}$, e, como $U_{\frac{M_n+1}{2}} = U_{2^{n-1}}$, e $V_k^2 - 12U_k^2 = 4(-2)^k$, segue que $V_{2^{n-1}}^2 - 12U_{2^{n-1}}^2 = 2^{2^{n-1}+2}$, e, se algum fator de M_n divide $U_{\frac{M_n+1}{2}}$, divide

também $2^{2^{n-1}+2}$, logo é igual a 1. Assim, pela proposição anterior, M_n é primo.

Por outro lado, se M_n é primo, como $D = 12$, $\left(\frac{12}{M_n}\right) = \left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = 1$, logo M_n divide $U_{M_n+1} = U_{2^n}$, e, como

$$\begin{aligned} V_{2^n-1}^2 &= V_{2^n} + 2(-2)^{2^{n-1}} = V_{2^n} + 2 \cdot 2^{\frac{M_n+1}{2}} \\ &= V_{2^n} + 4 \cdot 2^{\frac{M_n-1}{2}} \equiv V_{2^n} + 4 \left(\frac{2}{M_n}\right) \equiv V_{2^n} + 4 \pmod{M_n}, \end{aligned}$$

pois $2 \equiv 2^{n+1} \equiv (2^{\frac{n+1}{2}})^2 \pmod{M_n}$ (já sabemos que n deve ser um primo ímpar). Temos

$$V_{2^n} = (1 + \sqrt{3})^{2^n} + (1 - \sqrt{3})^{2^n} = (1 + \sqrt{3})^{M_n+1} + (1 - \sqrt{3})^{M_n+1},$$

que é igual a $(1 - \sqrt{3})(1 + \sqrt{3}) + (1 + \sqrt{3})(1 - \sqrt{3}) = -4$ em $K = \mathbb{Z}[\sqrt{3}]/(M_n)$ (pois $\left(\frac{3}{M_n}\right) = -1$) donde $V_{2^n-1}^2 = V_{2^n} + 4 \equiv 0 \pmod{M_n}$ e portanto $M_n \mid V_{2^n-1} = 2^{2^{n-2}} S_{n-2}$. Assim, M_n divide S_{n-2} , o que conclui nossa nova demonstração do critério de Lucas-Lehmer. \square

Se N é um primo ímpar e d não é quadrado módulo N , então $K = \mathbb{Z}[\sqrt{d}]/(N)$ é um corpo finito com N^2 elementos e portanto existem inteiros a e b tais que $x = a + b\sqrt{d}$ é uma raiz primitiva de K . Sejam $\bar{x} = a - b\sqrt{d}$ e, para $m \in \mathbb{N}$, $U_m = (x^m - \bar{x}^m)/2b\sqrt{d}$. Temos $U_0 = 0$, $U_1 = 1$ e $U_{m+2} = 2aU_{m+1} - (a^2 - db^2)U_m$ para todo $m \in \mathbb{N}$. Temos ainda $b \neq 0$ em K , senão x pertenceria a $\mathbb{Z}/(M) \subset K$ e $\text{ord}_K x$ dividiria $N - 1$. Assim, b e \sqrt{d} são invertíveis em K e, se $P = 2a$, $Q = a^2 - db^2$ então $D = P^2 - 4Q = 4db^2$ satisfaz $\left(\frac{D}{N}\right) = -1$. Pela proposição 7.31, $U_{N+1} \equiv 0 \pmod{N}$. Por outro lado, se m é menor que $N + 1$, caso N divida U_m teríamos $x^m = \bar{x}^m$ em K , donde teríamos em K , $(\bar{x}/x)^m = 1$. Pela proposição 7.30, $\bar{x} = x^N$, logo $x^{(N-1)m} = 1$, absurdo, pois $\text{ord}_K x = N^2 - 1 = (N - 1)(N + 1) > (N - 1)m$. Assim, $\text{ord}_N U = N + 1$. Isto fornece recíprocas para os resultados desta seção.

Problemas Propostos

7.17 (Lucas-Lehmer-Riesel). *Sejam a e $M_{n,a} = a \cdot 2^n - 1$ números primos com 6 tais que $2^n > a$. Definimos recursivamente a sequência $\{S_j\}$ onde $S_0 = (2 + \sqrt{3})^a + (2 - \sqrt{3})^a$ e $S_{j+1} = S_j^2 - 2$. Mostre que $M_{n,a}$ é primo se, e somente se, S_{n-2} é divisível por $M_{n,a}$.*

7.7 Aspectos Computacionais

Nas seções anteriores demonstramos vários critérios de primalidade. Aqui faremos várias considerações quanto ao valor prático destes critérios, sendo nosso objetivo dar uma ideia geral do funcionamento dos programas que encontraram os maiores números primos conhecidos. Veremos que uma das nossas principais preocupações será a de saber multiplicar inteiros rapidamente e os melhores algoritmos para esta tarefa estão baseados na transformada de Fourier discreta. A parte deste capítulo referente a este tema está fortemente baseada no livro de M. Clausen e U. Baum [35].

No endereço

`ftp://ftp.mat.puc-rio.br/pub/users/nicolau/merzenne/merzenne.tgz`

encontram-se implementações de alguns destes algoritmos escritas na linguagem C. Estes programas são de cunho puramente pedagógico, muito além do ideal, principalmente em termos de velocidade, e têm apenas o propósito de ilustrar os principais aspectos matemáticos de uma boa implementação dos testes de primalidade.

7.7.1 O Algoritmo de Multiplicação de Karatsuba

A forma de multiplicar inteiros ensinada na escola é simples e conveniente para inteiros relativamente pequenos, mas vejamos seu custo. Para multiplicar dois inteiros de n dígitos na base d procedemos basicamente a partir da fórmula:

$$\left(\sum_i a_i d^i\right)\left(\sum_j b_j d^j\right) = \sum_{i,j} a_i b_j d^{i+j} :$$

calculamos (ou olhamos na tabuada) todos os produtos de um dígito de um dos inteiros com um dígito do outro, multiplicamos pela potência de d apropriada (o que equivale a acrescentar zeros à direita) e somamos as n^2 parcelas obtidas. Efetuamos no processo n^2 multiplicações e um número comparável de somas; assim, o tempo gasto com este algoritmo é aproximadamente An^2 para alguma constante positiva A . Se isto fosse o melhor que pudessemos fazer, o tempo para checar a primalidade de M_p seria aproximadamente Ap^3 . Existem entretanto outros algoritmos de multiplicação: examinemos primeiro um algoritmo relativamente simples, o algoritmo de Karatsuba, usado pela biblioteca gmp (e portanto por nossos programas acima).

Sejam A e B dois inteiros com n dígitos cada um. Se $m = \lceil n/2 \rceil$, podemos escrever

$$\begin{aligned} A &= A_1 d^m + A_0, \\ B &= B_1 d^m + B_0 \quad \text{e} \\ AB &= A_1 B_1 d^{2m} + (A_1 B_0 + A_0 B_1) d^m + A_0 B_0. \end{aligned}$$

Pelo algoritmo anterior, calcularíamos os quatro produtos de inteiros com m dígitos. Entretanto, os produtos $A_1 B_0$ e $A_0 B_1$ não são necessários individualmente, e podemos calcular sua soma da seguinte forma:

$$A_1 B_0 + A_0 B_1 = (A_1 - A_0)(B_0 - B_1) + A_1 B_1 + A_0 B_0.$$

Em outras palavras, podemos escrever

$$AB = A_1 B_1 (d^{2m} + d^m) + (A_1 - A_0)(B_0 - B_1) d^m + A_0 B_0 (d^m + 1).$$

Assim, podemos calcular os três coeficientes com apenas três multiplicações (ao invés de quatro) e algumas somas. Mesmo que o número de somas aumente, já sabemos que somas são rápidas e portanto podemos esperar que este algoritmo represente uma melhora substancial em relação ao anterior.

Mais precisamente, repetimos este processo para diminuirmos o tamanho dos inteiros. Assim, se denotarmos por $f(n)$ o tempo necessário para multiplicar inteiros de n dígitos temos $f(n) \approx 3f(\lceil n/2 \rceil) + An$ e provamos facilmente que

$$f(n) \approx An^\alpha,$$

onde $\alpha = (\log 3)/(\log 2)$.

7.7.2 Multiplicação de Polinômios Usando FFT

Suponha que queiramos multiplicar dois polinômios $P, Q \in \mathbb{C}[x]$, de grau menor do que n , representados pelos seus coeficientes:

$$\begin{aligned} P(x) &= \sum_{0 \leq j < n} a_j x^j = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \\ Q(x) &= \sum_{0 \leq j < n} b_j x^j = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}. \end{aligned}$$

O método aprendido na escola exige n^2 multiplicações; o método de Karatsuba pode ser adaptado para este problema e exige aproximadamente n^α multiplicações, com $\alpha = (\log 3)/(\log 2)$. Veremos agora como efetuar esta multiplicação com um número muito menor de operações.

Uma ideia é a de considerar os polinômios como representados não pelos seus coeficientes e sim pelos seus valores em n pontos distintos ξ_0, \dots, ξ_{n-1} . Temos evidentemente $(P \cdot Q)(\xi_j) = P(\xi_j) \cdot Q(\xi_j)$: se o produto PQ tem grau menor do que n então PQ é o único polinômio que assume estes n valores. A dificuldade em usar este método está em calcular os valores de P e Q nos n pontos ξ_0, \dots, ξ_{n-1} e em recuperar PQ a partir de seu valor nestes mesmos pontos. Se os valores ξ_j forem escolhidos sem critério este método pode acabar sendo mais lento do que os outros que já apresentamos. Veremos que certas escolhas de n e ξ_j tornam o algoritmo rápido: uma das mais simples é tomar n uma potência de 2 e $\xi_j = \omega^j$, onde $\omega = e^{2\pi i/n}$ é uma raiz da unidade de ordem n .

Suponha que $\xi_k = -\xi_j \neq 0$ então as potências pares de ξ_j e ξ_k coincidem, enquanto as potências ímpares diferem pelo sinal. Isto nos permite economizar multiplicações quando calculamos $P(\xi_j)$ e $P(\xi_k) = P(-\xi_j)$ simultaneamente. Se n é par, podemos escrever

$$\begin{aligned} P(\xi_j) &= P_+(\xi_j^2) + \xi_j P_-(\xi_j^2), \\ P(-\xi_j) &= P_+(\xi_j^2) - \xi_j P_-(\xi_j^2), \end{aligned}$$

onde

$$\begin{aligned} P_+(x) &= \sum_{0 \leq j < n/2} a_{2j} x^j, \\ P_-(x) &= \sum_{0 \leq j < n/2} a_{2j+1} x^j, . \end{aligned}$$

Ou seja, reduzimos o problema de calcular um polinômio de grau n em dois pontos ao problemas de calcular dois polinômios de grau $n/2$ em um mesmo ponto, seguido de uma multiplicação, uma soma e uma subtração. Se os ξ_j sempre ocorrerem aos pares, com por exemplo $\xi_{j+(n/2)} = -\xi_j$, o cálculo de $P(\xi_0), \dots, P(\xi_n)$ reduz-se ao cálculo de

$$P_+(\xi_0^2), \dots, P_+(\xi_{(n/2)-1}^2), \quad P_-(\xi_0^2), \dots, P_-(\xi_{(n/2)-1}^2)$$

seguido de $3n/2$ operações.

O ideal é que pudéssemos repetir o processo acima, ou seja, que n seja múltiplo de 4 e que também no conjunto $\xi_0^2, \dots, \xi_{(n/2)-1}^2$ os números ocorressem em pares diferindo apenas por sinal. Reordenando os termos, podemos reformular esta condição como $\xi_{j+(n/4)}^2 = -\xi_j^2$, ou, sem perda de generalidade, como $\xi_{j+(n/4)} = i\xi_j$. Para podermos repetir este processo um número máximo de vezes, devemos tomar n como uma potência de 2 e $\xi_{j+k} = \omega^k \xi_j$, onde $\omega = e^{2\pi i/n}$. Devemos assim tomar $\xi_j = \omega^j \xi_0$ e a escolha $\xi_0 = 1$ parece particularmente simples.

Façamos agora uma estimativa de $T(n)$, o número de operações usadas neste algoritmo para calcular $P(\xi_0), \dots, P(\xi_n)$. Já vimos que $T(n) = 2T(n/2) + 3n/2$; claramente $T(1) = 0$. Daí temos $T(2) = 3$, $T(4) = 12$ e, por uma indução simples, $T(2^k) = 3k \cdot 2^{k-1}$. Assim, é possível calcular $P(1), \dots, P(\omega^{n-1})$ muito rapidamente.

Reformulemos este problema na linguagem de álgebra linear. Temos

$$\begin{pmatrix} P(1) \\ P(\omega) \\ P(\omega^2) \\ \vdots \\ P(\omega^{n-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)^2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix};$$

a matriz de ordem n e coeficientes ω^{ij} , $0 \leq i, j < n$, é chamada de DFT_n , a *transformada de Fourier discreta*. O que aprendemos nos parágrafos acima foi a multiplicar DFT_n por um vetor rapidamente (pelo menos quando n é uma potência de 2). Em termos algébricos, aprendemos a escrever DFT_n como um produto de $\log_2 n$ matrizes esparsas cujos coeficientes não nulos são potências de ω ; cada matriz esparsa correspondendo a uma etapa do algoritmo FFT.

Falta aprender a recuperar os coeficientes de um polinômio P a partir de

$$P(1), \dots, P(\omega^{n-1}),$$

ou seja, a multiplicar $(DFT_n)^{-1}$ por um vetor. Mas para isto basta

observar que

$$(DFT_n)^2 = n \cdot \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \end{pmatrix},$$

pois o coeficiente (i, k) de $(DFT_n)^2$ é

$$\sum_j \omega^{ij} \omega^{jk} = \sum_j \omega^{(i+k)j}$$

que é igual a n se $i + k \equiv 0 \pmod{n}$ e 0 caso contrário pois se $n \nmid \ell$, $\omega^\ell \neq 1$ e

$$\sum_j \omega^{\ell j} = \frac{\omega^{\ell n} - 1}{\omega^\ell - 1} = 0.$$

Assim, o coeficiente (i, j) de $(DFT_n)^{-1}$ é $(1/n)\omega^{-ij}$ e este processo de FFT inversa (ou interpolação) é tão fácil e rápido quanto FFT (ou avaliação). Temos portanto um algoritmo para multiplicar polinômios de grau n fazendo aproximadamente $Cn \log n$ operações (onde C é uma constante positiva).

Reproduzimos abaixo o pseudo-código de [35] para este algoritmo:

Input: O comprimento n (uma potência de 2); uma raiz primitiva da unidade ω de ordem n ; um vetor (a_0, \dots, a_{n-1}) de coeficientes complexos.

Output: O vetor $(A_0, \dots, A_{n-1})^t = (DFT_n)(a_0, \dots, a_{n-1})^t$.

procedure $FFT(n, \omega, a_0, a_1, \dots, a_{n-1}; A_0, A_1, \dots, A_{n-1})$;

begin

if $n = 1$ **then**

$A_0 = a_0$;

else

$FFT(n/2, \omega^2, a_0, a_2, \dots, a_{n-2}; E_0, \dots, E_{n/2-1})$;

$FFT(n/2, \omega^2, a_1, a_3, \dots, a_{n-1}; O_0, \dots, O_{n/2-1})$;

for $k = 0$ **to** $n/2 - 1$ **do**

$A_k = E_k + \omega^k O_k$;

$A_{k+n/2} = E_k - \omega^k O_k$;

end

Até agora consideramos polinômios com coeficientes em \mathbb{C} mas o leitor atento já deve ter percebido que podemos usar o mesmo algoritmo para multiplicar polinômios sobre qualquer corpo K desde que exista em K um elemento ω que seja uma raiz da unidade de ordem n . Um exemplo de corpo onde existe um tal ω é $\mathbb{Z}/(p)$ se $p \equiv 1 \pmod{n}$. Na verdade não é sequer necessário que os coeficientes estejam em um corpo: podemos trabalhar sobre qualquer anel A onde exista ω com as seguintes propriedades:

1. $\omega^n = 1$,
2. n é invertível em A ,
3. se $0 < \ell < n$ então $\omega^\ell - 1$ é invertível em A .

Na próxima seção veremos uma situação onde será interessante trabalhar com $A = \mathbb{Z}/(2^K + 1)$.

Lembramos que este algoritmo calcula corretamente o produto dos polinômios P e Q desde que este produto tenha grau menor do que n . Mais geralmente, estaremos encontrando o único polinômio de grau menor que n que coincide com PQ em $\xi_0, \xi_1, \dots, \xi_{n-1}$. Como estamos tomando sempre $\xi_j = \omega^j \xi_0$ temos

$$(x - \xi_0)(x - \xi_1) \cdots (x - \xi_{n-1}) = x^n - \xi_0^n$$

e nosso algoritmo calcula $PQ \bmod (x^n - \xi_0^n)$.

7.7.3 Multiplicação de Inteiros Usando FFT

Quando escrevemos um inteiro a na base d ,

$$a = \sum_k a_k d^k,$$

podemos pensar que estamos escrevendo

$$a = P(d), \quad P(x) = \sum_k a_k x^k.$$

Se desejarmos calcular ab onde

$$b = Q(d), \quad Q(x) = \sum_k b_k x^k$$

podemos usar o algoritmo da seção anterior para calcular os coeficientes c_k do produto

$$(PQ)(x) = \sum_k c_k x^k, \quad c_k = \sum_j a_j b_{k-j}$$

e temos $ab = (PQ)(d)$. Os c_k em geral não serão dígitos aceitáveis para uma expansão na base d do inteiro ab mas isto pode facilmente ser corrigido: escrevemos $c'_0 = c_0 + de_0$, $c'_1 = c_1 - e_0 + de_1$, ..., $c'_k = c_k - e_{k-1} + de_k$, ..., onde a cada passo tomamos c'_k como sendo um dígito aceitável. Ao final, teremos

$$ab = \sum_k c'_k d^k,$$

a expansão de ab na base d .

A dificuldade maior reside no fato que as contas descritas na seção anterior envolvem números complexos, e as partes real e imaginária destes números complexos são irracionais. Uma alternativa é fazer as contas usando variáveis do tipo double; teremos inevitavelmente erros de truncamento mas o fato de sabermos que a resposta final é um inteiro nos dá uma oportunidade de corrigir estes erros. É claro que precisamos ter o cuidado de evitar que os erros de truncamento somem mais do que 0,5: neste caso acabaríamos arredondando a resposta final para o inteiro errado. Esta possibilidade desastrosa pode ser evitada tomando d pequeno (e portanto grau grande, o que implica em uma transformada de Fourier de comprimento maior); também ajuda muito tomar o conjunto dos dígitos aceitáveis simétrico em relação ao zero, pois assim os produtos $a_j b_{k-j}$ serão menores e terão sinais diferentes, o que evita que os coeficientes c_k sejam grandes demais. Mesmo para inteiros bem maiores do que o maior primo conhecido existem valores de d que garantem o bom funcionamento deste método, um dos mais rápidos para multiplicar inteiros grandes (em parte porque a maioria dos computadores é capaz de multiplicar doubles com grande rapidez). Por isso, ele é usado pelo programa mprime-prime95, que encontrou os últimos 4 primos de Mersenne.

Uma segunda alternativa é escolher um primo p e fazer a multiplicação de polinômios considerando os coeficientes como elementos de $\mathbb{Z}/(p)$. Para recuperarmos os verdadeiros coeficientes do produto (que são inteiros), precisamos ter o cuidado de garantir que $|c_k| < p/2$ onde $c_k =$

$\sum a_j b_{k-j}$. Um primo usado em alguns programas³ é $p = 2^{64} - 2^{32} + 1$, que tem aliás várias propriedades especiais que o tornam particularmente apropriado para nossa tarefa. Com este valor de p , como $2^{32} \mid p - 1$, podemos fazer FFTs de comprimento 2^{32} com $d = 2^{16}$, o que permite (em princípio) multiplicar inteiros de módulo menor do que $2^{16 \cdot 2^{32} - 1}$, ou seja, inteiros com alguns *bilhões* de dígitos; o simples armazenamento de um tal inteiro exige memória maior do que a que tem a maioria dos computadores atuais.

Mas estas alternativas, apesar de computacionalmente atraentes, não satisfazem ao matemático puro pois funcionam para inteiros menores do que um certo tamanho fixo (apesar de muito grande). A segunda alternativa apresentada acima pode ser levada adiante tomando primos cada vez maiores, mas não será fácil provar que existem sempre primos com as propriedades desejadas. Veremos agora como multiplicar inteiros de tamanho arbitrário em tempo baixo fazendo as contas não em $\mathbb{Z}/(p)$, mas em $\mathbb{Z}/(2^K + 1)$ (mesmo $2^K + 1$ não sendo primo) e assim evitaremos esta dificuldade. Uma outra vantagem deste método é que será muito fácil multiplicar por potências de ω (assim tornando rápidas as FFTs).

Mais precisamente, mostraremos como multiplicar inteiros (dados por suas expansões binárias) módulo $2^N + 1$; esta é a versão simplificada de Schönhage de um algoritmo devido a Schönhage e Strassen. Se N for tomado suficientemente grande este algoritmo multiplica inteiros. Consideraremos apenas valores de $N \geq 320$ da forma

$$N = \nu \cdot 2^n, \quad n - 1 \leq \nu \leq 2n, \quad n \geq 4;$$

estes valores de N serão chamados de *aceitáveis*. Supomos que já sabemos multiplicar módulo $2^K + 1$, onde $K = \kappa \cdot 2^k < N$ também é um valor aceitável (a ser escolhido).

Para usar a multiplicação de polinômios, escrevemos os inteiros a e b a serem multiplicados na base d , i.e.,

$$a = \sum_{0 \leq i < 2^m - 1} a_i d^i, \quad b = \sum_{0 \leq j < 2^m - 1} b_j d^j, \quad 0 \leq a_i, b_j < d,$$

onde $m = \lfloor n/2 \rfloor + 1$ e $d = 2^{N/2^m}$. Temos $d^{2^m} = 2^N \equiv -1 \pmod{2^N + 1}$. Assim, podemos escrever $c \equiv ab \pmod{2^N + 1}$ com

$$c = \sum_{0 \leq \mu < 2^m - 1} b_\mu d^\mu, \quad c_\mu = \sum_{i+j=\mu} a_i b_j - \sum_{i+j=\mu+2^m} a_i b_j.$$

³Em particular no StrongARM, veja <http://www.axis.demon.co.uk/armprime/>

Pela seção anterior e por indução, sabemos efetuar estas contas módulo $2^K + 1$ mas novamente precisamos do valor de cada c_μ como inteiro, ou seja, precisamos escolher K de tal forma que possamos garantir que $|c_\mu| \leq 2^{K-1}$. É fácil verificar que podemos escolher $\kappa = \lceil (\nu + 1)/2 \rceil$ e $k = \lceil n/2 \rceil + 1$; observe que $K = \kappa \cdot 2^k$ é de fato aceitável.

Sejam $\tilde{\omega} = 2^{K/2^m}$ e $\omega = \tilde{\omega}^2$. Como $\omega^{2^{m-1}} \equiv -1 \pmod{2^K + 1}$ temos que ω é uma raiz da unidade em $\mathbb{Z}/(2^K + 1)$ de ordem 2^m : este valor de ω pode ser usado para fazer FFT como na seção anterior; temos

$$c_\mu \equiv \tilde{\omega}^{-\mu} \sum_{i+j \equiv \mu \pmod{2^m}} (\tilde{\omega}^i a_i) (\tilde{\omega}^j b_j) \pmod{2^K + 1}.$$

Note que podemos efetuar tanto FFT quanto FFT inversa pois 2^m e $\omega^i - 1$ são inversíveis módulo $2^K + 1$ (o que deixamos como exercício).

Falta apenas estimar o número de operações gasto por este algoritmo; note que por operação aqui queremos dizer uma operação sobre bits. Em todo o algoritmo, efetuamos duas FFTs de comprimento 2^m sobre $\mathbb{Z}/(2^K + 1)$, 2^m multiplicações ponto a ponto (também sobre $\mathbb{Z}/(2^K + 1)$) e uma FFT inversa de comprimento 2^m . Observe que como ω é uma potência de 2, as multiplicações por potências de ω que ocorrem nas FFTs são rápidas pois são apenas translações dos dígitos; mais precisamente, exigem no máximo CK operações cada uma (para alguma constante positiva C). Assim, cada FFT exige no máximo $Cm \cdot 2^m K$ operações. O número total $T(N)$ de operações satisfaz assim a recorrência

$$T(N) \leq 2^m T(K) + Cm \cdot 2^m K$$

donde podemos demonstrar que, para alguma constante positiva C ,

$$T(n) \leq CN \log N \log \log N.$$

Finalmente, mencionamos ainda que existem alternativas assintoticamente mais eficientes para multiplicar inteiros. O *algoritmo de Fürer* (ver [56]) tem complexidade $n \log n 2^{O(\log^* n)}$, onde $\log^* n$ denota a função definida recursivamente por

$$\log^* n = \begin{cases} 0 & \text{se } n \leq 1; \\ 1 + \log^*(\log n) & \text{se } n > 1 \end{cases}$$

Na vida real, entretanto, a diferença entre $\log \log n$ e $2^{\log^* n}$ é tão pequena que apenas se faz sentir para números astronomicamente gigantes.

7.7.4 A Complexidade das Operações Aritméticas

Vimos na seção anterior que o número de operações (e portanto o tempo) necessário para multiplicar inteiros de N dígitos é aproximadamente (a menos de um fator constante) $N \log N \log \log N$ se utilizarmos um dos algoritmos descritos. Não se conhece nenhum algoritmo que seja assintoticamente mais rápido mas também não se sabe demonstrar que não existe um tal algoritmo. Mostraremos nesta seção que o tempo necessário para realizar qualquer uma das operações abaixo é assintoticamente o mesmo (isto é, difere por uma constante multiplicativa). Note que adições e subtrações são mais rápidas e desprezaremos o tempo exigido por essas operações.

1. Multiplicar inteiros de N dígitos.
2. Elevar ao quadrado um inteiro de N dígitos.
3. Inverter, ou seja, encontrar os primeiros $2N$ dígitos depois da vírgula de $1/n$, onde n tem N dígitos, ou ainda, calcular $\lfloor Q^{2N}/n \rfloor$ (se trabalharmos na base Q).
4. Fazer a divisão com resto de dois inteiros de N dígitos, i.e., dados n e m encontrar q e r com $n = qm + r$, $0 \leq r < m$.

Estas operações podem ser reduzidas uma às outras com a mesma ordem de grandeza de tempo, i.e., multiplicando o tempo necessário por uma constante. Faremos isto da seguinte forma:

- (a) Quem sabe multiplicar sabe elevar ao quadrado.
- (b) Quem sabe elevar ao quadrado sabe multiplicar.
- (c) Quem sabe multiplicar sabe inverter.
- (d) Quem sabe inverter sabe elevar ao quadrado.
- (e) Quem sabe multiplicar e inverter sabe dividir com resto.
- (f) Quem sabe dividir com resto sabe inverter.

Os itens (a), (e) e (f) são triviais. O item (b) segue de $mn = ((m+n)^2 - (m-n)^2)/4$. O item (d) segue de $x^2 = (x^{-1} - (x+1)^{-1})^{-1} - x$. O item (c) segue do fato que se $x = n/Q^N \in (1/Q, 1]$ (x um número real

dado com uma certa precisão) e se $y \in [1, Q)$ é uma aproximação para $1/x$ com k casas de precisão então $y' = y(2 - xy)$ é uma aproximação para $1/x$ com aproximadamente $2k$ casas de precisão. De fato temos $y' - 1/x = -x(y - 1/x)^2$ donde $|y' - 1/x| \leq |y - 1/x|^2$. Este algoritmo pode ser visto como uma aplicação do método de Newton para a função $f(t) = -x + 1/t$. Note que as primeiras aproximações para $1/x$ podem ser calculadas com poucos dígitos de precisão, donde as primeiras multiplicações podem ser feitas com poucos dígitos; isto garante que o tempo total para obter N dígitos de $1/x$ é comparável ao tempo de uma multiplicação de inteiros com N dígitos.

7.8 Tabelas

Nesta última seção apresentaremos algumas tabelas indicando alguns dos maiores primos conhecidos no momento da conclusão do livro (24 de Junho de 2013). Estas tabelas se tornam obsoletas rapidamente, então ao leitor recomendamos consultar a página

<http://primes.utm.edu/largest.html>

para uma lista mais atualizada contendo os recordes de primos.

Maiores pares de primos gêmeos conhecidos

Primo	Número de dígitos	Data
$3756801695685 \cdot 2^{666669} \pm 1$	200700	2011
$65516468355 \cdot 2^{333333} \pm 1$	100355	2009
$2003663613 \cdot 2^{195000} \pm 1$	58711	2007
$194772106074315 \cdot 2^{171960} \pm 1$	51780	2007
$100314512544015 \cdot 2^{171960} \pm 1$	51780	2006
$16869987339975 \cdot 2^{171960} \pm 1$	51779	2005
$33218925 \cdot 2^{169690} \pm 1$	51090	2002
$22835841624 \cdot 7^{54321} \pm 1$	45917	2010
$1679081223 \cdot 2^{151618} \pm 1$	45651	2012
$84966861 \cdot 2^{140219} \pm 1$	42219	2012
$12378188145 \cdot 2^{140002} \pm 1$	42155	2010
$23272426305 \cdot 2^{140001} \pm 1$	42155	2010
$8151728061 \cdot 2^{125987} \pm 1$	37936	2010

Maiores primos de Sophie Germain conhecidos

Primo	Número de dígitos	Data
$18543637900515 \cdot 2^{666667} - 1$	200701	2012
$183027 \cdot 2^{265440} - 1$	79911	2010
$648621027630345 \cdot 2^{253824} - 1$	76424	2009
$620366307356565 \cdot 2^{253824} - 1$	76424	2009
$607095 \cdot 2^{176311} - 1$	53081	2009
$48047305725 \cdot 2^{172403} - 1$	51910	2007
$137211941292195 \cdot 2^{171960} - 1$	51780	2006
$31737014565 \cdot 2^{140003} - 1$	42156	2010
$14962863771 \cdot 2^{140001} - 1$	42155	2010
$33759183 \cdot 2^{123458} - 1$	37173	2009
$7068555 \cdot 2^{121301} - 1$	36523	2005
$2540041185 \cdot 2^{114729} - 1$	34547	2003
$1124044292325 \cdot 2^{107999} - 1$	32523	2006

Maiores primos de Mersenne conhecidos

Primo	Número de dígitos	Data
$2^{57885161} - 1$	17425170	2013
$2^{43112609} - 1$	12978189	2008
$2^{42643801} - 1$	12837064	2009
$2^{37156667} - 1$	11185272	2008
$2^{32582657} - 1$	9808358	2006
$2^{30402457} - 1$	9152052	2005
$2^{25964951} - 1$	7816230	2005
$2^{24036583} - 1$	7235733	2004
$2^{20996011} - 1$	6320430	2003
$2^{13466917} - 1$	4053946	2001

Denote por $n\#$ o produto dos primos menores do que ou iguais a n .
 Primos da forma $n\# \pm 1$ são chamados de *primoriais*, enquanto que os

da forma $n! \pm 1$ são chamados de *fatoriais*.

Maiores primos primoriais conhecidos

Primo	Número de dígitos	Data
1098133# - 1	476311	2012
843301# - 1	365851	2010
392113# + 1	169966	2001
366439# + 1	158936	2001
145823# + 1	63142	2000
42209# + 1	18241	1999
24029# + 1	10387	1993
23801# + 1	10273	1993
18523# + 1	8002	1989
15877# - 1	6845	1992
13649# + 1	5862	1987

Maiores primos fatoriais conhecidos

Primo	Número de dígitos	Data
150209! + 1	712355	2011
110059! + 1	507082	2011
103040! - 1	471794	2010
94550! - 1	429390	2010
34790! - 1	142891	2002
26951! + 1	107707	2002
21480! - 1	83727	2001
6917! - 1	23560	1998
6380! + 1	21507	1998
3610! - 1	11277	1993
3507! - 1	10912	1992
1963! - 1	5614	1992
1477! + 1	4042	1984

O maior primo conhecido ao longo da história

Primo	Algarismos	Data	Descobridores
$2^{17} - 1$	6	1588	Cataldi
$2^{19} - 1$	6	1588	Cataldi
$2^{31} - 1$	10	1772	Euler
999999000001	12	1851	Loof
$(2^{59} - 1)/179951$	13	1867	Landry
$(2^{53} + 1)/(3 \cdot 107)$	14	1867	Landry
$2^{127} - 1$	39	1876	Lucas
$(2^{148} + 1)/17$	44	1951	Ferrier
$180(2^{127} - 1)^2 + 1$	79	1951	Miller & Wheeler
$2^{521} - 1$	157	1952	Robinson
$2^{607} - 1$	183	1952	Robinson
$2^{1279} - 1$	386	1952	Robinson
$2^{2203} - 1$	664	1952	Robinson
$2^{2281} - 1$	687	1952	Robinson
$2^{3217} - 1$	969	1957	Riesel
$2^{4423} - 1$	1332	1961	Hurwitz
$2^{9689} - 1$	2917	1963	Gillies
$2^{9941} - 1$	2993	1963	Gillies
$2^{11213} - 1$	3376	1963	Gillies
$2^{19937} - 1$	6002	1971	Tuckerman
$2^{21701} - 1$	6533	1978	Noll & Nickel
$2^{23209} - 1$	6987	1979	Noll
$2^{44497} - 1$	13395	1979	Nelson & Slowinski
$2^{86243} - 1$	25962	1982	Slowinski
$2^{132049} - 1$	39751	1983	Slowinski
$2^{216091} - 1$	65050	1985	Slowinski
$91581 \cdot 2^{216193} - 1$	65087	1989	Amdahl Six ^(*)
$2^{756839} - 1$	227832	1992	Slowinski & Gage
$2^{859433} - 1$	258716	1994	Slowinski & Gage
$2^{1257787} - 1$	378632	1996	Slowinski & Gage
$2^{1398269} - 1$	420921	1996	Armengaud, Woltman, et al.

Primo	Algarismos	Data	Descobridores
$2^{2976221} - 1$	895932	1997	Spence, Woltman, et al.
$2^{3021377} - 1$	909526	1998	Clarkson, Woltman, Kurowski, et al.
$2^{6972593} - 1$	2098960	1999	Hajratwala, Woltman, Kurowski, et al.
$2^{13466917} - 1$	4053946	2001	Cameron, Woltman, Kurowski, et al.
$2^{20996011} - 1$	6320430	2003	Shafer, Woltman, Kurowski, et al.
$2^{24036583} - 1$	7235733	2004	Findley, Woltman, Kurowski, et al.
$2^{25964951} - 1$	7816230	2005	Nowak, Woltman, Kurowski, et al.
$2^{30402457} - 1$	9152052	2005	Cooper, Boone, Woltman, Kurowski, et al.
$2^{32582657} - 1$	9808358	2006	Cooper, Boone, Woltman, Kurowski, et al.
$2^{37156667} - 1$	11185272	2008	Elvenich, Woltman, Kurowski, et al.
$2^{43112609} - 1$	12978189	2008	E. Smith, Woltman, Kurowski, et al.
$2^{57885161} - 1$	17425170	2013	Cooper, Woltman, Kurowski, et al.

(*) O grupo Amdahl Six é formado por J. Brown, C. Noll, B. Parady, G. Smith, J. Smith e S. Zarantonello

Maiores primos conhecidos

Primo	Número de dígitos	Data
$2^{57885161} - 1$	17425170	2013
$2^{43112609} - 1$	12978189	2008
$2^{42643801} - 1$	12837064	2009
$2^{37156667} - 1$	11185272	2008
$2^{32582657} - 1$	9808358	2006
$2^{30402457} - 1$	9152052	2005
$2^{25964951} - 1$	7816230	2005
$2^{24036583} - 1$	7235733	2004
$2^{20996011} - 1$	6320430	2003
$2^{13466917} - 1$	4053946	2001
$19249 \cdot 2^{13018586} + 1$	3918990	2007
$475856^{524288} + 1$	2976633	2012
$356926^{524288} + 1$	2911151	2012
$341112^{524288} + 1$	2900832	2012
$27653 \cdot 2^{9167433} + 1$	2759677	2005
$90527 \cdot 2^{9162167} + 1$	2758093	2010
$75898^{524288} + 1$	2558647	2011
$28433 \cdot 2^{7830457} + 1$	2357207	2004
$3 \cdot 2^{7033641} + 1$	2117338	2011
$33661 \cdot 2^{7031232} + 1$	2116617	2007
$2^{6972593} - 1$	2098960	1999
$6679881 \cdot 2^{6679881} + 1$	2010852	2009
$1582137 \cdot 2^{6328550} + 1$	1905090	2009
$3 \cdot 2^{6090515} - 1$	1833429	2010
$7 \cdot 2^{5775996} + 1$	1738749	2012
$252191 \cdot 2^{5497878} - 1$	1655032	2012
$258317 \cdot 2^{5450519} + 1$	1640776	2008
$773620^{262144} + 1$	1543643	2012
$3 \cdot 2^{5082306} + 1$	1529928	2009
$676754^{262144} + 1$	1528413	2012
$5359 \cdot 2^{5054502} + 1$	1521561	2003
$525094^{262144} + 1$	1499526	2012
$265711 \cdot 2^{4858008} + 1$	1462412	2008
$1271 \cdot 2^{4850526} - 1$	1460157	2012
$361658^{262144} + 1$	1457075	2011

Primo	Número de dígitos	Data
$9 \cdot 2^{4683555} - 1$	1409892	2012
$121 \cdot 2^{4553899} - 1$	1370863	2012
$145310^{262144} + 1$	1353265	2011
$353159 \cdot 2^{4331116} - 1$	1303802	2011
$141941 \cdot 2^{4299438} - 1$	1294265	2011
$15 \cdot 2^{4246384} + 1$	1278291	2013
$3 \cdot 2^{4235414} - 1$	1274988	2008
$191 \cdot 2^{4203426} - 1$	1265360	2012
$40734^{262144} + 1$	1208473	2011
$9 \cdot 2^{4005979} - 1$	1205921	2012
$27 \cdot 2^{3855094} - 1$	1160501	2012
$24518^{262144} + 1$	1150678	2008
$123547 \cdot 2^{3804809} - 1$	1145367	2011
$415267 \cdot 2^{3771929} - 1$	1135470	2011
$11 \cdot 2^{3771821} + 1$	1135433	2013
$938237 \cdot 2^{3752950} - 1$	1129757	2007
$65531 \cdot 2^{3629342} - 1$	1092546	2011
$485767 \cdot 2^{3609357} - 1$	1086531	2008
$5 \cdot 2^{3569154} - 1$	1074424	2009
$1019 \cdot 2^{3536312} - 1$	1064539	2012
$7 \cdot 2^{3511774} + 1$	1057151	2008
$428639 \cdot 2^{3506452} - 1$	1055553	2011
$9 \cdot 2^{3497442} + 1$	1052836	2012
$1273 \cdot 2^{3448551} - 1$	1038121	2012
$191249 \cdot 2^{3417696} - 1$	1028835	2010
$59 \cdot 2^{3408416} - 1$	1026038	2010
$81 \cdot 2^{3352924} + 1$	1009333	2012
$1087 \cdot 2^{3336385} - 1$	1004355	2012
$464253 \cdot 2^{3321908} - 1$	1000000	2013
$191273 \cdot 2^{3321908} - 1$	1000000	2013
$3139 \cdot 2^{3321905} - 1$	999997	2008
$4847 \cdot 2^{3321063} + 1$	999744	2005
$223 \cdot 2^{3264459} - 1$	982703	2012
$9 \cdot 2^{3259381} - 1$	981173	2011
$211195 \cdot 2^{3224974} + 1$	970820	2013
$94373 \cdot 2^{3206717} + 1$	965323	2013
$113983 \cdot 2^{3201175} - 1$	963655	2008
$1087 \cdot 2^{3164677} - 1$	952666	2012

Primo	Número de dígitos	Data
$15 \cdot 2^{3162659} + 1$	952057	2012
$19 \cdot 2^{3155009} - 1$	949754	2012
$3 \cdot 2^{3136255} - 1$	944108	2007
$1019 \cdot 2^{3103680} - 1$	934304	2012
$5 \cdot 2^{3090860} - 1$	930443	2012
$21 \cdot 2^{3065701} + 1$	922870	2012
$5 \cdot 2^{3059698} - 1$	921062	2008
$383731 \cdot 2^{3021377} - 1$	909531	2011
$2^{3021377} - 1$	909526	1998
$7 \cdot 2^{3015762} + 1$	907836	2008
$43 \cdot 2^{2994958} + 1$	901574	2013
$1095 \cdot 2^{2992587} - 1$	900862	2011
$15 \cdot 2^{2988834} + 1$	899730	2012
$39 \cdot 2^{2978894} + 1$	896739	2013
$4348099 \cdot 2^{2976221} - 1$	895939	2008
$2^{2976221} - 1$	895932	1997
$198677 \cdot 2^{2950515} + 1$	888199	2012
$17 \cdot 2^{2946584} - 1$	887012	2013
$25 \cdot 2^{2927222} + 1$	881184	2013
$7 \cdot 2^{2915954} + 1$	877791	2008
$427194 \cdot 113^{427194} + 1$	877069	2012
$63 \cdot 2^{2898957} + 1$	872675	2013
$11 \cdot 2^{2897409} + 1$	872209	2013
$51 \cdot 2^{2881227} + 1$	867338	2013
$1207 \cdot 2^{2861901} - 1$	861522	2011
$222361 \cdot 2^{2854840} + 1$	859398	2006
$177 \cdot 2^{2816050} + 1$	847718	2012
$96 \cdot 10^{846519} - 1$	846521	2011
$63 \cdot 2^{2807130} + 1$	845033	2013
$43 \cdot 2^{2795582} + 1$	841556	2013
$15 \cdot 2^{2785940} + 1$	838653	2012
$57 \cdot 2^{2765963} + 1$	832640	2013
$57 \cdot 2^{2747499} + 1$	827082	2013
$17 \cdot 2^{2721830} - 1$	819354	2010
$165 \cdot 2^{2717378} - 1$	818015	2012
$45 \cdot 2^{2711732} + 1$	816315	2012

Capítulo 8

Aproximações Diofantinas

Neste capítulo, veremos alguns resultados da chamada teoria de aproximações diofantinas. Já vimos alguns resultados desta teoria quando estudamos frações contínuas. Os resultados deste capítulo complementam aquele estudo.

8.1 Teoria Métrica das Aproximações Diofantinas

O problema básico da teoria de aproximações diofantinas é o de estudar boas aproximações de números reais por números racionais. A principal técnica utilizada são as frações contínuas, que fornecem todas as boas aproximações de um irracional α por racionais.

Dado um número irracional α , um resultado clássico de Dirichlet (que já provamos usando frações contínuas, ver o teorema 3.11) afirma que existem infinitos racionais $\frac{p}{q}$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$. Vejamos outra prova simples (c.f. exemplo 0.10): dado $N \in \mathbb{N}$, consideramos os $N + 1$ elementos de $[0, 1)$ da forma $\{j\alpha\} \stackrel{\text{def}}{=} j\alpha - \lfloor j\alpha \rfloor$ (parte fracionária de $j\alpha$), com $0 \leq j \leq N$. Como $[0, 1) = \bigcup_{k=0}^{N-1} [\frac{k}{N}, \frac{k+1}{N})$, existem dois desses elementos, digamos $\{j_1\alpha\}$ e $\{j_2\alpha\}$ num mesmo intervalo $[\frac{k}{N}, \frac{k+1}{N})$ e, portanto, se $j_1 < j_2$, $q = j_2 - j_1$ e $p = \lfloor j_2\alpha \rfloor - \lfloor j_1\alpha \rfloor$, temos

$$0 < |q\alpha - p| < \frac{1}{N} \implies \left| \alpha - \frac{p}{q} \right| < \frac{1}{qN} \leq \frac{1}{q^2}.$$

Hurwitz e Markov provaram (teorema 3.13) que de fato $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$

tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$, para todo irracional α , e que $\sqrt{5}$ é a maior constante com essa propriedade. Markov provou que, para todo $c > 3$, o conjunto dos $\alpha \in \mathbb{R}$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{cq^2}$ tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$ é enumerável, mas o conjunto dos $\alpha \in \mathbb{R}$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{3q^2}$ tem apenas um número finito de soluções tem o mesmo cardinal que \mathbb{R} .

Nosso propósito é estudar desigualdades do tipo

$$\left| \alpha - \frac{p}{q} \right| < \frac{f(q)}{q}, \quad (1)$$

onde $f: \mathbb{N} \rightarrow \mathbb{R}^+$ é uma função decrescente, do ponto de vista da teoria da medida. Vamos provar o teorema de Khintchine, segundo o qual, se $\sum_{q=1}^{\infty} f(q) = +\infty$ então (1) tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$, para quase todo $\alpha \in \mathbb{R}$, mas se $\sum_{q=1}^{\infty} f(q) < +\infty$ então (1) tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$, para quase todo $\alpha \in \mathbb{R}$.

Note que do ponto de vista topológico a situação é diferente: qualquer que seja a função positiva f , (1) tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$ para $\alpha \in R_f$, onde R_f é um conjunto residual, i.e., contém (de fato é) uma interseção enumerável de abertos densos.

Uma extensão natural dos problemas acima é o estudo de aproximações simultâneas de n números reais por números racionais com o mesmo denominador: dados $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{R}$ queremos encontrar números racionais $\frac{p_1}{q}, \frac{p_2}{q}, \dots, \frac{p_n}{q}$ tais que $|\alpha_i - \frac{p_i}{q}|$ seja pequeno para todo $i \leq n$. Em geral, sempre é possível encontrar racionais tais que $|\alpha_i - \frac{p_i}{q}| < \frac{1}{q^{1+1/n}}$, o que estende o teorema de Dirichlet e pode ser provado de modo análogo: dado $N \in \mathbb{N}$ consideramos os $N^n + 1$ pontos

$$x_j = (\alpha_1 j - [\alpha_1 j], \alpha_2 j - [\alpha_2 j], \dots, \alpha_n j - [\alpha_n j]), \quad 0 \leq j \leq N^n$$

no hipercubo $[0, 1)^n$. Dividimos $[0, 1)^n$ em N^n cubos de lado $\frac{1}{N}$. Haverá necessariamente dois pontos x_{j_1} e x_{j_2} num mesmo cubo dessa decomposição, e, se $j_1 < j_2$, $q = j_2 - j_1$, $p_i = [j_2 \alpha_i] - [j_1 \alpha_i]$, teremos $|\alpha_i - \frac{p_i}{q}| < \frac{1}{Nq} \leq \frac{1}{q^{1+1/n}}$, para todo $i \leq n$.

Infelizmente não há um substituto satisfatório para a teoria de frações contínuas em dimensão maior que um, mas é possível provar uma versão n -dimensional do teorema de Khintchine (provada originalmente em [79]), o que faremos mais adiante.

Para maiores informações sobre aproximações diofantinas, veja [28] e [128].

8.2 Aproximações Não-Homogêneas

Vejam alguns resultados sobre a distribuição das partes fracionárias de um múltiplo de um irracional α . O primeiro destes resultados é a seguinte

Proposição 8.1. *Se $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ então $Y = \{m + n\alpha \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$ é denso em \mathbb{R} .*

DEMONSTRAÇÃO: Seja $X = \{m + n\alpha \mid m, n \in \mathbb{Z}\}$. Vamos provar inicialmente que X é denso em \mathbb{R} . Dado $\varepsilon > 0$ existem p, q inteiros com $p, q > 1/\varepsilon$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{q^2} \implies 0 < |q\alpha - p| < \frac{1}{q} < \varepsilon$. Dado $x \in \mathbb{R}$ existe $k \in \mathbb{Z}$ tal que x está entre $k(q\alpha - p)$ e $(k+1)(q\alpha - p)$, donde $|x - k(q\alpha - p)| \leq \varepsilon$. Como $k(q\alpha - p) = -pk + qk\alpha \in X$, o resultado está provado.

Seja agora $\beta \in \mathbb{R}$. Como X é denso em \mathbb{R} , dado $\varepsilon > 0$ existem $m, n \in \mathbb{Z}$ com $|\beta - (m + n\alpha)| < \varepsilon/2$. Por outro lado, existem p, q inteiros com $q > |n|$ tais que $|q\alpha - p| < \varepsilon/2$ (note que, se q é negativo, $|q| > |n|$ e $|q\alpha - p| < \varepsilon/2$, podemos trocar q por $-q$ e p por $-p$: teremos $-q = |q| > |n|$ e $|(-q)\alpha - (-p)| = |q\alpha - p| < \varepsilon/2$). Assim, $n + q \in \mathbb{N}$ e $|\beta - ((m-p) + (n+q)\alpha)| < |\beta - (m+n\alpha)| + |q\alpha - p| < \varepsilon/2 + \varepsilon/2 = \varepsilon$. \square

Exemplo 8.2. *Mostre que existe uma potência de 2 que se inicia com 2009 quando escrito na base decimal.*

SOLUÇÃO: Temos que 2^k começa com 2009 se existe n natural tal que $2009 \cdot 10^n \leq 2^k < 2010 \cdot 10^n$. Tomando logaritmos na base 10, obtemos

$$n + 3 + \log_{10} 2,009 \leq k \log_{10} 2 < n + 3 + \log_{10} 2,010$$

O problema portanto se reduz a encontrar um k inteiro tal que a parte fracionária de $k \log_{10} 2$ esteja entre $\log_{10} 2,009$ e $\log_{10} 2,010$. Isto é possível pelo teorema anterior pois $\log_{10} 2$ é irracional: se $p, q \in \mathbb{N}$ são tais que $p/q = \log_{10} 2$ então $10^p = 2^q$, o que é impossível pelo teorema fundamental da aritmética.

\square

O próximo resultado, devido a Kronecker, estende a proposição anterior para dimensão qualquer.

Proposição 8.3 (Kronecker). *Seja $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n$. Suponha que $1, \alpha_1, \dots, \alpha_n$ sejam linearmente independentes sobre \mathbb{Q} , isto é, $k + m_1\alpha_1 + m_2\alpha_2 + \dots + m_n\alpha_n = 0$ com $k, m_1, \dots, m_n \in \mathbb{Z}$ implica $k = m_1 = \dots = m_n = 0$. Então*

$$Y = \{k\alpha + m_1e_1 + m_2e_2 + \dots + m_ne_n \mid k \in \mathbb{N}, m_1, \dots, m_n \in \mathbb{Z}\}$$

é denso em \mathbb{R}^n , onde $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ são os elementos da base canônica de \mathbb{R}^n .

DEMONSTRAÇÃO: Seja

$$X = \{k\alpha + m_1e_1 + m_2e_2 + \dots + m_ne_n \mid k, m_1, \dots, m_n \in \mathbb{Z}\}$$

e seja $\overline{X} \subset \mathbb{R}^n$ o fecho de X , e $V \subset \overline{X}$ um subespaço vetorial maximal de \mathbb{R}^n contido em \overline{X} . Suponhamos por absurdo que $V \neq \mathbb{R}^n$.

Seja V^\perp o complemento ortogonal de V , e seja $\pi: \mathbb{R}^n \rightarrow V^\perp$ a projeção ortogonal sobre V^\perp . Para todo $x \in \overline{X}$, $\pi(x) \in \overline{X}$, pois $\pi(x) = x + (\pi(x) - x)$, $\pi(x) - x \in V \subset \overline{X}$ e \overline{X} é invariante por adição (pois X também é).

Seja $k = \dim V^\perp$. Escolhemos vetores $e_{i_1}, e_{i_2}, \dots, e_{i_k}$ de tal maneira que $\pi(e_{i_1}), \pi(e_{i_2}), \dots, \pi(e_{i_k})$ geram V^\perp . Se fizermos $e_0 = \alpha$, para todo $i = 0, 1, \dots, n$ escrevemos $\pi(e_i) = \sum_{j=1}^k \lambda_{ij} \pi(e_{i_j})$. Não podemos ter $\lambda_{i1} \in \mathbb{Q}$ para todo i , senão podemos definir um funcional linear f da seguinte forma: dado $x \in \mathbb{R}^n$ escrevemos $\pi(x)$ como $\sum_{j=1}^k \beta_j \pi(e_{i_j})$, e tomamos $f(x) = \beta_1$. Se $\lambda_{i1} = f(e_i) \in \mathbb{Q}$ para todo i , teríamos

$$\lambda_{01} = f(\alpha) = \sum_{i=1}^n \alpha_i f(e_i) = \sum_{i=1}^n \lambda_{i1} \alpha_i \in \mathbb{Q},$$

contradizendo a hipótese da proposição.

Seja então i_0 tal que $\lambda_{i_0 1} \notin \mathbb{Q}$. Tomamos $\gamma = (\lambda_{i_0 1}, \dots, \lambda_{i_0 k}) \in \mathbb{R}^k$. Pelo teorema de Dirichlet multidimensional, existem

$$x_m = q_m \gamma - (p_{1m}, p_{2m}, \dots, p_{km}) \neq 0$$

com $q_m, p_{1m}, \dots, p_{km} \in \mathbb{Z}$ e $\lim_{m \rightarrow \infty} |x_m| \leq \lim_{m \rightarrow \infty} |q_m|^{-1/k} = 0$, e portanto, se

$$w_m \stackrel{\text{def}}{=} q_m \pi(e_{i_0}) - \sum_{j=1}^k p_{jm} \pi(e_{i_j}) \in \overline{X} \cap V^\perp,$$

$\lim_{m \rightarrow \infty} w_m = 0$ (e $w_m \neq 0$, $\forall m$). Como a esfera unitária $S^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1\}$ é compacta, passando a uma subsequência, se necessário, podemos supor que $\lim_{m \rightarrow \infty} \frac{w_m}{|w_m|} = \tilde{w} \in S^{n-1}$. Para todo $t \in \mathbb{R}$, temos que

$$t\tilde{w} = \lim_{m \rightarrow \infty} \left\lfloor \frac{t}{|w_m|} \right\rfloor w_m \in \overline{X} \quad \forall m \in \mathbb{N}.$$

Portanto, como \overline{X} é invariante por adição, o subespaço $\tilde{V} = \{v + t\tilde{w} \mid v \in V, t \in \mathbb{R}\}$ é tal que $\tilde{V} \subset \overline{X}$ e \tilde{V} contém propriamente V , absurdo.

Finalmente, para concluir que Y é denso a partir do fato de que X é denso, dados $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{R}^n$ e $\varepsilon > 0$, existem $k, m_1, \dots, m_n \in \mathbb{Z}$ com $|\beta - (k\alpha + m_1e_1 + m_2e_2 + \dots + m_ne_n)| < \varepsilon/2$. Também existem $q > |k|, p_1, p_2, \dots, p_n$ inteiros tais que $|q\alpha + p_1e_1 + p_2e_2 + \dots + p_ne_n| < \varepsilon/2$. Temos então $q + k \in \mathbb{N}$ e

$$\begin{aligned} & |\beta - ((q + k)\alpha + (p_1 + m_1)e_1 + (p_2 + m_2)e_2 + \dots + (p_n + m_n)e_n)| < \\ & |\beta - (k\alpha + m_1e_1 + m_2e_2 + \dots + m_ne_n)| + |q\alpha + p_1e_1 + p_2e_2 + \dots + p_ne_n| < \\ & \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned} \quad \square$$

Observação 8.4. A hipótese da proposição 8.3 é necessária, pois se existem inteiros k, m_1, \dots, m_n não todos nulos tais que $k + m_1\alpha_1 + \dots + m_n\alpha_n = 0$ então

$$\overline{X} \subset \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid m_1x_1 + m_2x_2 + \dots + m_nx_n \in \mathbb{Z}\},$$

que é um fechado com interior vazio.

O teorema de Kronecker possui a seguinte generalização, devida a Weyl. Antes necessitamos de uma

Definição 8.5. Uma sequência $(a_n)_{n \geq 0}$ com $a_n \in [0, 1]^d$ é dita uniformemente distribuída se para qualquer paralelepípedo retangular $C \subset [0, 1]^d$, temos

$$\lim_{n \rightarrow \infty} \frac{\#\{j \mid 1 \leq j \leq n \text{ e } a_j \in C\}}{n} = m(C),$$

onde $m(C)$ é o volume de C .

Observação 8.6. Caso uma sequência $(a_n)_{n \geq 0}$ com $a_n \in [0, 1]^d$ seja uniformemente distribuída, então a propriedade da definição valerá não somente para paralelepípedos retangulares, mas também para qualquer conjunto $C \subset [0, 1]^d$ com volume (à la Riemann) bem definido (o que requer que o conjunto seja J -mensurável, i.e., que sua fronteira tenha medida nula).

Teorema 8.7 (Weyl). Seja $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{R}^d$ onde as coordenadas são tais que $1, \alpha_1, \dots, \alpha_d$ são linearmente independentes sobre \mathbb{Q} . Então a sequência

$$\{n\alpha\} \stackrel{\text{def}}{=} (n\alpha_1 - \lfloor n\alpha_1 \rfloor, \dots, n\alpha_d - \lfloor n\alpha_d \rfloor)$$

é uniformemente distribuída no cubo $[0, 1]^d$.

DEMONSTRAÇÃO: Sejam $C_1, C_2 \subset [0, 1)^d$ dois cubos abertos tais que o lado de C_2 é menor que o lado de C_1 . Então o fecho \overline{C}_2 de C_2 está contido em um transladado de C_1 ($\overline{C}_2 \subset C_1 + v$, $\exists v \in \mathbb{R}^d$). Como existem vetores \tilde{v} arbitrariamente próximos de v , com $\tilde{v} = (q\alpha_1 + p_1, \dots, q\alpha_d + p_d)$, $q, p_1, \dots, p_d \in \mathbb{Z}$, tomando um tal \tilde{v} de modo que sua distância a v seja menor que a distância de \overline{C}_2 à fronteira de $C_1 + v$, temos que

$$\{m\alpha\} \in \overline{C}_2 \implies \{(m - q)\alpha\} \in \overline{C}_2 - \tilde{v} \subset C_1.$$

Se definirmos, para cada paralelepípedo retangular C , $\mathcal{N}(n, \alpha, C) := \#\{j \mid 1 \leq j \leq n \text{ e } \{j\alpha\} \in C\}$, teremos então $\mathcal{N}(n, \alpha, C_2) \leq \mathcal{N}(n, \alpha, C_1) + |q|$ para todo $n \in \mathbb{N}$.

Seja então N um número natural grande dado e C um cubo dado de lado $\frac{1}{N}$. Considere a decomposição $[0, 1)^d = \left(\bigcup_{k=0}^N \left[\frac{k}{N+1}, \frac{k+1}{N+1} \right) \right)^d$ como

a união de $(N+1)^d$ cubos de lado $\frac{1}{N+1}$. Seja \mathcal{C} a coleção desses cubos. Para cada cubo $\tilde{C} \in \mathcal{C}$ dessa coleção, existe um inteiro $q^{(\tilde{C})}$ tal que $\mathcal{N}(n, \alpha, \tilde{C}) \leq \mathcal{N}(n, \alpha, C) + |q^{(\tilde{C})}|$ para todo $n \in \mathbb{N}$. Se \hat{q} é o máximo dos números $|q^{(\tilde{C})}|$, podemos usar o fato de que, para todo $n \in \mathbb{N}$, existe um cubo $\tilde{C} \in \mathcal{C}$ com $\mathcal{N}(n, \alpha, \tilde{C}) \geq \frac{n}{(N+1)^d}$ para concluir que $\mathcal{N}(n, \alpha, C) \geq \frac{n}{(N+1)^d} - \hat{q}$, $\forall n \in \mathbb{N}$, de onde obtemos $\liminf_{n \rightarrow \infty} \mathcal{N}(n, \alpha, C)/n \geq \frac{1}{(N+1)^d}$.

Analogamente, considerando a decomposição

$$[0, 1)^d = \left(\bigcup_{k=0}^{N-2} \left[\frac{k}{N-1}, \frac{k+1}{N-1} \right) \right)^d$$

como a união de $(N-1)^d$ cubos de lado $\frac{1}{N-1}$, podemos provar que $\limsup_{n \rightarrow \infty} \mathcal{N}(n, \alpha, C)/n \leq \frac{1}{(N-1)^d}$.

Seja agora $B = \prod_{i=1}^d [a_i, b_i)$ um paralelepípedo retangular dado. Para cada número natural grande N , B contém uma união disjunta de $\prod_{i=1}^d \lfloor N(b_i - a_i) \rfloor$ cubos de lado $1/N$. Assim, da discussão acima, segue que

$$\begin{aligned} \liminf_{n \rightarrow \infty} \frac{\mathcal{N}(n, \alpha, B)}{n} &\geq \frac{1}{(N+1)^d} \prod_{i=1}^d \lfloor N(b_i - a_i) \rfloor \\ &\geq \left(\frac{N}{N+1} \right)^d \prod_{i=1}^d \left(b_i - a_i - \frac{1}{N} \right), \end{aligned}$$

e, fazendo N tender a infinito, obtemos

$$\liminf_{n \rightarrow \infty} \frac{\mathcal{N}(n, \alpha, B)}{n} \geq \prod_{i=1}^d (b_i - a_i) = m(B).$$

Por outro lado, B está contido numa união de $\prod_{i=1}^d \lceil N(b_i - a_i) \rceil$ cubos de lado $1/N$, donde, pela discussão acima,

$$\begin{aligned} \limsup_{n \rightarrow \infty} \frac{\mathcal{N}(n, \alpha, B)}{n} &\geq \frac{1}{(N-1)^d} \prod_{i=1}^d \lceil N(b_i - a_i) \rceil \\ &\geq \left(\frac{N}{N-1} \right)^d \prod_{i=1}^d (b_i - a_i + 1/N), \end{aligned}$$

e, fazendo N tender a infinito, obtemos

$$\limsup_{n \rightarrow \infty} \mathcal{N}(n, \alpha, B)/n \leq \prod_{i=1}^d (b_i - a_i) = m(B).$$

Portanto $\lim_{n \rightarrow \infty} \mathcal{N}(n, \alpha, B)/n = \prod_{i=1}^d (b_i - a_i) = m(B)$. \square

Observação 8.8. *É possível provar o teorema anterior com técnicas de análise de Fourier. Dizemos que uma sequência $(w_n)_{n \geq 0}$ com $w_n \in \mathbb{R}^d$ é dita uniformemente distribuída módulo 1 se $(\{w_n\})_{n \geq 0}$ é uniformemente distribuída em $[0, 1]^d$, onde, para $w = (w_1, w_2, \dots, w_d) \in \mathbb{R}^d$, $\{w\} := (\{w_1\}, \{w_2\}, \dots, \{w_d\})$. É possível provar que $(w_n)_{n \geq 0}$ é uniformemente distribuída módulo 1 se, e somente se, para todo vetor $v \in \mathbb{Z}^d$ com $v \neq (0, 0, \dots, 0)$,*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{1 \leq j \leq n} \exp(2\pi i \langle w_n, v \rangle) = 0$$

(onde $\langle u, v \rangle$ denota o produto interno dos vetores u e v). Não é difícil verificar esta condição para a sequência $w_n = n\alpha$, onde $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{R}^d$ é tal que $1, \alpha_1, \dots, \alpha_d$ são linearmente independentes sobre \mathbb{Q} .

Esta caracterização de sequências uniformemente distribuídas módulo 1 pode ser usada para provar o seguinte fato: uma condição suficiente (mas não necessária) para que uma sequência $(w_n)_{n \geq 0}$ com $w_n \in \mathbb{R}$ seja uniformemente distribuída módulo 1 é que, para todo inteiro positivo h , a sequência $(w_{n+h} - w_n)_{n \in \mathbb{N}}$ seja uniformemente distribuída. Este fato, por sua vez, pode ser usado para provar (por indução no grau) que, para todo polinômio $p(x) = \alpha_d x^d + \alpha_{d-1} x^{d-1} + \dots + \alpha_0$ que tenha algum coeficiente não constante $\alpha_j, j \geq 1$ irracional, a sequência $(p(n))_{n \in \mathbb{N}}$ é uniformemente distribuída módulo 1.

Vea o capítulo IV de [28] ou [145], páginas 105-113 para mais detalhes.

8.3 O Teorema de Khintchine

8.3.1 O Caso Unidimensional

Teorema 8.9 (Khintchine). *Seja $f: \mathbb{N} \rightarrow \mathbb{R}^+$ uma função decrescente tal que $h(n) = nf(n): \mathbb{N} \rightarrow \mathbb{R}^+$ também seja decrescente.*

- (a) *Se $\sum_{n=1}^{\infty} f(n) < +\infty$ então a equação $|\alpha - \frac{p}{q}| < \frac{f(q)}{q}$ tem apenas um número finito de soluções racionais p/q , para quase todo $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*
- (b) *Se $\sum_{n=1}^{\infty} f(n) = +\infty$ então a equação $|\alpha - \frac{p}{q}| < \frac{f(q)}{q}$ tem um número infinito de soluções racionais p/q , para quase todo $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*

Observação 8.10. *A condição de $nf(n)$ ser decrescente não é de fato necessária, como veremos mais adiante, mas simplifica a prova. Por outro lado, não podemos retirar a hipótese de f ser decrescente (veja [29]).*

Antes de proceder com a demonstração do teorema de Khintchine, precisamos dos seguintes lemas.

Lema 8.11. *Sejam $n, k \in \mathbb{N}$, e seja $\alpha = [0; a_1, a_2, \dots]$ a expansão de um número $\alpha \in [0, 1)$ como fração contínua. A probabilidade de um termo a_{n+1} ser igual a k dado que $a_1 = k_1, a_2 = k_2, \dots, a_n = k_n$ está entre $1/(k+1)(k+2)$ e $2/k(k+1)$, $\forall k_1, k_2, \dots, k_n \in \mathbb{N}_{>0}$.*

DEMONSTRAÇÃO: Considere as convergentes

$$\frac{p_{n-1}}{q_{n-1}} = [0; a_1, a_2, \dots, a_{n-1}] \quad \text{e} \quad \frac{p_n}{q_n} = [0; a_1, a_2, \dots, a_{n-1}, a_n]$$

Se $\alpha \in [0, 1)$, escrevendo $\alpha = [0; a_1, a_2, \dots, a_n, \alpha_{n+1}]$ com $\alpha_{n+1} \in [1, +\infty)$ então $\alpha \in \left[\frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{p_n}{q_n} \right)$, e além disso

$$a_{n+1} = k \implies \alpha \in \left[\frac{kp_n + p_{n-1}}{kq_n + q_{n-1}}, \frac{(k+1)p_n + p_{n-1}}{(k+1)q_n + q_{n-1}} \right),$$

e valem as recíprocas (as ordens dos extremos dos intervalos podem estar trocadas). Os comprimentos dos referidos intervalos são, respectivamente, $\frac{1}{q_n(q_n + q_{n-1})}$ e $\frac{1}{(kq_n + q_{n-1})((k+1)q_n + q_{n-1})}$ (pois $|p_n q_{n-1} - p_{n-1} q_n| = 1$)

e portanto a razão entre seus comprimentos é

$$\frac{q_n(q_n + q_{n-1})}{(kq_n + q_{n-1})((k+1)q_n + q_{n-1})} = \frac{1 + \bar{\alpha}}{(k + \bar{\alpha})(k + 1 + \bar{\alpha})},$$

onde $\bar{\alpha} = q_{n-1}/q_n \in [0, 1]$. Portanto a razão pertence a $[1/(k+1)(k+2), 2/k(k+1)]$. \square

Como $\sum_{j \geq k} \frac{1}{(j+1)(j+2)} = \frac{1}{k+1}$ e $\sum_{j \geq k} \frac{2}{j(j+1)} = \frac{2}{k}$, obtemos o seguinte

Corolário 8.12. *A probabilidade de $a_{n+1} \geq k$, nos termos do lema acima, pertence a $[1/(k+1), 2/k]$.*

Lema 8.13. *Para quase todo $\alpha \in \mathbb{R}$ existe $c \in \mathbb{R}$ tal que $q_n \leq c^n$, para todo $n \in \mathbb{N}$.*

Antes de provar o lema vamos mostrar como termina a prova do teorema de KHintchine.

DEMONSTRAÇÃO: (DO TEOREMA DE KHintCHINE)

Observe inicialmente que podemos supor sem perda de generalidade que $\alpha \in [0, 1]$. Note ainda que $|\alpha - \frac{p}{q}| < \frac{f(q)}{q}$ tem infinitas soluções racionais p/q se, e somente se, existem infinitas convergentes p_n/q_n de α tais que $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$. De fato, se $\frac{p}{q}$ satisfaz a desigualdade acima e $q_n \leq q < q_{n+1}$ então pelo teorema 3.15 temos

$$\left| \alpha - \frac{p_n}{q_n} \right| \leq \frac{q}{q_n} \left| \alpha - \frac{p}{q} \right| < \frac{q}{q_n} \cdot \frac{f(q)}{q} \leq \frac{f(q_n)}{q_n}.$$

(a) Suponhamos agora que $\sum f(n) < \infty$ e seja $\gamma = \frac{1+\sqrt{5}}{2}$. Se a aproximação p_n/q_n de α é tal que $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$ então pela proposição 3.4 temos (na notação da proposição)

$$\begin{aligned} \frac{1}{(\alpha_{n+1} + \beta_{n+1})q_n^2} &= \left| \alpha - \frac{p_n}{q_n} \right| < \frac{f(q_n)}{q_n} \\ \implies a_{n+1} + 2 &> \alpha_{n+1} + \beta_{n+1} > \frac{1}{q_n f(q_n)}. \end{aligned}$$

Por outro lado, temos que $q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2}$ e por indução temos facilmente que $q_n \geq \gamma^{n-1}$, $\forall n \in \mathbb{N}$. Como $n f(n)$ é decrescente, temos portanto que $a_{n+1} + 2 > \frac{1}{\gamma^{n-1} f(\gamma^{n-1})}$, logo $a_{n+1} > A(n)$

onde $A(n) = \frac{1}{\gamma^{n-1}f(\gamma^{n+1})} - 2$. Assim, para mostrar que há somente um número finito de convergentes tais que $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$ para quase todo α , basta mostrar que com probabilidade total $a_{n+1} \leq A(n)$ para todo n suficientemente grande.

Pelo corolário 8.12, a probabilidade de $a_{n+1} \leq A(n)$ é pelo menos $1 - \frac{2}{A(n)}$, para todo $n \in \mathbb{N}$, e a hipótese de $\sum_{n=1}^{\infty} f(n) < \infty$ implica que $\sum_{n=1}^{\infty} \frac{2}{A(n)} < \infty$, por comparação com

$$\sum_{k=1}^{\infty} \gamma^k f(\gamma^k) = \frac{\gamma}{\gamma-1} \sum_{k=0}^{\infty} (\gamma^{k+1} - \gamma^k) f(\gamma^{k+1}) \leq \frac{\gamma}{\gamma-1} \sum_{n=1}^{\infty} f(n) < +\infty.$$

Temos portanto $\prod_{n=1}^{\infty} (1 - \frac{2}{A(n)}) > 0$, logo para cada $\varepsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que $\prod_{n=n_0}^{\infty} (1 - \frac{2}{A(n)}) > 1 - \varepsilon$, donde a proporção dos números α para os quais $a_{n+1} \leq A(n)$ para todo n suficientemente grande é maior do que $1 - \varepsilon$. Como $\varepsilon > 0$ é arbitrário, o resultado segue.

(b) Suponhamos agora que $\sum f(n) = +\infty$, fixemos $c > 0$ e vamos nos restringir ao conjunto X_c dos $\alpha \in [0, 1]$ tais que $q_n < c^n$ para todo $n \in \mathbb{N}$ (a união dos conjuntos X_c para todo $c \in \mathbb{N}$ tem probabilidade total em $[0, 1]$, pelo lema anterior).

Se $a_{n+1} > \frac{1}{q_n f(q_n)}$ então α pertence ao intervalo cujos extremos são $\frac{p_n}{q_n}$ e $\frac{\frac{1}{q_n f(q_n)} p_n + p_{n-1}}{\frac{1}{q_n f(q_n)} q_n + q_{n-1}}$ donde $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$. Como $q_n < c^n$, $\frac{1}{q_n f(q_n)} < \frac{1}{c^n f(c^n)}$. Vamos mostrar que com probabilidade total temos $a_{n+1} \geq \frac{1}{c^n f(c^n)}$ para infinitos valores de $n \in \mathbb{N}$. Isso segue do corolário 8.12 e de $\prod_{n=1}^{\infty} \left(1 - \frac{1}{B(n)+1}\right) = 0$, onde $B(n) = \frac{1}{c^n f(c^n)}$, que por sua vez segue de

$$\sum_{n=1}^{\infty} c^n f(c^n) \geq c^{-1} \sum_{n=1}^{\infty} (c^{n+1} - c^n) f(c^n) \geq c^{-1} \sum_{n=1}^{\infty} f(n) = +\infty.$$

Portanto, para todo $n_0 \in \mathbb{N}$, temos $\prod_{n=n_0}^{\infty} \left(1 - \frac{1}{B(n)+1}\right) = 0$, e, com probabilidade total, existe $n \geq n_0$ com $a_{n+1} \geq \frac{1}{c^n f(c^n)}$, donde a equação $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$ é satisfeita com probabilidade total para infinitos valores de $n \in \mathbb{N}$. \square

DEMONSTRAÇÃO: (DO LEMA)

Sejam $n, k \in \mathbb{N}$. A probabilidade de que k apareça pelo menos $4n/k(k+1)$ vezes entre a_1, a_2, \dots, a_n é limitada por $\sum_{j=sn}^n \binom{n}{j} \left(\frac{s}{2}\right)^j \left(1 - \frac{s}{2}\right)^{n-j}$, onde $s = \frac{4}{k(k+1)}$. Este número, por sua vez, é menor que $\left(\frac{3}{4}\right)^{\frac{n}{k(k+1)}}$ para $\frac{n}{k(k+1)}$ grande: de fato, se $j \geq \frac{3sn}{4}$,

$$\frac{\binom{n}{j+1} \left(\frac{s}{2}\right)^{j+1} \left(1 - \frac{s}{2}\right)^{n-j-1}}{\binom{n}{j} \left(\frac{s}{2}\right)^j \left(1 - \frac{s}{2}\right)^{n-j}} = \frac{n-j}{j+1} \cdot \frac{s}{2-s} < \frac{4-3s}{3s} \cdot \frac{s}{2-s} = \frac{4-3s}{6-3s} < \frac{2}{3},$$

logo, como $\sum_{j=0}^n \binom{n}{j} \left(\frac{s}{2}\right)^j \left(1 - \frac{s}{2}\right)^{n-j} = 1$, para $j = \frac{3sn}{4}$, $\binom{n}{j} \left(\frac{s}{2}\right)^j \left(1 - \frac{s}{2}\right)^{n-j} \leq 1$, donde aplicando reiteradamente a desigualdade acima obtemos $\binom{n}{sn} \left(\frac{s}{2}\right)^{sn} \left(1 - \frac{s}{2}\right)^{(1-s)n} \leq \left(\frac{2}{3}\right)^{sn/4}$ e

$$\begin{aligned} \sum_{j=sn}^n \binom{n}{j} \left(\frac{s}{2}\right)^j \left(1 - \frac{s}{2}\right)^{n-j} &\leq \left(\frac{2}{3}\right)^{sn/4} \sum_{k=0}^{\infty} \left(\frac{2}{3}\right)^k = 3 \left(\frac{2}{3}\right)^{sn/4} \\ &= 3 \left(\frac{2}{3}\right)^{n/k(k+1)} < \left(\frac{3}{4}\right)^{n/k(k+1)}, \end{aligned}$$

se $n/k(k+1)$ é suficientemente grande.

Portanto a probabilidade de que, para algum $k < \lfloor \sqrt[3]{n} \rfloor$, k apareça pelo menos $4n/k(k+1)$ vezes entre a_1, a_2, \dots, a_n é no máximo $\sqrt[3]{n} \cdot \left(\frac{3}{4}\right)^{\sqrt[3]{n}}$, que converge a zero quando $n \rightarrow +\infty$. Por outro lado, procedendo como na demonstração anterior e utilizando o fato de que $\sum \frac{1}{n^2}$ converge, temos, com probabilidade total, que $a_n < n^2$ para todo n suficientemente grande. Um cálculo similar ao acima, que deixamos como exercício para o leitor, mostra que também com probabilidade total o número de termos maiores ou iguais a $\sqrt[3]{n}$ entre a_1, a_2, \dots, a_n é no máximo $4n/\sqrt[3]{n}$, para n suficientemente grande. Assim, com probabilidade total, para todo n grande,

$$q_n < \prod_{k=1}^n (a_k + 1) < \left(\prod_{r=1}^{\sqrt[3]{n}} (r+1)^{\frac{4n}{r(r+1)}} \right) \cdot (n^2)^{4n/\sqrt[3]{n}}$$

Como $\lim_{n \rightarrow \infty} (8 \log n)/\sqrt[3]{n} = 0$, temos com probabilidade total

$$\limsup_{n \rightarrow \infty} \sqrt[n]{q_n} \leq \exp \left(\sum_{r=1}^{\infty} \frac{4 \log(r+1)}{r(r+1)} \right) < +\infty.$$

□

Observação 8.14. *Pode-se provar com métodos de teoria ergódica que para quase todo $\alpha \in \mathbb{R}$ vale*

$$\lim_{n \rightarrow \infty} \sqrt[n]{q_n} = e^{\pi^2/12 \ln 2} \approx 3,2758229 \dots$$

Corolário 8.15. (i) *Para quase todo $\alpha \in \mathbb{R}$, $|\alpha - \frac{p}{q}| < \frac{1}{q^2 \log^2 q}$ tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$, e portanto $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$ tem apenas um número finito de soluções racionais $\frac{p}{q}$, para todo $\varepsilon > 0$. Em particular $\text{ord } \alpha = 2$ para quase todo $\alpha \in \mathbb{R}$ onde*

$$\text{ord } \alpha = \sup \left\{ \nu > 0 \mid \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\nu} \text{ tem infinitas soluções } \frac{p}{q} \in \mathbb{Q} \right\}$$

(ii) *Para quase todo $\alpha \in \mathbb{R}$, $|\alpha - \frac{p}{q}| < \frac{1}{q^2 \log q}$ tem infinitas soluções racionais p/q , e portanto, para todo $k \in \mathbb{R}$, $|\alpha - \frac{p}{q}| < \frac{1}{kq^2}$ tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$.*

8.3.2 O Teorema de Khintchine Multidimensional

Teorema 8.16 (Khintchine). *Sejam $f_1, f_2, \dots, f_n: \mathbb{N} \rightarrow \mathbb{R}^+$ funções decrescentes e $F: \mathbb{N} \rightarrow \mathbb{R}^+$ dada por $F(k) = f_1(k)f_2(k)\dots f_n(k)$. Seja $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$. O sistema de aproximações simultâneas*

$$\left| \alpha_i - \frac{p_i}{q} \right| < \frac{f_i(q)}{q}, \quad 1 \leq i \leq n, \quad (*)$$

é tal que

- (a) *Se $\sum_{q=1}^{\infty} F(q) < +\infty$ então, para quase todo $\alpha \in \mathbb{R}^n$, (*) tem apenas um número finito de soluções $(\frac{p_1}{q}, \dots, \frac{p_n}{q}) \in \mathbb{Q}^n$*
- (b) *Se $\sum_{q=1}^{\infty} F(q) = +\infty$ então, para quase todo $\alpha \in \mathbb{R}^n$, (*) tem infinitas soluções $(\frac{p_1}{q}, \dots, \frac{p_n}{q}) \in \mathbb{Q}^n$.*

Antes de provar o teorema acima, vamos demonstrar primeiro o seguinte resultado auxiliar sobre a função φ de Euler.

Lema 8.17. *Para todo $k \in \mathbb{N}$ existe $c_k > 0$ tal que $\sum_{j=1}^n \left(\frac{\varphi(j)}{j}\right)^k \geq c_k n$ para todo n .*

DEMONSTRAÇÃO: O caso $k = 1$ segue da proposição 5.29, que implica

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n \frac{\varphi(j)}{j} = \frac{6}{\pi^2}$$

Como $h(x) = x^k$ é convexa para $k \geq 1$, temos

$$\frac{1}{n} \sum_{j=1}^n \left(\frac{\varphi(j)}{j}\right)^k \geq \left(\frac{1}{n} \sum_{j=1}^n \frac{\varphi(j)}{j}\right)^k,$$

donde segue o resultado no caso geral. \square

DEMONSTRAÇÃO: (DO TEOREMA DE KHINTCHINE)

(a) Dado $q_0 \in \mathbb{N}$, consideremos o conjunto

$$S(q_0) = \bigcup_{q \geq q_0} \bigcup_{0 \leq p_1, \dots, p_n < q} \prod_{i=1}^n \left(\frac{p_i}{q} - \frac{f_i(q)}{q}, \frac{p_i}{q} + \frac{f_i(q)}{q} \right),$$

que é o conjunto dos $\alpha \in [0, 1)^n$ para os quais o sistema (*) do enunciado do teorema tem alguma solução com $q \geq q_0$ e, portanto, $S = \bigcap_{q_0 \in \mathbb{N}} S(q_0)$ é o conjunto dos $\alpha \in [0, 1)^n$ para os quais (*) tem infinitas soluções $(\frac{p_1}{q}, \dots, \frac{p_n}{q}) \in \mathbb{Q}^n$. Particionando \mathbb{R}^n em (uma quantidade enumerável de) cubos de aresta 1, é suficiente mostrar que S tem medida nula. Temos

$$m(S(q_0)) \leq \sum_{q=q_0}^{\infty} q^n \cdot \frac{2^n F(q)}{q^n} = 2^n \sum_{q=q_0}^{\infty} F(q),$$

que tende a 0 quando $q_0 \rightarrow \infty$, pois $\sum_{q=1}^{\infty} F(q)$ converge. Portanto $m(S) = 0$.

(b) Em primeiro lugar, vamos substituir as funções f_1, \dots, f_n por funções $g_1, \dots, g_n: \mathbb{N} \rightarrow \mathbb{R}^+$ tais que cada g_i é decrescente, $\lim_{q \rightarrow \infty} \frac{g_i(q)}{f_i(q)} = 0$ e $G = g_1 g_2 \cdots g_n: \mathbb{N} \rightarrow \mathbb{R}^+$ satisfaz

$$\lim_{q \rightarrow \infty} qG(q) = 0 \quad \text{e} \quad \sum_{q=1}^{\infty} G(q) = +\infty.$$

Para isto, basta tomar

$$\begin{aligned} G_1(k) &= (F(1) + \cdots + F(k))^{-1} \cdot F(k) \quad \text{e} \\ G(k) &= (G_1(1) + G_1(2) + \cdots + G_1(k))^{-1} G_1(k), \end{aligned}$$

para todo $k \in \mathbb{N}$. É fácil verificar que G_1 e G são decrescentes, $G_1(k) \leq 1/k$, $kG(k) \rightarrow 0$, $\Sigma G_1(k) = \infty$, $\Sigma G(k) = \infty$. Definindo $g_i(q) = f_i(q) \cdot (G(q)/F(q))^{1/n}$, todas as condições acima são satisfeitas.

Agora, para $q_0 \in \mathbb{N}$, definimos os conjuntos

$$\begin{aligned} A(q_0) &= \bigcup_{q \geq q_0} \bigcup_{0 \leq p_1, \dots, p_n < q} \prod_{i=1}^n \left(\frac{p_i}{q} - \frac{g_i(q)}{q}, \frac{p_i}{q} + \frac{g_i(q)}{q} \right) \\ A_\infty &= \bigcap_{q \in \mathbb{N}} A(q). \end{aligned}$$

Afirmamos que para finalizar a prova de (b) basta mostrar que $m(A_\infty) > 0$. De fato, se $\bar{\alpha} = (\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) \in A_\infty$, o sistema $|\bar{\alpha}_i - \frac{p_i}{q}| < \frac{g_i(q)}{q}$, $i = 1, 2, \dots, n$, tem infinitas soluções $(\frac{p_1}{q}, \frac{p_2}{q}, \dots, \frac{p_n}{q}) \in \mathbb{Q}^n$. Como $m(A_\infty) > 0$, dado $\varepsilon > 0$ existe um cubo $Q = \prod_{i=1}^n [\frac{b_i}{C}, \frac{b_i+1}{C}] \subset \mathbb{R}^n$, $C \in \mathbb{N}$, $b_i \in \mathbb{Z}$, $0 \leq b_i < C$, tal que $m(A_\infty \cap Q) \geq (1 - \varepsilon)m(Q)$. Se $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ é dada por

$$T(X_1, \dots, X_n) = (CX_1 - b_1, CX_2 - b_2, \dots, CX_n - b_n),$$

temos $T(Q) = [0, 1]^n$ e $m(T(Q \cap A_\infty)) \geq 1 - \varepsilon$. Além disso, se $\alpha = (\alpha_1, \dots, \alpha_n) \in T(Q \cap A_\infty)$ com $\alpha = T(\bar{\alpha})$, $\bar{\alpha} = (\bar{\alpha}_1, \dots, \bar{\alpha}_n) \in A_\infty \cap Q$, temos que $|\alpha_i - \frac{r_i}{q}| < \frac{Cg_i(q)}{q}$ (e portanto o sistema original $|\alpha_i - \frac{r_i}{q}| < \frac{f_i(q)}{q}$) tem infinitas soluções

$$\left(\frac{r_1}{q}, \frac{r_2}{q}, \dots, \frac{r_n}{q} \right) = \left(\frac{Cp_1}{q} - b_1, \frac{Cp_2}{q} - b_2, \dots, \frac{Cp_n}{q} - b_n \right) \in \mathbb{Q}^n,$$

e como $\varepsilon > 0$ pode ser feito arbitrariamente pequeno e \mathbb{R}^n pode ser particionado em translações de $[0, 1]^n$, isto completará a prova do item (b).

Para provar que $m(A_\infty) > 0$ basta mostrar que existe $c > 0$ para o qual $m(A(q_0)) > c$ para todo q_0 suficientemente grande. Fixemos agora $q_0 \in \mathbb{N}$ grande e definamos

$$s_0 = s_0(q_0) = \min\{s \in \mathbb{N} \mid G(q_0) + G(q_0 + 1) + \cdots + G(s) \geq \tilde{c}\},$$

onde \tilde{c} é uma constante que escolheremos posteriormente. Note que como G é decrescente e $\lim_{q \rightarrow \infty} qG(q) = 0$ temos $\lim_{q \rightarrow \infty} \frac{s_0(q)}{q} = +\infty$.

Para cada s fixado, $q_0 \leq s \leq s_0$, e cada ponto $(\frac{r_1}{s}, \dots, \frac{r_n}{s})$, $0 \leq r_i < s$, $\text{mdc}(r_i, s) = 1$, $1 \leq i \leq n$, consideremos o bloco $\prod_{i=1}^n (\frac{r_i}{s} - \frac{g_i(s)}{s}, \frac{r_i}{s} + \frac{g_i(s)}{s})$, contido em $A(q_0)$. Para dar um limitante inferior para $m(A(q_0))$, devemos estimar o número de “blocos novos” para cada s , isto é, blocos disjuntos dos associados a pontos com denominadores estritamente menores do que s . Para isto, fixado s , vamos estimar o número de $(\frac{r_1}{s}, \frac{r_2}{s}, \dots, \frac{r_n}{s}) \in \mathbb{Q}^n$ com $r_i \in \mathbb{Z}$, $0 \leq r_i < s$, $1 \leq i \leq n$, tais que existem q com $q_0 \leq q < s$, $p_1, p_2, \dots, p_n \in \mathbb{Z}$, $0 \leq p_i < q$, satisfazendo

$$\left| \frac{r_i}{s} - \frac{p_i}{q} \right| < \frac{g_i(s)}{s} + \frac{g_i(q)}{q} \quad \text{para todo } i = 1, 2, \dots, n. \quad (**)$$

(ou seja, os blocos associados a $(\frac{r_1}{s}, \frac{r_2}{s}, \dots, \frac{r_n}{s})$ e $(\frac{p_1}{q}, \frac{p_2}{q}, \dots, \frac{p_n}{q})$ se intersectam). Como cada g_i é decrescente, $(**)$ implica

$$|r_i q - p_i s| < 2s g_i(q), \quad i = 1, 2, \dots, n.$$

Se $q_0 \leq q < s$, o número de soluções de $|r_i q - p_i s| < 2s g_i(q)$ com $0 \leq p_i < q$, $0 \leq r_i < s$ é no máximo $4s g_i(q)$ desde que $\text{mdc}(r_i, s) = 1$. De fato, nessas condições $r_i q - p_i s$ não se anula, senão teríamos $\frac{p_i}{q} = \frac{r_i}{s}$, que é uma fração irredutível de denominador $s > q$, absurdo. Seja $d = \text{mdc}(s, q)$. Dado $k \in \mathbb{Z}$, a equação diofantina $r q - p s = k$ só tem solução se $d \mid k$ e neste caso tem d soluções com $0 \leq r < s$. Portanto $0 < r q - p s < x$ (respectivamente $-x < r q - p s < 0$) tem no máximo $d \lfloor \frac{x}{d} \rfloor \leq x$ soluções (p, r) com $0 \leq r < s$, o que claramente implica a afirmação. Portanto o número total de soluções $((p_1, r_1); \dots; (p_n, r_n))$ do sistema de desigualdades acima é no máximo $4^n s^n G(q)$. Portanto a quantidade de pontos $(\frac{r_1}{s}, \frac{r_2}{s}, \dots, \frac{r_n}{s})$ satisfazendo as condições acima não ultrapassa $4^n s^n \sum_{q=q_0}^{s-1} G(q)$.

Há $\varphi(s)^n$ pontos $(\frac{r_1}{s}, \dots, \frac{r_n}{s})$, $0 \leq r_i < s$, $\text{mdc}(r_i, s) = 1$, $1 \leq i \leq n$. Assim, há pelo menos $\varphi(s)^n - 4^n s^n \sum_{q=q_0}^{s-1} G(q)$ blocos novos associados a pontos com denominador s . Como cada um destes blocos novos tem

volume $\frac{2^n G(s)}{s^n}$, obtemos

$$\begin{aligned} m(A(q_0)) &\geq \sum_{s=q_0}^{s_0} \left(\varphi(s)^n - 4^n s^n \sum_{q=q_0}^{s-1} G(q) \right) \frac{2^n G(s)}{s^n} \\ &= 2^n \sum_{s=q_0}^{s_0} \left(\frac{\varphi(s)}{s} \right)^n G(s) - 8^n \sum_{s=q_0}^{s_0} \left(\sum_{q=q_0}^{s-1} G(q) \right) G(s). \end{aligned}$$

Para estimar o primeiro termo, temos pelo lema anterior e pela definição de $s_0 = \min\{s \geq q_0 \mid \sum_{q=q_0}^s G(q) \geq \tilde{c}\}$ que

$$\begin{aligned} &\sum_{s=q_0}^{s_0} \left(\frac{\varphi(s)}{s} \right)^n G(s) \\ &= \sum_{s=q_0}^{s_0-1} (G(s) - G(s+1)) \sum_{j=q_0}^s \left(\frac{\varphi(j)}{j} \right)^n + G(s_0) \sum_{j=q_0}^{s_0} \left(\frac{\varphi(j)}{j} \right)^n \\ &\geq \sum_{s=q_0}^{s_0-1} (G(s) - G(s+1))(c_n s - q_0) + G(s_0)(c_n s_0 - q_0) \\ &= c_n \sum_{s=q_0+1}^{s_0} G(s) - (1 - c_n)q_0 G(q_0) \\ &\geq c_n \tilde{c} + \varepsilon_1 \end{aligned}$$

onde $\varepsilon_1 \rightarrow 0$ quando $q_0 \rightarrow \infty$ pois $\lim_{q_0 \rightarrow \infty} q_0 G(q_0) = 0$.

Por outro lado, novamente pela definição de s_0 , temos

$$\sum_{s=q_0}^{s_0} \left(\sum_{q=q_0}^{s-1} G(q) \right) G(s) \leq \tilde{c} \sum_{s=q_0}^{s_0} G(s) \leq \tilde{c}(\tilde{c} + \varepsilon_2)$$

onde $\varepsilon_2 = G(s_0) \rightarrow 0$ quando $q_0 \rightarrow \infty$.

Assim, $m(A(q_0)) \geq 2^n(c_n \tilde{c} + \varepsilon_1) - 8^n \tilde{c}(\tilde{c} + \varepsilon_2)$. Tomando $\tilde{c} = \frac{c_n}{4^{n+1}}$ temos que, se q_0 é suficientemente grande (e logo ε_1 e ε_2 suficientemente pequenos), o volume de $A(q_0)$ é pelo menos $c_n^2/2^{n+3} > 0$, como queríamos demonstrar.

□

8.4 Números de Liouville

Vimos no corolário 8.15 do teorema de Khintchine que $\text{ord } \alpha = 2$ para quase todo $\alpha \in \mathbb{R}$. Dado $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, dizemos que α é um *número de Liouville* se $\text{ord } \alpha = \infty$, isto é, se para todo $n > 0$ existem infinitos racionais $\frac{p}{q}$ com $|\alpha - \frac{p}{q}| < \frac{1}{q^n}$. O conjunto dos números de Liouville é portanto dado por

$$L = \bigcap_{n \in \mathbb{N}} \bigcup_{q \geq 2} \bigcup_{p \in \mathbb{Z}} \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n} \right).$$

Assim, L é uma interseção enumerável de abertos densos e portanto é um conjunto genérico no sentido de Baire, embora, como vimos, tenha medida nula.

Uma parte do interesse dos números de Liouville é motivado pelo seguinte resultado, que implica que todo número de Liouville é transcendente (a recíproca entretanto é falsa, já que o conjunto dos números algébricos é enumerável e portanto o conjunto dos números transcendentos tem medida total).

Proposição 8.18. *Seja $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ um número algébrico de grau n , isto é, α é raiz de um polinômio não nulo de grau n com coeficientes inteiros. Então existe $c > 0$ tal que*

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^n}$$

para todo $p/q \in \mathbb{Q}$. Em particular, $\text{ord } \alpha \leq n$.

DEMONSTRAÇÃO: Seja $P(x)$ um polinômio de grau n com coeficientes inteiros tal que $P(\alpha) = 0$. Existe um $d > 0$ tal que $P(x) \neq 0$ para todo $0 < |x - \alpha| < d$. Sejam

$$k = \max_{|x - \alpha| \leq 1} |P'(x)| \quad \text{e} \quad c = \min \left\{ 1, d, \frac{1}{k} \right\}$$

Se $|\alpha - \frac{p}{q}| < \frac{c}{q^n}$, com $p, q \in \mathbb{N}_{>0}$, teríamos $|\alpha - \frac{p}{q}| < c \leq d$, donde $P(\frac{p}{q}) \neq 0$. Assim, como $q^n \cdot P(\frac{p}{q}) \in \mathbb{Z}$, $|q^n \cdot P(\frac{p}{q})| \geq 1 \iff |P(\frac{p}{q})| \geq \frac{1}{q^n}$. Por outro lado,

$$\left| P\left(\frac{p}{q}\right) \right| = \left| P\left(\frac{p}{q}\right) - P(\alpha) \right| = \left| P'(y) \cdot \left(\frac{p}{q} - \alpha\right) \right|,$$

para algum y estritamente entre α e $\frac{p}{q}$, pelo teorema do valor médio, mas $|y - \alpha| < |\alpha - \frac{p}{q}| < c \leq 1$ implica $|P'(y)| \leq k$, logo

$$\frac{1}{q^n} \leq \left| P\left(\frac{p}{q}\right) \right| \leq k \left| \alpha - \frac{p}{q} \right| < \frac{kc}{q^n} \leq \frac{1}{q^n}$$

o que é absurdo. □

Um teorema não trivial devido a Roth (e que lhe rendeu uma medalha Fields) mostra que, de fato, $\text{ord } \alpha = 2$, para *todo* α algébrico (veja por exemplo [90]).

Lembramos que, usando a fração contínua de e , é possível provar que $\text{ord}(e) = 2$ (veja o capítulo 3), isto é, o número e é transcendente, mas “não muito”.

Problemas Propostos

8.1. *Mostre que a sequência (a_n) com $a_n \in [0, 1]^d$ é uniformemente distribuída se, e só se, para qualquer função contínua $f: [0, 1]^d \rightarrow \mathbb{R}$, temos*

$$\lim_{n \rightarrow \infty} \frac{f(a_1) + f(a_2) + \cdots + f(a_n)}{n} = \int_{[0,1]^d} f.$$

8.2. *Prove que $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ é um número de Liouville e, portanto, é transcendente.*

8.3. *Mostrar que se α e β são números irracionais positivos satisfazendo $\frac{1}{\alpha} + \frac{1}{\beta} = 1$, então as sequências*

$$[\alpha], [2\alpha], [3\alpha], \dots \quad e \quad [\beta], [2\beta], [3\beta], \dots$$

juntas contém todo inteiro positivo exatamente uma vez.

8.4. *Mostrar que se a e b são números inteiros positivos arbitrários, então*

$$|a\sqrt{2} - b| > \frac{1}{2(a+b)}.$$

8.5. Construa uma sequência infinita limitada x_0, x_1, x_2, \dots tal que para todos os números naturais i e j com $i \neq j$ se tenha

$$|x_i - x_j||i - j| \geq 1.$$

Obs.: Uma consequência imediata deste fato é que, dado um real $a > 1$, existe uma sequência infinita limitada x_0, x_1, x_2, \dots tal que para todos os números naturais i e j com $i \neq j$ se tenha

$$|x_i - x_j||i - j|^a \geq 1.$$

O problema 6 da IMO de 1991 consistiu em provar esta última afirmação.

8.6. Sejam a, b, c inteiros não todos nulos. Mostrar que

$$\frac{1}{4a^2 + 3b^2 + 2c^2} \leq |\sqrt[3]{4a} + \sqrt[3]{2b} + c|.$$

8.7. Mostrar que a sequência $\{a_n\}_{n \geq 1}$ definida por $a_n = \lfloor n\sqrt{2} \rfloor$ contém um número infinito de termos que são potências de 2.

8.8. Seja $\{a_n\}$ uma sequência crescente de inteiros positivos tais que para todo K existe um $n \in \mathbb{N}$ tal que $a_{n+1} > Ka_n$. Mostrar que $\sum_{n=1}^{\infty} 2^{-a_n}$ é um número de Liouville (e portanto é transcendente).

8.9. a) Prove que existe $n \in \mathbb{N}$ tal que os 2010 primeiros dígitos de 2^n são iguais a 1.

b) Prove que existe $n \in \mathbb{N}$ tal que os 2010 primeiros dígitos de 2^n são iguais a 1 e os 2010 primeiros dígitos de 3^n são iguais a 2.

8.10. Prove que, para todo inteiro a com $1 \leq a \leq 9$ temos

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{\#\{j \mid 1 \leq j \leq n \text{ e o primeiro dígito de } 2^j \text{ é } a\}}{n} \\ = \frac{\log(a+1) - \log a}{\log 10}. \end{aligned}$$

Capítulo 9

Introdução às Curvas Elípticas

Este capítulo é uma breve introdução à teoria de curvas elípticas. Além de ser um belo tópico que combina Álgebra, Análise, Topologia e Geometria, curvas elípticas tiveram e continuam a ter um papel central na Teoria dos Números contemporânea, sendo um dos ingredientes centrais na prova do último teorema de Fermat. Aqui, limitamo-nos aos aspectos mais elementares desta teoria.

9.1 Curvas Elípticas como Curvas Projetivas Planas

Em capítulos anteriores (ver exemplo 4.5), vimos como estabelecer uma bijeção entre os pontos racionais de uma cônica e os pontos racionais de uma reta acrescida de um “ponto no infinito”, ou seja, uma *reta projetiva*. Nesta seção, novamente será conveniente trabalharmos no mundo projetivo, então faremos um breve resumo dos conceitos que utilizaremos.

Dado um corpo k , o *espaço projetivo* \mathbb{P}_k^n de dimensão n sobre k é definido como o conjunto de todas as direções no espaço afim k^{n+1} de dimensão $n + 1$. Em outras palavras, um ponto em \mathbb{P}_k^n pode ser representado como um vetor *não nulo* $(a_0, a_1, \dots, a_n) \in k^{n+1}$; dois vetores (a_0, a_1, \dots, a_n) e (b_0, b_1, \dots, b_n) definem o mesmo ponto se eles são *homotéticos*, isto é, existe um $\lambda \in k$ não nulo tal que $a_i = \lambda b_i$ para $i =$

$0, 1, \dots, n$. Representamos o ponto definido pelo vetor (a_0, a_1, \dots, a_n) através da sugestiva notação $(a_0 : a_1 : \dots : a_n)$.

Por exemplo, temos que a reta projetiva pode ser decomposta como

$$\mathbb{P}_k^1 = \{(1 : a_1) \mid a_1 \in k\} \cup \{(0 : 1)\}$$

pois se $a_0 \neq 0$ então $(a_0 : a_1) = (1 : \frac{a_1}{a_0})$ e se $a_0 = 0$ então $(0 : a_1) = (0 : 1)$. Assim, a reta projetiva consiste de uma “reta afim”, composta pelos pontos da forma $(1 : a_1)$, e mais um “ponto no infinito” $(0 : 1)$. Da mesma forma, temos que o plano projetivo

$$\mathbb{P}_k^2 = \{(1 : a_1 : a_2) \mid (a_1, a_2) \in k^2\} \cup \{(0 : a_1 : a_2) \mid a_1 \neq 0 \text{ ou } a_2 \neq 0\}$$

é a união de um “plano afim” (primeiro termo, já que $(1 : a_1 : a_2) = (1 : a'_1 : a'_2) \iff a_1 = a'_1 \text{ e } a_2 = a'_2$) e uma reta projetiva no “infinito” (segundo termo). Note que a escolha de “reta no infinito” é completamente arbitrária, pois poderíamos tomar uma outra decomposição, por exemplo

$$\mathbb{P}_k^2 = \{(a_0 : a_1 : 1) \mid (a_0, a_1) \in k^2\} \cup \{(a_0 : a_1 : 0) \mid a_0 \neq 0 \text{ ou } a_1 \neq 0\}$$

e agora os pontos com $a_2 = 0$ formam a “reta no infinito”.

Agora falaremos um pouco sobre curvas algébricas planas. No plano afim k^2 , temos que qualquer polinômio $p(x, y) \in k[x, y]$ define uma curva

$$C = \{(a, b) \in k^2 \mid p(a, b) = 0\}$$

(que pode eventualmente degenerar em um ponto, em todo o plano, ou mesmo no conjunto vazio, mas não vamos nos preocupar com estes detalhes agora). Porém, no mundo projetivo só podemos considerar polinômios *homogêneos*, isto é, polinômios cujos monômios têm todos o mesmo grau. De fato, se $p(x_0, x_1, x_2) \in k[x_0, x_1, x_2]$ é homogêneo de grau d então temos que

$$p(a_0, a_1, a_2) = 0 \implies p(\lambda a_0, \lambda a_1, \lambda a_2) = \lambda^d p(a_0, a_1, a_2) = 0.$$

Assim, faz sentido dizer quando um polinômio homogêneo $p(x_0, x_1, x_2)$ se anula em uma classe de vetores homotéticos e podemos considerar a curva projetiva definida por $p(x_0, x_1, x_2)$:

$$C = \{(a_0 : a_1 : a_2) \in \mathbb{P}_k^2 \mid p(a_0, a_1, a_2) = 0\}.$$

Por exemplo temos que $x_0 = 0$ é uma equação da “reta no infinito” descrita acima. Temos que para qualquer $(a, b, c) \neq (0, 0, 0)$ a equação $ax_0 + bx_1 + cx_2 = 0$ define uma reta projetiva em \mathbb{P}_k^2 ; esta reta é a união de uma reta afim de equação $a + bx + cy = 0$ ($x_0 \neq 0$) e de um “ponto no infinito” $(0 : -c : b)$ (supondo $b \neq 0$ ou $c \neq 0$), intersecção das retas $ax_0 + bx_1 + cx_2 = 0$ e $x_0 = 0$.

Em geral, duas retas distintas

$$\begin{cases} ax_0 + bx_1 + cx_2 = 0 \\ dx_0 + ex_1 + fx_2 = 0 \end{cases}$$

possuem exatamente um ponto de intersecção, pois a solução do sistema linear homogêneo acima é 1 dimensional (não pode ser 2 dimensional, pois neste caso as retas seriam coincidentes), logo define exatamente um ponto em \mathbb{P}_k^2 (ou seja, uma direção em k^3).

Agora estamos prontos para dar a (primeira) definição de curva elíptica:

Definição 9.1. *Seja k um corpo, de característica diferente de 2 e 3 para simplificar (isto é, $2 \neq 0$ e $3 \neq 0$ em k). Uma curva projetiva plana definida por uma equação da forma*

$$y^2z = x^3 + axz^2 + bz^3, \quad a, b \in k,$$

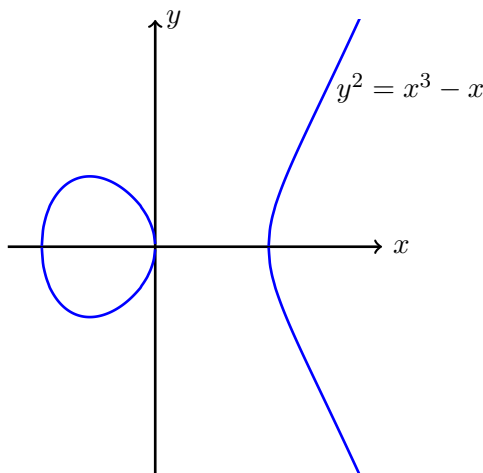
é denominada de curva elíptica sobre k .

Observe que a curva acima é a união da curva afim de equação ($z \neq 0$)

$$y^2 = x^3 + ax + b \quad (*)$$

e de um único “ponto no infinito” $O = (0 : 1 : 0)$, intersecção da curva projetiva acima com a “reta no infinito” $z = 0$. Por este motivo, muitas vezes, ao fazermos as contas, trabalhamos com a equação afim (*), que é mais simples, retornando ao modelo projetivo conforme necessário.

Vejamos uma curva elíptica real, por exemplo $y^2 = x^3 - x$. Note que na figura as duas pontas do ramo da direita se encontram no “ponto do infinito” $O = (0 : 1 : 0)$, que é o ponto de intersecção da “reta no infinito” com qualquer reta “vertical” $x - cz = 0$. Em outras palavras, O é o ponto de concorrência de todas as retas verticais.



Veja! Uma curva elíptica!

9.2 A Lei da Corda-Tangente

Vamos tentar imitar o procedimento do exemplo 4.5 para encontrar os pontos racionais de uma curva elíptica sobre \mathbb{Q} . A primeira dificuldade com a qual nos deparamos é que enquanto em geral uma reta intercepta uma cônica em 2 pontos, ela intercepta uma curva elíptica em 3 pontos! Observe por exemplo o eixo das abscissas na figura anterior.

Por outro lado, se tivermos *dois* pontos racionais $P = (x_P, y_P)$ e $Q = (x_Q, y_Q)$ em uma curva elíptica, então podemos encontrar um novo ponto racional $R = (x_R, y_R)$, intersecção da curva elíptica com a reta r que liga P e Q . Para ver que este ponto é racional, observe que a reta que passa por P e Q tem equação

$$y - y_P = \frac{y_P - y_Q}{x_P - x_Q} \cdot (x - x_P)$$

cujos coeficientes são racionais. As abscissas dos pontos de intersecção desta reta com a curva elíptica (*) são as soluções de

$$\left(y_P + \frac{y_P - y_Q}{x_P - x_Q} \cdot (x - x_P) \right)^2 = x^3 + ax + b$$

que também é uma equação com coeficientes racionais. Como duas de suas raízes x_P e x_Q são racionais, a terceira raiz x_R também será racional pelas relações entre coeficientes e raízes de um polinômio. Assim

obtemos

$$x_R = -x_P - x_Q + \left(\frac{y_P - y_Q}{x_P - x_Q} \right)^2 \quad \text{e} \quad y_R = y_P + \frac{y_P - y_Q}{x_P - x_Q} \cdot (x_R - x_P)$$

Mas o que fazer se conhecemos apenas um ponto racional? Aí tomamos $P = Q$, ou seja, tomamos a reta tangente a este ponto! Basta substituir o coeficiente angular $\frac{y_P - y_Q}{x_P - x_Q}$ por $\frac{3x_P^2 + a}{2y_P}$ nas fórmulas acima. Por exemplo, considere a curva elíptica

$$y^2 = x^3 + 17$$

Ela possui um ponto racional $P = Q = (-1, 4)$. Fazendo as contas acima encontramos o insuspeito terceiro ponto racional $R = (\frac{137}{64}, \frac{2651}{512})$. Simples, não?

Observe que qualquer curva elíptica sempre possui um ponto racional, a saber, o “ponto no infinito” $O = (0 : 1 : 0)$! Será que podemos obter novos pontos racionais a partir de O ? Para responder esta questão, observe que a curva (*) é tangente à “reta no infinito” $z = 0$ em O : de fato, trabalhando no plano afim $y \neq 0$ que contém O , temos que a curva elíptica tem equação

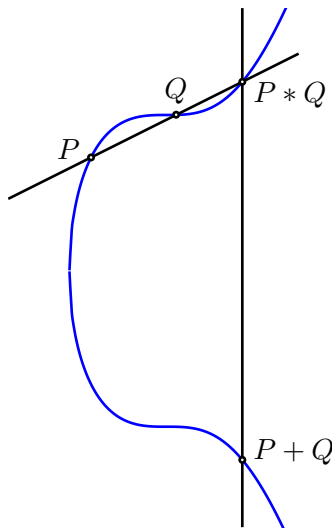
$$z = x^3 + axz^2 + bz^3$$

e assim a única intersecção com $z = 0$ é o ponto O , ou seja, O é um ponto de *inflexão* da curva. Logo aplicando o procedimento acima com $P = Q = O$ obtemos novamente o ponto O ! De certa forma O age como uma espécie de “elemento neutro” para a operação acima. Podemos ser mais precisos.

Dados dois pontos racionais P e Q de uma curva elíptica, denote por $P * Q$ o ponto R que é o terceiro ponto de intersecção da curva elíptica com a reta que passa por P e Q . Definimos a soma de P e Q como sendo

$$P + Q \stackrel{\text{def}}{=} (P * Q) * O.$$

Note que $(P * Q) * O$ nada mais é que o simétrico de $P * Q$ com relação ao eixo x pois a reta que passa por O e $P * Q$ nada mais é do que a reta “vertical” que passa por $P * Q$.



A lei da corda-tangente

Esta regra, que associa a P e Q o ponto racional $P + Q$ é popularmente conhecida como *lei da corda-tangente*.

Teorema 9.2. *A lei da corda-tangente define um grupo abeliano sobre os pontos racionais de uma curva elíptica. Em outras palavras, temos*

1. (Associatividade) $(P + Q) + R = P + (Q + R)$ para quaisquer três pontos racionais P , Q e R ;
2. (Elemento Neutro) $P + O = O + P = P$ para qualquer ponto racional P ;
3. (Inverso) para qualquer ponto racional P , existe um outro ponto racional $-P$ tal que $P + (-P) = (-P) + P = O$;
4. (Comutatividade) $P + Q = Q + P$ para quaisquer dois pontos racionais P e Q .

DEMONSTRAÇÃO: A associatividade é a propriedade mais difícil de ser verificada e sua prova será postergada até a próxima seção. A comutatividade é clara, pois $P * Q = Q * P$. Agora seja $P = (x_P, y_P)$ um ponto racional da curva. Então $P * O = (x_P, -y_P)$ é o simétrico de P com relação ao eixo x . Analogamente, temos $(x_P, -y_P) * O = (x_P, y_P) = P$, o que mostra que O é o elemento neutro deste grupo. Da mesma forma,

é fácil ver que $-P = (x_P, -y_P)$, o simétrico de P com relação ao eixo x . \square

Note que $P * Q = -(P + Q)$, logo $P + Q + P * Q = O$. Assim, a lei da corda tangente pode ser assim enunciada: *três pontos têm soma zero se, e somente se, eles estão alinhados.*

Temos agora algumas questões. Como decidir se a curva elíptica tem algum ponto racional além do ponto no infinito O ? Como encontrá-lo explicitamente? Finalmente, o procedimento acima gera todos os pontos racionais da curva elíptica?

Aqui a situação não é tão simples assim. O problema de decidir a existência de pontos racionais está em aberto. Felizmente sabe-se que o procedimento acima realmente gera todos os pontos racionais a partir de um certo conjunto finito de pontos. Este é o famoso

Teorema 9.3 (Mordell-Weil). *O grupo de uma curva elíptica é finitamente gerado.*

Há uma demonstração elementar deste teorema, que pode ser vista no excelente livro de Silverman e Tate [143]. Entretanto, as provas mais naturais são aquelas que utilizam ferramentas um pouco mais avançadas, que são úteis em outros contextos também, mais especificamente a teoria de *cohomologia galoisiana* ou a teoria de *cohomologia étale*, para a qual recomendamos o excelente livro do Milne [103] (ver theorem 4.22, p. 133, e sua transparente demonstração de 1 página!).

Infelizmente a demonstração do teorema de Mordell-Weil não é construtiva e não permite achar explicitamente os geradores deste grupo, mas existe um algoritmo conjectural (não muito simples de descrever) para encontrar estes geradores: a questão é saber se ele para ou não. Até hoje, em todas as curvas elípticas testadas, ele sempre parou...

9.3 Curvas Elípticas como Rosquinhas

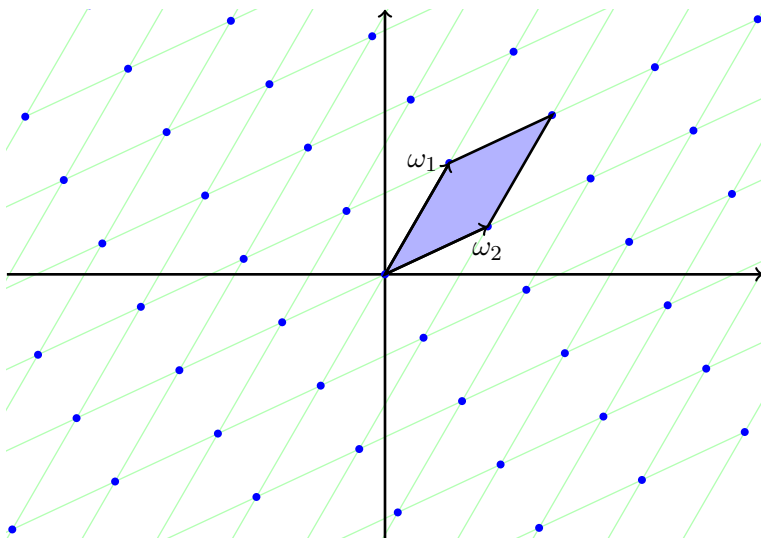
Considere o seguinte reticulado Λ gerado por dois números complexos ω_1 e ω_2 linearmente independentes sobre \mathbb{R} :

$$\Lambda = \{n_1\omega_1 + n_2\omega_2 \in \mathbb{C} \mid n_1, n_2 \in \mathbb{Z}\}$$

Identificando dois números complexos z e w se $z \equiv w \pmod{\Lambda}$, isto é, se $z - w \in \Lambda$, obtemos que todo número complexo é equivalente a exatamente um elemento do *paralelogramo fundamental*

$$P = \{r_1\omega_1 + r_2\omega_2 \in \mathbb{C} \mid r_1, r_2 \in \mathbb{R}, 0 \leq r_1, r_2 < 1\}$$

como mostra a figura a seguir.



O reticulado Λ e seu paralelogramo fundamental

Como os lados opostos (do fecho) deste paralelogramo estão identificados, temos um quociente \mathbb{C}/Λ que topologicamente é uma *rosquinha* (como diria Homer Simpson) ou, em termos mais científicos, um *toro*. Este toro é a *curva elíptica complexa definida pelo reticulado Λ* . Esta rosquinha vem, de fábrica, equipada com uma estrutura de grupo abeliano: dados dois pontos $P, Q \in \mathbb{C}/\Lambda$ representados por números complexos $z, w \in \mathbb{C}$, a soma $P + Q \in \mathbb{C}/\Lambda$ é o ponto correspondente ao número complexo $z + w$ (em outras palavras, a estrutura de grupo abeliano é o quociente do grupo aditivo de \mathbb{C} módulo o subgrupo Λ).

Mas o que rosquinhas têm a ver com a definição anterior de curva elíptica como curva projetiva plana? Para responder esta questão, vamos estudar as funções meromorfas em \mathbb{C}/Λ , ou seja, as funções meromorfas $f: \mathbb{C} \rightarrow \mathbb{C} \cup \{\infty\}$ que são invariantes por translações por elementos em Λ . Tais funções são popularmente conhecidas como *funções duplamente periódicas* pois elas possuem dois períodos:

$$f(z + \omega_1) = f(z) \quad \text{e} \quad f(z + \omega_2) = f(z)$$

para todo $z \in \mathbb{C}$.

Teorema 9.4. *Seja f uma função duplamente periódica com relação ao reticulado Λ .*

1. *Se f é holomorfa então f é constante.*
2. *Seja P o paralelogramo fundamental de Λ .*
 - (a) *contando multiplicidades, o número de zeros e polos de f em P são iguais;*
 - (b) *a soma dos resíduos de f em P é 0.*
 - (c) *a soma dos zeros menos a soma dos polos em P (multiplicidades contadas) é igual a 0 módulo Λ .*

DEMONSTRAÇÃO: (1) Se f é holomorfa, então ela é contínua e portanto atinge um máximo no fecho de P , que é um conjunto compacto. Assim, f é limitada em todo o plano complexo. Pelo teorema de Liouville f é constante.

(2) Transladando P por uma constante, podemos assumir que nenhum zero ou polo de $f(z)$ ou $f'(z)$ está no bordo ∂P de P . Assim, a diferença entre o número de zeros e polos de f em P é igual a

$$\frac{1}{2\pi i} \int_{\partial P} \frac{f'(z)}{f(z)} dz = 0,$$

já que $f'(z)/f(z)$ é duplamente periódica e portanto as integrais em lados opostos do paralelogramo P se cancelam. A prova do segundo item é análoga, utilizando o integrando $f(z)$. Para o último item, note que a soma dos zeros menos polos em P é igual a

$$S = \frac{1}{2\pi i} \int_{\partial P} \frac{zf'(z)}{f(z)} dz.$$

Se L é o segmento de reta ligando a origem a ω_1 , temos

$$\begin{aligned} \frac{1}{2\pi i} \int_L \frac{zf'(z)}{f(z)} dz - \frac{1}{2\pi i} \int_L \frac{(z + \omega_2)f'(z + \omega_2)}{f(z + \omega_2)} dz &= -\frac{\omega_2}{2\pi i} \int_L \frac{f'(z)}{f(z)} dz \\ &= -\frac{\omega_2}{2\pi i} \int_f \frac{1}{w} dw \end{aligned}$$

onde a última integral é sobre o caminho dado pela imagem de f (que é fechado já que $f(0) = f(\omega_1)$). Assim, o valor acima é um múltiplo inteiro

de ω_2 . Analogamente, a integral sobre os outros dois lados opostos de ∂P será um múltiplo inteiro de ω_1 e portanto $S \in \Lambda$, como queríamos. \square

Vamos exibir funções duplamente periódicas (não constantes) explicitamente. Pelo teorema acima, tal função deve ter pelo menos um polo, mas não pode ter apenas um polo simples pois a soma dos resíduos é 0. A próxima coisa mais simples a se tentar é um polo duplo em cada $\omega \in \Lambda$, algo como $\sum_{\omega \in \Lambda} (z - \omega)^{-2}$. Infelizmente esta soma não converge, mas uma pequena modificação resolve este problema:

Definição 9.5. *Seja Λ um reticulado em \mathbb{C} e $\Lambda' = \Lambda \setminus \{0\}$. A função \wp de Weierstraß com relação a Λ é definida como*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

Vamos mostrar que $\wp(z)$ é realmente duplamente periódica, mas antes vamos nos livrar das questões de convergência. Para $n \geq 3$, defina

$$G_n \stackrel{\text{def}}{=} \sum_{\omega \in \Lambda'} \frac{1}{\omega^n}$$

que é absolutamente convergente (observe que $G_n = 0$ se n é ímpar). De fato, quebramos a soma em “camadas de cebola” (quadrada, é claro), onde a k -ésima camada é formada pelos pontos de Λ' sobre os lados do paralelogramo de vértices $k(\omega_1 + \omega_2)$, $k(\omega_1 - \omega_2)$, $k(-\omega_1 + \omega_2)$ e $k(-\omega_1 - \omega_2)$. Seja $d > 0$ a distância entre a origem e o paralelogramo da primeira camada. Temos $8k$ pontos na k -ésima camada, logo

$$|G_n| \leq \sum_{k \geq 1} \frac{8k}{(kd)^n} = \frac{8}{d^n} \sum_{k \geq 1} \frac{1}{k^{n-1}} = \frac{8}{d^n} \cdot \zeta(n-1) < \infty$$

pois $n \geq 3$.

Agora suponha que $|z| \leq R$. Para $|\omega|$ suficientemente grande, temos

$$\left| \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2(z - \omega)^2} \right| \leq \frac{c}{|\omega|^3}$$

para alguma constante c . Pelas estimativas anteriores, com exceção de um número finito de termos, a soma em $\wp(z)$ converge absoluta e

uniformemente no disco $|z| \leq R$, logo $\wp(z)$ é meromorfa. Ela possui polos duplos apenas em Λ . Para mostrar que $\wp(z)$ é duplamente periódica, é mais fácil trabalhar com a derivada

$$\wp'(z) = - \sum_{\omega \in \Lambda} \frac{2}{(z - \omega)^3}$$

que é claramente duplamente periódica. Seja $f(z) = \wp(z + \omega_1) - \wp(z)$. Como $\wp'(z)$ é duplamente periódica, $f'(z) = 0$, logo $f(z)$ é constante. Mas $\wp(z)$ é uma função par, logo $f(-\omega_1/2) = 0$ e assim $f(z) = 0$. Analogamente $\wp(z + \omega_2) = \wp(z)$, o que completa a prova.

Teorema 9.6. *A função \wp satisfaz a equação diferencial*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2 \cdot \wp(z) - g_3$$

onde

$$g_2 = 60G_4 = 60 \sum_{\omega \in \Lambda'} \frac{1}{\omega^4} \quad e \quad g_3 = 140G_6 = 140 \sum_{\omega \in \Lambda'} \frac{1}{\omega^6}.$$

DEMONSTRAÇÃO: Vamos determinar a expansão em série de Taylor de $\wp(z)$ e $\wp'(z)$ em torno do 0. Para $|z| < |\omega|$, temos $(z - \omega)^{-1} = -\frac{1}{\omega} \sum_{n \geq 0} (z/\omega)^n$. Derivando,

$$-\frac{1}{(z - \omega)^2} = -\frac{1}{\omega} \sum_{n \geq 0} n \left(\frac{z}{\omega}\right)^{n-1} \frac{1}{\omega} \iff \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} = \sum_{n \geq 1} \frac{(n+1)z^n}{\omega^{n+2}}$$

Assim,

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \sum_{n \geq 1} \frac{(n+1)z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n \geq 1} (2n+1)G_{2n+2} \cdot z^{2n}$$

pois $G_{2n+1} = 0$. Portanto

$$\begin{aligned}
 & \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 \\
 &= \left(-\frac{2}{z^3} + \sum_{n \geq 1} 2n(2n+1)G_{2n+2}z^{2n-1} \right)^2 \\
 &\quad - 4 \cdot \left(\frac{1}{z^2} + \sum_{n \geq 1} (2n+1)G_{2n+2}z^{2n} \right)^3 \\
 &\quad + 60G_4 \cdot \left(\frac{1}{z^2} + \sum_{n \geq 1} (2n+1)G_{2n+2}z^{2n} \right) + 140G_6 \\
 &= \left(\frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + (36G_4 - 168G_8)z^2 + \dots \right) \\
 &\quad - 4 \cdot \left(\frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + \dots \right) \\
 &\quad + 60G_4 \cdot \left(\frac{1}{z^2} + 3G_4z^2 + \dots \right) + 140G_6 \\
 &= (108G_4^2 - 252G_8)z^2 + \dots
 \end{aligned}$$

que uma função holomorfa duplamente periódica, logo é constante. Como esta função é 0 para $z = 0$, esta constante deve ser 0, o que completa a prova. \square

Observe que o teorema anterior assevera que para qualquer $z \in \mathbb{C}$ o ponto $(\wp(z), \wp'(z))$ de \mathbb{C}^2 é um ponto da curva elíptica E de equação $y^2 = 4x^3 - g_2 \cdot x - g_3$! (o coeficiente 4 não é importante, podemos nos livrar dele fazendo $y \leftarrow 2y$ por exemplo). Podemos até incluir o “ponto no infinito” fazendo-o corresponder a $z = 0$. Assim, obtemos um mapa

$$\begin{aligned}
 \mathbb{C}/\Lambda &\rightarrow E \\
 z \bmod \Lambda &\mapsto (z^3\wp(z) : z^3\wp'(z) : z^3)
 \end{aligned}$$

De fato, as figuras das seções anteriores mostram um “corte” de um toro em $\mathbb{C}^2 = \mathbb{R}^4$ por um plano \mathbb{R}^2 . Note por exemplo que a primeira figura é um corte transversal, definindo dois “círculos” (lembre-se de incluir o ponto do infinito na segunda componente conexa!).

Agora vamos mostrar que este mapa é uma bijeção e que a soma natural \mathbb{C}/Λ corresponde à soma dada pela lei da corda-tangente em E . Em outras palavras, o mapa acima é um isomorfismo de grupos abelianos! Com esta identificação, completaremos a demonstração da

associatividade da lei da corda-tangente, pois a operação em \mathbb{C}/Λ é obviamente associativa!

Teorema 9.7 (Curvas Elípticas como Rosquinhas). *1. O mapa acima é uma bijeção.*

2. Sejam P_1, P_2 e P_3 três pontos da curva elíptica $y^2 = 4x^3 + g_2x - g_3$ correspondentes a três pontos $z_1, z_2, z_3 \in \mathbb{C}$. Temos que P_1, P_2 e P_3 estão alinhados se, e somente se, $z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda}$.

DEMONSTRAÇÃO: (1) Vamos mostrar primeiro a injetividade no caso afim, deixando para o leitor as modificações no caso projetivo. Suponha que $(\wp(z), \wp'(z)) = (\wp(w), \wp'(w))$. Considere $\wp(z) - \wp(w)$ como uma função em z . No paralelogramo fundamental, esta função tem um único polo de ordem 2, logo ela tem também exatamente 2 zeros, que são claramente $\pm w$ a menos que $w \equiv -w \pmod{\Lambda}$. Mas neste caso $\wp'(w) = 0$ (veja exercício 9.6), logo w é um zero duplo. Logo temos em qualquer caso que $\wp(z) = \wp(w) \iff z \equiv \pm w \pmod{\Lambda}$. Como $\wp'(z) = \wp'(w)$ por hipótese, se $z \equiv -w \pmod{\Lambda}$ então $-\wp'(w) = \wp'(-w) = \wp'(w) \iff \wp'(w) = 0$ e novamente $w \equiv -w \pmod{\Lambda}$. Assim, $z \equiv w \pmod{\Lambda}$, como queríamos demonstrar.

Agora, a sobrejetividade. Seja (a, b) um ponto de E . Então, no paralelogramo fundamental, $\wp(z) - a$ tem um polo duplo e portanto dois zeros, z_0 e $-z_0$ (se $z_0 \equiv -z_0 \pmod{\Lambda}$, então como acima z_0 é um zero duplo). Como $(\wp(z_0), \wp'(z_0))$ e $(\wp(-z_0), \wp'(-z_0)) = (\wp(z_0), -\wp'(z_0))$ são ambos pontos em E com a mesma coordenada $x = a$, um deles deve ser igual a (a, b) .

(2) Seja $y = mx + c$ a equação de uma reta e $P_1 = (\wp(z_1), \wp'(z_1))$, $P_2 = (\wp(z_2), \wp'(z_2))$ e $P_3 = (\wp(z_3), \wp'(z_3))$ os três pontos de interseção com a curva elíptica E . No paralelogramo fundamental, a função $\wp'(z) - m\wp(z) - c$ tem um único polo triplo na origem, assim seus três zeros somam 0 módulo Λ pelo teorema 9.4. Mas estes três zeros são exatamente z_1, z_2 e z_3 , o que termina a prova. \square

Como último resultado, observamos que devido ao teorema seguinte, cuja demonstração pode ser encontrada em [140], toda curva elíptica sobre \mathbb{C} não singular (isto é, tal que o discriminante $\Delta = -4(a^3 - 27b^2)$ do polinômio cúbico $4x^3 - ax - b$ é não zero, o que significa que $4x^3 - ax - b$ não possui raízes múltiplas) pode ser realizada como um toro complexo para algum reticulado conveniente.

Teorema 9.8 (Uniformização). *Sejam $a, b \in \mathbb{C}$ tais que $a^3 - 27b^2 \neq 0$. Então existe um único reticulado Λ tal que $g_2(\Lambda) = a$ e $g_3(\Lambda) = b$.*

Problemas Propostos

9.1 (OBM2001). *Considere o ponto racional $P = (3, 8)$ na curva elíptica $y^2 = x^3 - 43x + 166$. Calcule $2001P$.*

9.2. (Fórmula de adição) *Prove:*

$$\wp(z+w) = \frac{1}{4} \cdot \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2 - \wp(z) - \wp(w)$$

onde $\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}$ deve ser interpretado como $\frac{\wp''(z)}{\wp'(z)}$ para $z = w$.

9.3. *Mostre que para uma curva elíptica sobre \mathbb{C} temos um isomorfismo $E[n] \cong \mathbb{Z}/(n) \times \mathbb{Z}/(n)$ de grupos abelianos, onde $E[n]$ é o conjunto de pontos P tais que $nP = O$.*

9.4. *Mostre que uma curva elíptica possui no máximo 9 pontos de inflexão.*

9.5. *Mostre que qualquer função duplamente periódica par é uma função racional em $\wp(z)$. Conclua que qualquer função duplamente periódica é uma função racional em $\wp(z)$ e $\wp'(z)$.*

Dica: Para f par, sejam $\pm a_1, \dots, \pm a_n$ e $\pm b_1, \dots, \pm b_m$ as listas de zeros e polos de f distintos da origem no paralelogramo fundamental (multiplicidades contadas, é claro). Mostre que

$$f(z) \cdot \frac{\prod_{1 \leq i \leq m} (\wp(z) - \wp(b_i))}{\prod_{1 \leq i \leq n} (\wp(z) - \wp(a_i))}$$

é homolorfa e portanto constante.

9.6. *Mostre que os zeros de $\wp'(z)$ no paralelogramo fundamental são os pontos de ordem 2 em \mathbb{C}/Λ , ou seja, $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ e $\frac{\omega_1 + \omega_2}{2}$. Conclua que*

$$\begin{aligned} \wp'(z)^2 &= 4\wp(z)^3 - g_2\wp(z) - g_3 \\ &= 4\left(\wp(z) - \wp\left(\frac{\omega_1}{2}\right)\right) \cdot \left(\wp(z) - \wp\left(\frac{\omega_2}{2}\right)\right) \cdot \left(\wp(z) - \wp\left(\frac{\omega_1 + \omega_2}{2}\right)\right) \end{aligned}$$

9.7. *Dada uma curva elíptica definida sobre \mathbb{Q} , mostre que as coordenadas dos pontos complexos de ordem n são números algébricos.*

Dica: utilize o fato de que um número em \mathbb{C} é algébrico se, e somente se, sua órbita por qualquer automorfismo de \mathbb{C} é finita.

Parte III

Apêndices

Apêndice A

O Teorema dos Números Primos

(por Jorge Aarão)

Seja $\mathbb{N} = \{1, 2, \dots\}$ o conjunto dos naturais e \mathbb{Z} o dos inteiros. Por $\sum_{n \geq 1} a_n$ entenderemos a série $\sum_{n=1}^{\infty} a_n$, por $\sum_p b_p$ entenderemos o somatório sobre os números primos. Se $q \in \mathbb{N}$, $\sum_{p|q} b_p$ significa a soma apenas sobre os primos que dividem q . As mesmas considerações valem para os produtos $\prod_{n \geq 1} a_n$, $\prod_p b_p$, etc.

O máximo divisor comum entre q e ℓ será indicado por (q, ℓ) , e a função de Euler será $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ definida por

$$\varphi(q) = \text{card } \{x \in \mathbb{N}, (x, q) = 1, x \leq q\}.$$

Algumas outras funções são:

$$\pi(x) = \sum_{p \leq x} 1 = \text{card } \{\text{primos menores ou iguais a } x\},$$

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z}; n \leq x\}.$$

Se $(q, \ell) = 1$ temos também

$$\begin{aligned} \pi(x; q, \ell) &= \sum_{\substack{p \leq x \\ p \equiv \ell \pmod{q}}} 1 \\ &= \text{card } \{\text{primos } \leq x \text{ na progressão } (\ell + nq), n \in \mathbb{Z}\}. \end{aligned}$$

Para $s \in \mathbb{C}$, escreveremos $\sigma = \Re s$ sempre que não haja ambiguidade. Diremos que $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ é $O(x)$ quando $f(x) \leq Cx$ para alguma constante C e x grande.

O objetivo principal deste trabalho é provar os seguintes teoremas:

Teorema A.1 (Teorema dos Números Primos). *Tem-se que*

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Teorema A.2 (Teorema dos Números Primos em PAs). *Se $(\ell, q) = 1$, então*

$$\lim_{x \rightarrow \infty} \frac{\pi(x; q, \ell)}{x/\log x} = \frac{1}{\varphi(q)}.$$

O primeiro destes teoremas foi conjecturado por Legendre e Gauß mas as primeiras demonstrações só apareceram cem anos depois, dadas independentemente por Hadamard e de La Vallée Poussin, ambas de 1896, e usando ideias devidas a Riemann. O segundo pode ser achado em Landau [3]. Para uma nota histórica detalhada, ver Edwards [2], que traz inclusive uma tradução para o inglês do trabalho original de Riemann.

As demonstrações que exibiremos para ambos teoremas se apóiam num único resultado de variáveis complexas, que é uma adaptação de um teorema apresentado por Wiener em [8]:

Teorema A.3. *Seja $f: [1, \infty) \rightarrow \mathbb{R}$ integrável em qualquer intervalo finito, não negativa, não decrescente e $O(x)$. Defina a função*

$$g(s) = s \int_1^\infty f(x) x^{-1-s} dx,$$

onde s é uma variável complexa.

Esta integral representa uma função analítica em $\Re s > 1$, e se existe constante c tal que

$$g(s) - \frac{c}{s-1}$$

possui continuação analítica sobre a reta $\Re s = 1$, então

$$\lim_{x \rightarrow \infty} \frac{f(x)}{x} = c.$$

Este teorema, que fornece um meio (nada ortodoxo) de se calcular os limites que desejamos, é devido a Ikehara e Wiener (ver [8]), embora nossa demonstração seja de Newman [5] conforme apresentada por Korevaar [4]. Esta demonstração se divide em dois passos: no primeiro, usando o teorema A.19 que fornece condições para convergência de integrais impróprias usando a transformada de Laplace, provamos que $\int_1^\infty \left(\frac{f(x)}{x} - c \right) \frac{dx}{x}$ converge; como segundo passo demonstramos que a convergência desta integral implica na existência do limite $\frac{f(x)}{x} \rightarrow c$ (ver teorema A.20).

Evidentemente será necessária uma preparação para provar que a função $g(s) - \frac{c}{s-1}$ competente em cada caso possui continuação analítica sobre $\Re s = 1$, e para tanto apresentaremos a função zeta de Riemann e suas propriedades básicas, bem como a noção de caráter de um grupo abeliano finito e as L -séries de Dirichlet.

A distribuição deste material pelas seguintes seções será:

Seção A.1: Propriedades básicas da função zeta de Riemann, definição da função de Tchebyshev $\psi(x)$, sua relação com a função zeta e com $\pi(x)$.

Seção A.2: Demonstração do teorema de Newman e sua aplicação ao teorema dos números primos.

Seção A.3: Propriedades dos caracteres e das L -séries de Dirichlet, definição da função de Tchebyshev em progressões aritméticas e sua relação com $\pi(x; q, \ell)$. Para demonstrar o teorema em progressões necessitaremos do lema de Landau, que será provado na seção A.4.

Para os fatos básicos de teoria dos números utilizamos os textos seguintes: Serre [6], Apostol [1], Edwards [2] e o artigo de Korevaar [4].

A.1 Os Conceitos Básicos

A.1.1 A Função Zeta de Riemann

Para motivar o que segue, apresentamos a demonstração de Euler de que há infinitos primos: partindo da identidade

$$(1) \quad \sum_{n \geq 1} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1},$$

válida para $s > 1$ (e que demonstraremos posteriormente), tomamos o logaritmo obtendo

$$\log\left(\sum_{n \geq 1} \frac{1}{n^s}\right) = - \sum_p \log(1 - p^{-s}),$$

e a expansão do logaritmo em série de potências fornece

$$\log\left(\sum_{n \geq 1} \frac{1}{n^s}\right) = \sum_p \sum_{m \geq 1} \frac{1}{mp^{ms}} = \sum_p \frac{1}{p^s} + \sum_p \sum_{m \geq 2} \frac{1}{mp^{ms}},$$

porém

$$\sum_p \sum_{m \geq 2} \frac{1}{mp^{ms}} < \sum_p \sum_{m \geq 2} \frac{1}{p^m} = \sum_p \frac{1}{p(p-1)} < \sum_{n \geq 2} \frac{1}{n(n-1)} = 1.$$

Como $\lim_{s \rightarrow 1+} \sum_{n \geq 1} \frac{1}{n^s} = +\infty$, obtemos pois que $\lim_{s \rightarrow 1+} \sum_p \frac{1}{p^s} = +\infty$, logo $\sum_p \frac{1}{p}$ diverge e há infinitos primos.

A força deste argumento reside na identidade (1) e, em última análise, na função $\sum_{n \geq 1} \frac{1}{n^s}$.

Definição A.4. A função zeta de Riemann, indicada por $\zeta(s)$, é a única extensão meromorfa de $\sum_{n \geq 1} \frac{1}{n^s}$ para o plano complexo \mathbb{C} .

Observação A.5. A expressão $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ é válida em $\Re s > 1$, pois a série $\sum_{n \geq 1} \frac{1}{n^s}$ converge uniformemente em $\Re s \geq \delta$ para todo $\delta > 1$, e representa portanto em $\Re s > 1$ uma função analítica que coincide com $\zeta(s)$.

Evidentemente a função zeta possui um polo em $s = 1$, e nossa primeira proposição analisa este fato:

Proposição A.6. A função possui um único polo em $\Re s > 0$; este polo é simples, de resíduo 1 e localizado em $s = 1$.

Para demonstrar este resultado provaremos o seguinte lema:

Lema A.7 (Lema da representação integral). *Seja $f(s)$ uma função meromorfa e $(a_n)_{n \in \mathbb{N}}$ uma sequência complexa tal que $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ em $\Re s > a$. Sendo $P(x) = \sum_{n \leq x} a_n$, suponha que $\sum_{n \geq 1} \frac{P(n)}{n^s}$ e $\sum_{n \geq 1} \frac{P(n-1)}{n^s}$ convergem em $\Re s > b$, e que $\int_1^\infty P(x)x^{-1-s}dx$ representa uma função analítica em $\Re s > c$. Então*

$$f(s) = s \int_1^\infty P(x)x^{-1-s}dx$$

em $\Re s > c$.

DEMONSTRAÇÃO: As seguintes igualdades são válidas em $\Re s > \max\{a, b\}$

$$\begin{aligned} f(s) &= \sum_{n \geq 1} \frac{a_n}{n^s} = \sum_{n \geq 1} \frac{P(n) - P(n-1)}{n^s} \\ &= \sum_{n \geq 1} \frac{P(n)}{n^s} - \sum_{n \geq 1} \frac{P(n-1)}{n^s} = \sum_{n \geq 1} \frac{P(n)}{n^s} - \sum_{n \geq 1} \frac{P(n)}{(n+1)^s} \\ &= \sum_{n \geq 1} P(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) = \sum_{n \geq 1} sP(n) \int_n^{n+1} x^{-1-s} dx \\ &= s \sum_{n \geq 1} \int_n^{n+1} P(x)x^{-1-s} dx = s \int_1^\infty P(x)x^{-1-s} dx \end{aligned}$$

Segue-se o resultado em $\Re s > c$ por continuação analítica. \square

DEMONSTRAÇÃO: (DA PROPOSIÇÃO A.6) Com $P(x) = \lfloor x \rfloor$, temos que $\sum_{n \geq 1} \frac{P(n)}{n^s}$ e $\sum_{n \geq 1} \frac{P(n-1)}{n^s}$ convergem em $\Re s > 2$, e $\int_1^\infty P(x)x^{-1-s}dx$ representa uma função analítica em $\Re s > 1$, logo

$$\zeta(s) = s \int_1^\infty \lfloor x \rfloor x^{-1-s} dx \text{ em } \Re s > 1.$$

Como $s \int_1^\infty x \cdot x^{-1-s} dx = 1 + \frac{1}{s-1}$, temos

$$\zeta(s) = 1 + \frac{1}{s-1} + s \int_1^\infty (\lfloor x \rfloor - x)x^{-1-s} dx,$$

e esta última integral é convergente em $\Re s > 0$, isto é, representa uma função analítica neste domínio, seguindo-se nosso resultado. \square

Vamos agora proceder à demonstração da identidade fundamental (1), com uma generalidade que será necessária na seção A.3.

Definição A.8. *Uma função $f: \mathbb{N} \rightarrow \mathbb{C}$ é dita multiplicativa se $f(m \cdot n) = f(m) \cdot f(n)$ sempre que $(m, n) = 1$, e estritamente multiplicativa se $f(m \cdot n) = f(m) \cdot f(n)$ sem restrições.*

Proposição A.9. *Seja $f: \mathbb{N} \rightarrow \mathbb{C}$ multiplicativa e limitada. Então*

$$\sum_{n \geq 1} \frac{f(n)}{n^s} = \prod_p \left(\sum_{m \geq 0} f(p^m) p^{-ms} \right)$$

em $\Re s > 1$. No caso estritamente multiplicativo temos

$$\sum_{n \geq 1} \frac{f(n)}{n^s} = \prod_p (1 - p^{-s} f(p))^{-1}$$

no mesmo domínio.

DEMONSTRAÇÃO: Como f é limitada a série $\sum_{n \geq 1} \frac{f(n)}{n^s}$ converge uniformemente em $\Re s \geq \delta$ para todo $\delta > 1$. Chamaremos $S = \sum_{n \geq 1} \frac{f(n)}{n^s}$ e $P(x) = \prod_{p \leq x} (1 + f(p)/p^s + f(p^2)/p^{2s} + \cdots)$, s fixo com $\Re s > 1$.

Como $P(x)$ é o produto finito de séries absolutamente convergentes podemos reescrever $P(x) = \sum_{n \in N_x} \frac{f(n)}{n^s}$, onde N_x é o conjunto dos inteiros cujos fatores primos são menores ou iguais a x . Observando enfim que os inteiros entre 1 e x estão em N_x obtemos

$$|P(x) - S| \leq \sum_{n > x} \left| \frac{f(n)}{n^s} \right|,$$

e como S converge absolutamente temos que $\lim_{x \rightarrow \infty} P(x) = S$. Mais precisamente, se $\Re a \geq \delta$ com $\delta > 1$, a convergência uniforme de S implica que $P(x)$ converge uniformemente a S neste domínio.

Sendo f estritamente multiplicativa teremos $f(p^m) = (f(p))^m$, daí

$$\sum_{m \geq 0} f(p^m) p^{-ms} = \sum_{m \geq 0} (f(p) p^{-s})^m = \frac{1}{1 - f(p) p^{-s}}$$

□

Corolário A.10. (a) (*Fórmula de Euler*)

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}, \text{ em } \Re s > 1.$$

(b) $\zeta(s) \neq 0$ em $\Re s > 1$.

DEMONSTRAÇÃO: (b) Por (a) temos em $\Re s \geq \sigma > 1$ que

$$\frac{1}{|\zeta(s)|} = \prod_p |1 - p^{-s}| \leq \prod_p \left(1 + \frac{1}{|p^s|}\right) \leq \prod_p \left(1 + \frac{1}{p^\sigma}\right).$$

Provando que o último produto é finito obteremos

$$0 < \frac{1}{\prod_p (1 + \frac{1}{p^\sigma})} \leq |\zeta(s)|.$$

Provaremos que se $\sum_{i \geq 1} a_i$ converge com $a_i \geq 0$, então $\prod_{i \geq 1} (1 + a_i)$ converge. Sem perda de generalidade podemos supor $a_i < 1 - a_i$, e definindo $P_n = \prod_{i=1}^n (1 + a_i)$ obtemos:

$$\begin{aligned} \log P_n &= \sum_{i=1}^n \log(1 + a_i) = \sum_{i=1}^n \sum_{m \geq 1} \frac{(-1)^{m+1} a_i^m}{m} \leq \sum_{i=1}^n \sum_{m \geq 1} a_i^m \\ \log P_n &\leq \sum_{i=1}^n a_i + \sum_{i=1}^n \frac{a_i^2}{1 - a_i} \leq \sum_{i=1}^n a_i + \sum_{i=1}^n a_i \leq 2 \sum_{i \geq 1} a_i = 2S. \end{aligned}$$

Dessa forma

$$P_n \leq e^{2S} \text{ para todo } n \text{ e } \lim_{n \rightarrow \infty} P_n = \prod_{i \geq 1} (1 + a_i) \leq e^{2S}.$$

□

Observemos que este corolário nos permitirá tomar logaritmos da função zeta em $\Re s > 1$.

Conforme já frisamos na seção anterior, estaremos interessados na continuação analítica de certas funções sobre a reta $\Re s = 1$, e com esse objetivo surge a proposição seguinte:

Proposição A.11. *Em $\Re s = 1$ temos $\zeta(s) \neq 0$.*

DEMONSTRAÇÃO: (Mertens, 1889) Observemos que $3 + 4 \cos \theta + \cos 2\theta = 2(1 + \cos \theta)^2 \geq 0$, onde $\theta \in \mathbb{R}$.

Vamos supor que para algum b real não nulo temos $\zeta(1 + ib) = 0$, definimos $\varphi(s) = \zeta^3(s)\zeta^4(s + ib)\zeta(s + 2ib)$.

Dessa forma $s = 1$ é um zero de φ pois o polo simples de ζ não cancela o zero em $s = 1 + ib$. Consequentemente

$$\lim_{s \rightarrow 1} \log |\varphi(s)| = -\infty.$$

Agora com s real maior que 1 temos

$$\begin{aligned} \log |\zeta(s + it)| &= \Re \log \zeta(s + it) = \Re \log \prod_p (1 - p^{-s-it})^{-1} \\ &= -\Re \sum_p \log(1 - p^{-s-it}) \\ &= \Re \sum_p \left(p^{-s-it} + \frac{1}{2}(p^2)^{-s-it} + \frac{1}{3}(p^3)^{-2-it} + \dots \right), \end{aligned}$$

onde o logaritmo foi tomado de acordo com o desenvolvimento em série na última igualdade. Podemos escrever o último somatório como

$$\log |\zeta(s + it)| = \Re \sum_{n \geq 1} a_n n^{-s-it},$$

onde $a_n \geq 0$. Daí obtemos

$$\begin{aligned} \log |\varphi(s)| &= 3\Re \sum_{n \geq 1} a_n n^{-s} + 4\Re \sum_{n \geq 1} a_n n^{-s-ib} + \Re \sum_{n \geq 1} a_n n^{-s-2ib} \\ &= \Re \sum_{n \geq 1} a_n n^{-s} (3 + 4n^{-ib} + n^{-2ib}). \end{aligned}$$

Finalmente,

$$\log |\varphi(s)| = \sum_{n \geq 1} a_n n^{-s} (3 + 4 \cos(b \log n) + \cos(2b \log n)) \geq 0.$$

contrariando o limite $\lim_{s \rightarrow 1} \log |\varphi(s)| = -\infty$. □

Unindo as proposições A.6 e A.11 obtemos

Proposição A.12. *A função $-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ possui continuação analítica sobre a reta $\Re s = 1$.*

DEMONSTRAÇÃO: Pela proposição A.6 a função $-\frac{\zeta'(s)}{\zeta(s)}$ possui um polo de tipo $\frac{1}{s-1}$, e pela proposição A.11 ele é o único sobre a reta $\Re s = 1$.

Observe também que esta função é analítica em $\Re s > 1$ (corolário A.10).

□

A.1.2 A Função $\psi(x)$

Definição A.13. *A função $\psi: \mathbb{R}^+ \rightarrow \mathbb{R}$ é definida por*

$$\psi(x) = \sum_{n \leq x} \Lambda(n),$$

onde

$$\Lambda(n) = \begin{cases} \log p & \text{se } n \text{ é potência do primo } p; \\ 0 & \text{caso contrário.} \end{cases}$$

A função Λ é a chamada função de von Mangoldt, enquanto ψ é a função de Tchebyshev. Podemos também escrever

$$\psi(x) = \sum_{p^n \leq x} \log p = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

Proposição A.14. *A função $g(s) = s \int_1^\infty \psi(x) x^{-1-s} dx$ é analítica em $\Re s > 1$ e neste domínio $g(s) = -\frac{\zeta'(s)}{\zeta(s)}$.*

DEMONSTRAÇÃO: Como $\psi(x) \leq x \log x$, segue-se a primeira afirmativa. Por outro lado temos em $\Re s > 1$

$$\log \zeta(s) = - \sum_p \log(1 - p^{-s}) = \sum_p \sum_{m \geq 1} \frac{1}{mp^{ms}},$$

e a convergência uniforme da última série em $\Re s \geq \delta > 1$ nos permite derivar dentro do somatório. Assim sendo,

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{p^{-s}}{1-p^{-s}} \log p = \sum_p (p^{-s} + p^{-2s} + \cdots) \log p = \sum_{n \geq 1} \Lambda(n) n^{-s}.$$

Usamos agora o lema da representação integral com $a_n = \Lambda(n)$, $P(x) = \psi(x)$. Como $\psi(n) \leq n^2$, as igualdades envolvidas são válidas em $\Re s > 3$. Daí $g(s) = -\frac{\zeta'(s)}{\zeta(s)}$ em $\Re s > 1$. \square

Proposição A.15. *A seguinte equivalência ocorre:*

$$\lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1 \Leftrightarrow \lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

DEMONSTRAÇÃO: Temos que

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \leq \log x \sum_{p \leq x} 1 = \pi(x) \cdot \log x.$$

Por outro lado se $1 < y < x$,

$$\pi(x) = \pi(y) + \sum_{y < p \leq x} 1 \leq \pi(y) + \sum_{y < p \leq x} \frac{\log p}{\log y} < y + \frac{\psi(x)}{\log y}.$$

Para x suficientemente grande temos $1 < \frac{x}{\log^2 x} < x$, logo

$$\pi(x) < \frac{x}{\log^2 x} + \frac{\psi(x)}{\log \left(\frac{x}{\log^2 x} \right)},$$

$$\frac{\pi(x) \log x}{x} < \frac{1}{\log x} + \frac{\psi(x)}{x} \frac{\log x}{\log x - 2 \log \log x}.$$

Como $\lim_{x \rightarrow \infty} \frac{\log x}{\log x - 2 \log \log x} = 1$, segue-se o desejado. \square

Proposição A.16. *A função ψ é $O(x)$.*

DEMONSTRAÇÃO: O número $\binom{2n}{n}$ é divisível por todos os primos em $(n, 2n]$, logo

$$\prod_{n < p \leq 2n} p \leq \binom{2n}{n} < \sum_{i=0}^{2n} \binom{2n}{i} = 2^{2n}$$

$$\sum_{n < p \leq 2n} \log p < 2n \log 2.$$

Daqui vem

$$\sum_{2^{k-1} < p \leq 2^k} \log p \leq 2^k \log 2$$

$$\sum_{p \leq 2^k} \log p \leq \sum_{i=0}^k 2^i \cdot \log 2 < 2^{k+1} \cdot \log 2$$

Se k é um inteiro tal que $2^{k-1} < x \leq 2^k$ temos

$$\sum_{p \leq x} \log p \leq \sum_{p \leq 2^k} \log p < 2^{k+1} \log 2 = (4 \log 2) \cdot 2^{k-1} < 4x \log 2.$$

Para $m > 1$ fixo temos

$$\sum_{p^m \leq x} \log p = \sum_{p \leq x^{1/m}} \log p < 4 \log 2 \cdot x^{1/m},$$

e é claro que se para algum $m > 1$ existe um primo p tal que $p^m \leq x$, então $2^m \leq x$. Daí teremos

$$\begin{aligned} \psi(x) &= \sum_{p \leq x} \log p + \sum_{m \geq 2} \sum_{p^m \leq x} \log p \\ &= \sum_{p \leq x} \log p + \sum_{p \leq x^{1/2}} \log p + \cdots + \sum_{p \leq x^\alpha} \log p, \end{aligned}$$

como $\alpha = \frac{1}{\left\lfloor \frac{\log x}{\log 2} \right\rfloor}$. Assim sendo

$$\begin{aligned} \psi(x) &\leq 4 \log 2 \cdot x + 4 \log 2 \cdot \sum_{m=2}^{1/\alpha} x^{1/2} \\ &\leq 4x \log 2 + 4x^{1/2} \log 2 \cdot \alpha^{-1} \\ \psi(x) &< 4x \log 2 + 4x^{1/2} \log x, \end{aligned}$$

e isso completa nosso resultado. \square

A.2 Teoremas Tauberianos e o Teorema dos Números Primos

A.2.1 Teoremas Tauberianos

Na seção anterior demonstramos que $-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ possui continuação analítica sobre a reta $\Re s = 1$. Em $\Re s > 1$ vale a expressão

$$-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1} = 1 + s \int_1^\infty (\psi(x) - x)x^{-1-s} dx,$$

e apesar da continuação analítica ainda não temos garantias de que a última integral vá convergir para $\Re s = 1$. Porém, se este é o caso, então em particular para $s = 1$ a integral $\int_1^\infty (\psi(x) - x)x^{-2} dx$ converge e há um modo de provar que isto implica na existência do limite de $\frac{\psi(x) - x}{x}$ quando x cresce, e este limite é zero. Esta é exatamente a equivalência enunciada na última seção para o teorema dos números primos. Esta seção se dedica a demonstrar os teoremas da análise que garantirão a existência do limite acima. O primeiro demonstra a convergência da integral, e a demonstração que apresentamos é devida a Newman [5], na forma exposta em Korevaar [4]; o segundo prova a existência do limite, e a demonstração vem das mesmas fontes.

Começamos com dois lemas:

Lema A.17. *Se $F: (0, \infty) \rightarrow \mathbb{R}$ é limitada e integrável em qualquer subintervalo finito, então a transformada de Laplace de F , definida por*

$$G(z) = \int_0^\infty F(t)e^{-zt} dt$$

está bem definida e é analítica no semiplano $\Re z > 0$.

DEMONSTRAÇÃO: Como a transformada de Laplace é bem conhecida, damos apenas uma referência: Widder [7]. \square

Lema A.18. *Se $f: [1, \infty) \rightarrow \mathbb{R}$ é integrável em qualquer subintervalo finito, não negativa, não decrescente, e $O(x)$, então a transformada de Mellin de f , dada por*

$$g(s) = s \int_1^\infty f(x)x^{-1-s} dx$$

está bem definida e é analítica no semiplano $\Re s > 1$.

DEMONSTRAÇÃO: Como f é $O(x)$, seja $\lambda > 1$ grande o suficiente para que $\left| \frac{f(x)}{x} \right| < C$ quando tivermos $x > \lambda$. Para $\Re s \geq \sigma > 1$ temos:

$$\left| \int_{\lambda}^{\infty} f(x)x^{-1-s}dx \right| \leq \int_{\lambda}^{\infty} \left| \frac{f(x)}{x} \right| x^{-\sigma} dx \leq \frac{C}{\sigma-1} \lambda^{1-\sigma}.$$

Dai

$$\lim_{\lambda \rightarrow \infty} \int_1^{\lambda} f(x)x^{-1-s}dx = \int_1^{\infty} f(x)x^{-1-s}dx$$

uniformemente em $\Re s \geq \sigma > 1$, e isto garante a analiticidade de $g(s)$ em $\Re s > 1$. \square

Teorema A.19. *Seja $F: (0, \infty) \rightarrow \mathbb{R}$ como no lema A.17, G sua transformada de Laplace. Se G possui continuação analítica sobre a reta $\Re z = 0$, então a integral imprópria $\int_0^{\infty} F(t)dt$ converge e*

$$G(0) = \int_0^{\infty} F(t)dt.$$

DEMONSTRAÇÃO: Chamaremos ainda de $G(z)$ a continuação analítica da transformada de Laplace de F numa vizinhança do semiplano $\Re z \geq 0$. Sem perda de generalidade supomos $|F(t)| \leq 1$ e definimos

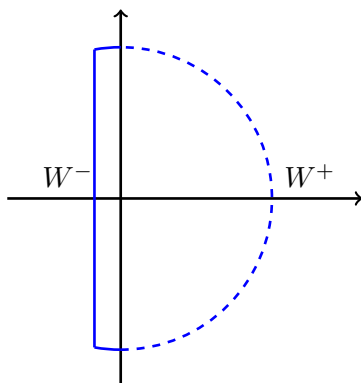
$$G_{\lambda}(z) = \int_0^{\lambda} F(t)e^{-tz}dt,$$

que é analítica em \mathbb{C} para todo $\lambda > 0$ finito.

Mostraremos que

$$G_{\lambda}(0) \rightarrow G(0) \text{ quando } \lambda \rightarrow \infty.$$

Seja $\varepsilon > 0$ dado, tomamos $R = \frac{1}{\varepsilon}$ e olhamos o disco de raio R em torno da origem, isto é, $D_R(0) = \{z \in \mathbb{C} \mid |z| \leq R\}$. Como G é analítica numa vizinhança de $\Re z \geq 0$, existe $\delta = \delta(R) > 0$ pequeno o suficiente para que G seja analítica em $D_R(0) \cap \{\Re z \geq -\delta\}$. A fronteira deste conjunto chamamos de W , sendo $W^+ = \{z \in W \mid \Re z > 0\}$ e $W^- = \{z \in W \mid \Re z < 0\}$.



Pela fórmula de Cauchy,

$$G(0) - G_\lambda(0) = \frac{1}{2\pi i} \int_W \frac{G(z) - G_\lambda(z)}{z} dz.$$

Observe porém que se φ é uma função analítica em $D_R(0) \cap \{\Re z \geq -\delta\}$ temos

$$\begin{aligned} \varphi(0) &= \frac{1}{2\pi i} \int_W \frac{\varphi(z)e^{\lambda z}}{z} dz, \\ 0 &= \frac{1}{2\pi i} \int_W \frac{\varphi(z)e^{\lambda z} z}{R^2} dz. \end{aligned}$$

Somando obtemos

$$\varphi(0) = \frac{1}{2\pi i} \int_W \varphi(z)e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz.$$

Fazendo $\varphi = G - G_\lambda$ e abreviando $I(z) = (G(z) - G_\lambda(z))e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right)$ obtemos a seguinte alteração da fórmula de Cauchy:

$$G(0) - G_\lambda(0) = \int_W I(z) dz.$$

Nosso objetivo agora é dividir o caminho de integração W em partes, e majorar a integral em cada uma delas. A primeira parte é o próprio W^+ . Para a segunda parte, observe que $G(z) \left(\frac{1}{z} + \frac{z}{R^2} \right)$ é analítica sobre W , logo existe B tal que $|G(z) \left(\frac{1}{z} + \frac{z}{R^2} \right)| \leq B$ para todo $z \in W^-$. Definimos $\delta_1 = \delta_1(\varepsilon, \delta, B) > 0$ de tal forma que $0 < \delta_1 < \delta$, e se $W_2^- = \{z \in W^- \mid -\delta_1 \leq \Re z\}$, então

$$\frac{B}{2\pi} \int_{W_2^-} |dz| < \varepsilon.$$

A terceira parte é $W_1^- = \{z \in W^- \mid \Re z < -\delta_1\} = W^- - W_2^-$. Chamamos também de W_*^- o conjunto $\{z \in \mathbb{C} \mid \Re z < 0 \text{ e } |z| = R\}$. Algumas estimativas preliminares antes do resultado final: se $x = \Re z$ e $|z| = R$, então

$$\frac{1}{z} + \frac{z}{R^2} = \frac{\bar{z}}{R^2} + \frac{z}{R^2} = \frac{2x}{R^2}.$$

Se além disso $x > 0$ teremos

$$|G(z) - G_\lambda(z)| \leq \int_\lambda^\infty |F(t)| e^{-xt} dt \leq \frac{e^{-\lambda x}}{x}.$$

Para $x < 0$ tiramos

$$|G_\lambda(z)| \leq \int_0^\lambda e^{-xt} dt = \frac{e^{-\lambda x}}{|x|} - \frac{1}{|x|} < \frac{e^{-\lambda x}}{|x|},$$

e se $z \in W_1^-$

$$|e^{\lambda z}| = e^{\lambda x} \leq e^{-\delta_1 \lambda}.$$

Estamos prontos para avaliar $G(0) - G_\lambda(0)$:

$$2\pi i(G(0) - G_\lambda(0)) = \int_W I(z) dz = \int_{W^+} I(z) dz + \int_{W^-} I(z) dz.$$

Como $G_\lambda(z)$ é analítica em \mathbb{C} , temos que

$$\int_{W^-} G_\lambda(z) e^{\lambda z} \left(\frac{1}{z} + \frac{1}{R^2} \right) dz = \int_{W_*^-} G_\lambda(z) e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz,$$

pelo teorema de Cauchy.

Nossa decomposição fica:

$$\begin{aligned} 2\pi i(G(0) - G_\lambda(0)) &= \int_{W^+} I(z) dz - \int_{W_*^-} G_\lambda(z) e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \\ &\quad + \int_{W_1^-} G(z) e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \\ &\quad + \int_{W_2^-} G(z) e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz. \end{aligned}$$

Mas usando nossas estimativas obtemos:

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{W^+} I(z) dz \right| &\leq \frac{1}{2\pi} \int_{W^+} e^{\lambda x} \cdot \frac{e^{-\lambda x}}{x} \cdot \frac{2x}{R^2} |dz| \\ &= \frac{1}{\pi R^2} \int_{W^+} |dz| = \frac{\pi R}{\pi R^2} = \frac{1}{R} = \varepsilon, \end{aligned}$$

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{W_*^-} G_\lambda(z) e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \right| &\leq \frac{1}{2\pi} \int_{W_*^-} e^{\lambda x} \cdot \frac{e^{-\lambda x}}{|x|} \cdot \frac{2|x|}{R^2} |dz| \\ &= \frac{1}{\pi R^2} \int_{W_*^-} |dz| = \frac{1}{R} = \varepsilon, \end{aligned}$$

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{W_1^-} G(z) e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \right| &\leq \frac{1}{2\pi} \cdot B \cdot e^{-\lambda \delta_1} \cdot \int_{W_1^-} |dz|, \\ \left| \frac{1}{2\pi i} \int_{W_2^-} G(z) e^{\lambda z} \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \right| &\leq \frac{1}{2\pi} \int_{W_2^-} e^{\lambda x} B |dz| \leq \frac{B}{2\pi} \int_{W_2^-} |dz| < \varepsilon. \end{aligned}$$

Logo

$$|G(0) - G_\lambda(0)| \leq 3 \cdot \varepsilon + \frac{B}{2\pi} \cdot \int_{W_1^-} |dz| \cdot e^{-\lambda \delta_1},$$

e tomando λ suficientemente grande obtemos $|G(0) - G_\lambda(0)| < 4\varepsilon$. \square

Passemos agora à nossa versão teorema de Ikehara-Wiener (ver Korevaar [4]):

Teorema A.20. *Seja $f: [1, \infty) \rightarrow \mathbb{R}$ como no lema A.18, e $g(s)$ a sua transformada de Mellin. Se existe $c \in \mathbb{R}$ constante tal que*

$$g(s) - \frac{c}{s-1}$$

possui continuação analítica sobre a reta $\Re s = 1$, então

$$\lim_{x \rightarrow \infty} \frac{f(x)}{x} = c.$$

DEMONSTRAÇÃO:

Primeiro Passo: definimos $F(t) = e^{-t} f(e^t) - c$, para $t > 0$. Assim F é limitada em $(0, \infty)$, pois f é $O(x)$, e integrável em intervalos finitos pois f o é. Sua transformada de Laplace G será

$$G(z) = \int_0^\infty (e^{-t} f(e^t) - c) e^{-zt} dt.$$

Trocando variáveis ($x = e^t$) obtemos

$$\begin{aligned} G(z) &= \int_1^\infty f(x) x^{-2-z} dx - \frac{c}{z} = \frac{g(z+1)}{z+1} - \frac{c}{z} \\ &= \frac{1}{z+1} \left(g(z+1) - \frac{c}{z} - c \right). \end{aligned}$$

Por hipótese, $g(z+1) - \frac{c}{z}$ possui extensão analítica sobre $\Re(z+1) = 1$, logo G possui extensão analítica sobre $\Re z = 0$. Do teorema A.19 concluímos que

$$G(0) = \int_0^\infty (e^{-t}f(e^t) - c)dt = \int_1^\infty \frac{f(x) - cx}{x^2}dx.$$

Segundo Passo: Resta verificar que a convergência da integral implica $\lim_{x \rightarrow \infty} \frac{f(x)}{x} = c$.

De fato, suponhamos que $\limsup \frac{f(x)}{x} > c$, então existe $\delta > 0$ com

$$0 < 2\delta < \limsup \frac{f(x)}{x} - c.$$

Definimos $\rho = \frac{c+2\delta}{c+\delta} > 1$ (observe que $c \geq 0$, caso contrário $\int_1^\infty \frac{f(x)-cx}{x^2}dx \geq \int_1^\infty \frac{-cx}{x^2}dx = +\infty$). Como $\limsup \frac{f(x)}{x} > c$, seja $(y_n)_{n \in \mathbb{N}}$ uma sequência tendendo ao infinito tal que

$$f(y_n) > (c + 2\delta)y_n$$

para todo $n \in \mathbb{N}$.

Para $y_n < x < \rho y_n$ temos (pois f é não decrescente)

$$f(x) \geq f(y_n) > (c + 2\delta)y_n > (c + \delta)x.$$

logo

$$\frac{f(x) - cx}{x} > \delta,$$

e portanto

$$\int_{y_n}^{\rho y_n} \frac{f(x) - cx}{x^2}dx \geq \int_{y_n}^{\rho y_n} \frac{\delta}{x}dx = \delta \log \rho > 0.$$

Como $G(0) = \int_1^\infty \frac{f(x)-cx}{x^2}dx$, dado $\varepsilon > 0$ existe $M > 1$ tal que se $a \geq M$, então

$$\left| \int_a^\infty \frac{f(x) - cx}{x^2}dx \right| < \varepsilon.$$

Tomemos $0 < \varepsilon < \frac{\delta}{2} \log \rho$, como $y_n \rightarrow \infty$ existe $n_0 \in \mathbb{N}$ tal que se $a \geq y_{n_0}$, então

$$\left| \int_a^\infty \frac{f(x) - cx}{x^2}dx \right| < \varepsilon.$$

Mas

$$\begin{aligned} \delta \log \rho &< \left| \int_{y_{n_0}}^{\rho y_{n_0}} \frac{f(x) - cx}{x^2} dx \right| \\ &\leq \left| \int_{y_{n_0}}^{\infty} \frac{f(x) - cx}{x^2} dx \right| + \left| \int_{\rho y_{n_0}}^{\infty} \frac{f(x) - cx}{x^2} dx \right| < 2\varepsilon < \delta \log \rho. \end{aligned}$$

Concluimos que $\limsup \frac{f(x)}{x} \leq c$, e raciocínio análogo para $\liminf \frac{f(x)}{x} \geq c$ conclui que $\lim_{x \rightarrow \infty} \frac{f(x)}{x} = c$. \square

A.2.2 O Teorema dos Números Primos

Teorema A.21. *Tem-se:*

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

DEMONSTRAÇÃO: Pela proposição A.15 é equivalente provar que $\frac{\psi(x)}{x} \rightarrow 1$ quando $x \rightarrow \infty$. A função ψ é não decrescente, não negativa, integrável em intervalos finitos e $O(x)$ pela proposição A.16. Sua transformada de Mellin é

$$g(s) = s \int_1^{\infty} \psi(x) x^{-1-s} dx = -\frac{\zeta'(s)}{\zeta(s)},$$

e pela proposição A.12 $g(s) - \frac{1}{s-1}$ possui continuação analítica sobre $\Re s = 1$. Aplicando o teorema A.20 obtemos que $\lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1$. \square

A.3 Caráteres de Grupos, L -Séries de Dirichlet e o Teorema em Progressões Aritméticas

A.3.1 A Função $\psi(x; q, \ell)$

Nesta seção pretendemos demonstrar que se $(q, \ell) = 1$ então

$$\lim_{x \rightarrow \infty} \frac{\pi(x; q, \ell)}{x/\log x} = \frac{1}{\varphi(q)}.$$

Tentaremos pois imitar o procedimento anterior para $\pi(x)$, e definiremos o equivalente da função ψ . Nesta seção $(q, \ell) = 1$.

Definição A.22.

$$\psi(x; q, \ell) = \sum_{\substack{0 \leq n \leq x \\ n \equiv \ell \pmod{q}}} \Lambda(n).$$

Proposição A.23. *Temos que*

$$\lim_{x \rightarrow \infty} \frac{\pi(x; q, \ell)}{x / \log x} = \frac{1}{\varphi(q)} \Leftrightarrow \lim_{x \rightarrow \infty} \frac{\psi(x; q, \ell)}{x} = \frac{1}{\varphi(q)}.$$

DEMONSTRAÇÃO: Seja $M = \lfloor \frac{\log x}{\log 2} \rfloor$, para $m \geq 2$ fixo temos

$$\sum_{\substack{p^m \leq x \\ p^m \equiv \ell \pmod{q}}} \log p \leq \sum_{p^m \leq x} \log p \leq \log x \sum_{p^m \leq x} 1 = \log x \cdot \pi(x^{1/m}).$$

Desta forma

$$\begin{aligned} \psi(x; q, \ell) &= \sum_{\substack{p \leq x \\ p \equiv \ell \pmod{q}}} \log p + \sum_{\substack{p^m \leq x \\ p^m \equiv \ell \pmod{q} \\ m \geq 2}} \log p \\ &\leq \log x \sum_{\substack{p \leq x \\ p \equiv \ell \pmod{q}}} 1 + \sum_{m=2}^M \log x \cdot \pi(x^{1/m}) \\ &\leq \log x \cdot \pi(x; q, \ell) + M \cdot \log x \cdot \pi(x^{1/2}) \\ &\leq \log x \cdot \pi(x; q, \ell) + \frac{\log^2 x}{\log 2} \pi(x^{1/2}) \end{aligned}$$

Como $\lim_{x \rightarrow \infty} \frac{\log^2 x \cdot \pi(x^{1/2})}{x} = 0$ temos

$$\lim_{x \rightarrow \infty} \frac{\psi(x; q, \ell)}{x} \leq \lim_{x \rightarrow \infty} \frac{\log x}{x} \cdot \pi(x; q, \ell).$$

Por outro lado se $1 < y < x$

$$\pi(x; q, \ell) = \pi(y; q, \ell) + \sum_{\substack{y < p \leq x \\ p \equiv \ell \pmod{q}}} 1 \leq y + \sum_{\substack{y < p \leq x \\ p \equiv \ell \pmod{q}}} \frac{\log p}{\log y} \leq y + \frac{\psi(x; q, \ell)}{\log y}.$$

Tomando $y = \frac{x}{\log^2 x}$ e x adequadamente grande:

$$\frac{\pi(x; q, \ell)}{x / \log x} \leq \frac{1}{\log x} + \frac{\psi(x; q, \ell)}{x} \frac{\log x}{\log x - 2 \log \log x}$$

□

Evidentemente $\psi(x; q, \ell)$ é $O(x)$, não decrescente e integrável em qualquer intervalo finito. Chamando $g(s)$ sua transformada de Mellin, basta provar que $g(s) - \frac{1}{\varphi(q)} \frac{1}{(s-1)}$ possui continuação analítica sobre $\Re s = 1$ para concluir que $\lim_{x \rightarrow \infty} \frac{\psi(x; q, \ell)}{x} = \frac{1}{\varphi(q)}$ (pelo teorema A.20), que é equivalente ao teorema dos números primos em progressões aritméticas. Para demonstrar esta continuação analítica introduzimos os caracteres e as L -séries de Dirichlet.

A.3.2 Caráteres

Definição A.24. *Seja G um grupo abeliano finito. Um caráter de G é um homomorfismo $\chi: G \rightarrow \mathbb{C}^*$. Escreveremos χ_1 para indicar o caráter trivial $\chi_1(x) = 1 \ \forall x \in G$.*

Nesta seção, ao nos referirmos a um grupo G , ele será abeliano finito.

Proposição A.25. *Se $|G| = n$ e χ é caráter de G , então*

$$\sum_{x \in G} \chi(x) = \begin{cases} n, & \text{se } \chi = \chi_1; \\ 0, & \text{caso contrário.} \end{cases}$$

DEMONSTRAÇÃO: O caso a considerar é $\chi \neq \chi_1$. Seja $y \in G$ tal que $\chi(y) \neq 1$. Daí

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x),$$

logo

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0,$$

donde

$$\sum_{x \in G} \chi(x) = 0.$$

□

Se χ e χ' são caracteres de G , podemos definir o produto

$$(\chi \cdot \chi')(x) = \chi(x) \cdot \chi'(x),$$

e isto fornece uma estrutura de grupo abeliano ao conjunto \hat{G} dos caracteres de G .

Proposição A.26. *O grupo \hat{G} é finito da mesma ordem de G .*

DEMONSTRAÇÃO: Se G é cíclico de ordem g , digamos que $G = \langle \sigma \rangle$, então para todo $\chi \in \hat{G}$ temos $[\chi(\sigma)]^g = \chi(\sigma^g) = 1$, ou seja, $\chi(\sigma)$ é raiz g -ésima da unidade. Por outro lado se $w \in \mathbb{C}$ com $w^g = 1$ temos que a aplicação $\sigma^n \mapsto w^n$ é um caráter. Concluimos daí que $|\hat{G}| = g$.

Se G não é cíclico o teorema de representação de grupos abelianos finitos diz que $G \simeq G_1 \oplus G_2 \oplus \cdots \oplus G_n$, onde cada G_i é cíclico de ordem g_i e gerador σ_i . Para aplicar o que concluimos no caso cíclico devemos mostrar que $\hat{G} \simeq \hat{G}_1 \oplus \cdots \oplus \hat{G}_n$. Basta provar que $\widehat{G_1 \oplus G_2} \simeq \hat{G}_1 \oplus \hat{G}_2$ (G_1 e G_2 não necessariamente cíclicos).

Se χ_i é caráter de G_i , $i = 1, 2$ então $(x_1, x_2) \mapsto \chi_1(x_1)\chi_2(x_2)$ é um caráter de $G_1 \oplus G_2$, onde $x_i \in G_i$, $i = 1, 2$. Por outro lado se χ é caráter de $G_1 \oplus G_2$ então $x_1 \mapsto \chi(x_1, e_2)$ é caráter de G_1 e $x_2 \mapsto \chi(e_1, x_2)$ é caráter de G_2 , onde $e_i \in G_i$ é a identidade do grupo G_i , $i = 1, 2$. Como os mapas do tipo $(x_1, x_2) \mapsto \chi_1(x_1)\chi_2(x_2)$ são inversos aos mapas do tipo $x_1 \mapsto \chi(x_1, e_2); x_2 \mapsto \chi(e_1, x_2)$, segue-se o resultado. \square

Proposição A.27. *Se $|G| = n$ e $x \in G$, temos*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n, & \text{se } x = e_G; \\ 0, & \text{caso contrário} \end{cases}$$

DEMONSTRAÇÃO: A aplicação

$$\begin{aligned} x: \hat{G} &\rightarrow \mathbb{C}^* \\ \chi &\mapsto \chi(x) \end{aligned}$$

define um caráter de \hat{G} , isto é, um elemento de $\hat{\hat{G}}$. Aplique agora as proposições A.25 e A.26. \square

As fórmulas enunciadas nas proposições A.25 e A.27 são as chamadas relações de ortogonalidade.

Consideremos agora o caso em que G é o grupo multiplicativo dos elementos invertíveis do anel $\mathbb{Z}/q\mathbb{Z}$, onde $q \geq 1$, dizemos que $(\widehat{\mathbb{Z}/q\mathbb{Z}})^*$ é o grupo dos caráters módulo q . Neste caso é conveniente estender a definição de caráter para uma função de \mathbb{Z} em \mathbb{C} da seguinte maneira: se $\chi \in (\widehat{\mathbb{Z}/q\mathbb{Z}})^*$, definimos

$$\begin{aligned} \tilde{\chi}: \mathbb{Z} &\rightarrow \mathbb{C} \\ a &\mapsto \tilde{\chi}(a) = \begin{cases} 0 & \text{se } (q, a) > 1 \\ \chi(a \bmod q) & \text{se } (q, a) = 1. \end{cases} \end{aligned}$$

Daqui por diante nos referimos aos caráters módulo q como sendo estas extensões.

Observe que o número de caráters módulo q é $\varphi(q)$.

Vamos agora relacionar os caráters módulo q à função $\psi(x; q, \ell)$.

Definição A.28. *Seja χ um caráter módulo q . Então*

$$\psi(x, \chi) = \sum_{n \leq x} \Lambda(n) \chi(n).$$

Proposição A.29. *Se $(q, \ell) = 1$ então*

$$\psi(x, q, \ell) = \frac{1}{\varphi(q)} \sum_{\chi} \psi(x, \chi) \overline{\chi(\ell)},$$

onde \sum_{χ} é a soma sobre os caráters módulo q e $\overline{\chi(\ell)}$ é o conjugado complexo de $\chi(\ell)$.

DEMONSTRAÇÃO: Vamos identificar em nossa notação um elemento $x \in \mathbb{Z}/q\mathbb{Z}$ e os elementos de sua classe mod q em \mathbb{Z} . Como $(\ell, q) = 1$, temos ℓ invertível em $\mathbb{Z}/q\mathbb{Z}$, chamemos ℓ^{-1} seu inverso. Daí $\overline{\chi(\ell)} = \chi(\ell^{-1})$ e

$$\sum_{n \leq x} \Lambda(n) \chi(n) \overline{\chi(\ell)} = \sum_{n \leq x} \Lambda(n) \chi(n\ell^{-1}).$$

Desta forma

$$\begin{aligned} \sum_{\chi} \psi(x, \chi) \overline{\chi(\ell)} &= \sum_{\chi} \sum_{n \leq x} \Lambda(n) \chi(n\ell^{-1}) = \sum_{n \leq x} \sum_{\chi} \Lambda(n) \chi(n\ell^{-1}) \\ &= \sum_{n \leq x} \Lambda(n) \sum_{\chi} \chi(n\ell^{-1}). \end{aligned}$$

A proposição A.27 fornece

$$\sum_{\chi} \chi(n\ell^{-1}) = \begin{cases} 0, & \text{se } n\ell^{-1} \not\equiv 1 \pmod{q}; \\ \varphi(q), & \text{se } n\ell^{-1} \equiv 1 \pmod{q}. \end{cases}$$

Isto é,

$$\sum_{\chi} \psi(x, \chi) \overline{\chi(\ell)} = \sum_{\substack{n \leq x \\ n \equiv \ell \pmod{q}}} \Lambda(n) \cdot \varphi(q) = \varphi(q) \cdot \varphi(x; q, \ell)$$

□

A.3.3 L -séries de Dirichlet

Definição A.30. *Seja χ um caráter módulo q . Uma L -série de Dirichlet é a extensão meromorfa de $\sum_{n \geq 1} \frac{\chi(n)}{n^s}$ para o plano complexo, e indicada por $L(s, \chi)$.*

É imediato verificar que se $\sigma > 1$, então a série acima converge uniformemente em $\Re s \geq \sigma$, pois χ é limitada.

Proposição A.31. *Em $\Re s > 1$ temos*

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s} \right)^{-1}.$$

DEMONSTRAÇÃO: Os caracteres são funções estritamente multiplicativas e limitadas, logo esta proposição é corolário de A.10.

□

Proposição A.32. *Em $\Re s > 1$ temos*

$$s \int_1^\infty \psi(x, \chi) x^{-1-s} dx = \frac{L'(s, \chi)}{L(s, \chi)}.$$

DEMONSTRAÇÃO: Em $\Re s > 1$ temos

$$\frac{1}{|L(s, \chi)|} = \prod_p \left| 1 - \frac{\chi(p)}{p^s} \right| \leq \prod_p \left(1 + \frac{1}{p^\sigma} \right),$$

onde $\sigma = \Re s$. Na demonstração de A.10 provamos que

$$\prod_p \left(1 + \frac{1}{p^\sigma} \right) \leq e^{2S},$$

$$S = \sum_p \frac{1}{p^\sigma} < \infty.$$

Logo $|L(s, \chi)| \geq e^{-2S} > 0$, $\Re s > 1$.

Podemos portanto tomar logaritmos na expressão

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s} \right)^{-1},$$

$$\log L(s, \chi) = - \sum_p \log \left(1 - \frac{\chi(p)}{p^s} \right) = \sum_p \sum_{m \geq 1} \frac{\chi(p^m)}{mp^{ms}}.$$

Derivando:

$$\begin{aligned} -\frac{L'(s, \chi)}{L(s, \chi)} &= \sum_p \frac{\chi(p)/p^s}{1 - \chi(p)/p^s} \log p \\ &= \sum_p \left(\frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \dots \right) \log p = \sum_{n \geq 1} \frac{\Lambda(n) \chi(n)}{n^s}. \end{aligned}$$

Usando o lema de representação integral segue-se em $\Re s > 1$ que

$$-\frac{L'(s, \chi)}{L(s, \chi)} = s \int_1^\infty \psi(x, \chi) x^{-1-s} dx.$$

□

Juntando as proposições A.29 e A.32 obtemos

$$\begin{aligned} g(s) &= s \int_1^\infty \psi(x; q, \ell) x^{-1-s} dx \\ &= -\frac{1}{\varphi(q)} \frac{L'(s, \chi_1)}{L(s, \chi_1)} - \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_1} \overline{\chi(\ell)} \frac{L'(s, \chi)}{L(s, \chi)}, \end{aligned}$$

que chamaremos fórmula de decomposição. Provaremos a seguir que:

- (a) $-\frac{L'(s, \chi_1)}{L(s, \chi_1)} - \frac{1}{(s-1)}$ possui continuação analítica sobre $\Re s = 1$;
- (b) $\sum_{\chi \neq \chi_1} \overline{\chi(\ell)} \frac{L'(s, \chi)}{L(s, \chi)}$ é analítica sobre $\Re s = 1$.

Pela fórmula de decomposição $g(s) - \frac{1}{\varphi(q)} \frac{1}{(s-1)}$ possuirá continuação analítica sobre $\Re s = 1$, daí estaremos aptos a utilizar o teorema A.20.

Proposição A.33. *Temos*

$$L(s, \chi_1) = \zeta(s) \prod_{p|q} (1 - p^{-s}).$$

Em particular $L(s, \chi_1)$ possui um polo simples em $s = 1$, que é seu único polo em $\Re s > 0$, e $L(1 + it, \chi_1) \neq 0$ para t real não nulo.

DEMONSTRAÇÃO: Pela fórmula de Euler e pela proposição A.31 temos que $L(s, \chi_1) = \zeta(s) \prod_{p|q} (1 - p^{-s})$ em $\Re s > 1$. Como $\prod_{p|q} (1 - p^{-s})$ é analítica em \mathbb{C} , a fórmula vale no domínio de definição de ζ e $L(s, \chi_1)$. Como $\prod_{p|q} (1 - p^{-s})$ não se anula em $\Re s = 1$ e pelas propriedades de $\zeta(s)$, segue-se o enunciado. \square

Proposição A.34. *Se $\chi \neq \chi_1$, então $L(s, \chi)$ é analítica em $\Re s > 0$.*

DEMONSTRAÇÃO: Chamando $P(x) = \sum_{n \leq x} \chi(n)$ e escrevendo $[x] = aq + r$, com $a \in \mathbb{N}$ e $0 \leq r < q$, temos pela proposição A.25 que

$$P(x) = \sum_{n=1}^{aq} \chi(n) + \sum_{n=aq+1}^{[x]} \chi(n) = \sum_{n=aq+1}^{[x]} \chi(n).$$

Logo

$$|P(x)| \leq \sum_{n=aq+1}^{\lfloor x \rfloor} |\chi(n)| \leq r < q.$$

Pelo lema da representação integral obtemos

$$L(s, \chi) = s \int_1^\infty P(x) x^{-1-s} dx,$$

expressão válida em $\Re s > 0$ pois $P(x)$ é limitada. \square

Olhemos novamente para a fórmula de decomposição. Como $L(s, \chi_1) = \zeta(s) \prod_{p|q} (1 - p^{-s})$, temos que $-\frac{L'(s, \chi_1)}{L(s, \chi_1)} - \frac{1}{s-1}$ admite extensão analítica sobre $\Re s = 1$ da mesma forma que $-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ admite. Resta ver que $\sum_{\chi \neq \chi_1} \overline{\chi(\ell)} \frac{L'(s, \chi)}{L(s, \chi)}$ é analítica em $\Re s = 1$, e como já provamos que $L(s, \chi)$ é analítica em $\Re s > 0$, basta provar que se $\chi \neq \chi_1$ temos $L(1 + it, \chi) \neq 0$ para todo $t \in \mathbb{R}$. Nossa demonstração deste fato divide-se em duas partes: na primeira mostramos que se $\chi^2 \neq \chi_1$ o resultado é verdadeiro, e para $\chi^2 = \chi_1$ o resultado é verdadeiro em $s \neq 1$. A segunda parte trata de $\chi^2 = \chi_1$ e $s = 1$, e neste ponto necessitaremos do lema de Landau, cuja demonstração encontra-se na seção final.

Proposição A.35. *Se $\chi \neq \chi_1$, então $L(s, \chi) \neq 0$ em $\Re s = 1$.*

DEMONSTRAÇÃO: Seguimos a demonstração de Mertens para $\zeta(s) \neq 0$ em $\Re s = 1$.

Seja $t \in \mathbb{R}$. Para p primo escreveremos

$$\log(1 - p^{-s} \chi(p))^{-1} = \sum_{m \geq 1} \frac{1}{m p^{ms}} \chi(p^m),$$

onde $\Re s > 1$. Logo

$$\begin{aligned} \log L(s, \chi) &= \sum_p \sum_{m \geq 1} \frac{1}{m p^{ms}} \chi(p^m) \\ &= \sum_p \sum_{m \geq 1} \frac{1}{m p^{m\sigma}} \cdot e^{-itm \log p} \chi(p^m), \end{aligned}$$

com $s = \sigma + it$. Daí vem

$$\begin{aligned}
 & \log |L^3(\sigma, \chi_1) \cdot L^4(\sigma + it, \chi) \cdot L(\sigma + 2it, \chi^2)| \\
 &= \Re \log L^3(\sigma, \chi_1) \cdot L^4(\sigma + it, \chi) \cdot L(\sigma + 2it, \chi^2) \\
 &= \Re \sum_p \sum_{m \geq 1} \frac{1}{mp^{m\sigma}} (3\chi_1^m(p) + 4e^{-imt \log p} \chi^m(p) + e^{-2imt \log p} \chi^{2m}(p)) \\
 &= \Re \sum_{p \nmid q} \sum_{m \geq 1} \frac{1}{mp^{m\sigma}} (3 + 4e^{-imt \log p} \chi^m(p) + e^{-2imt \log p} \chi^{2m}(p)).
 \end{aligned}$$

Como $|\chi(p)| = 1$ para todo primo p que não divide q , temos $\chi(p) = e^{ic_p}$ para algum $c_p \in \mathbb{R}$; a última expressão torna-se

$$\sum_{p \nmid q} \sum_{m \geq 1} \frac{1}{mp^{m\sigma}} \{3 + 4 \cos m(t \log p + c_p) + \cos 2m(t \log p + c_p)\} \geq 0, \quad (*)$$

pois $3 + 4 \cos \theta + \cos 2\theta = 2(1 + \cos \theta)^2 \geq 0$, $\theta \in \mathbb{R}$.

Suponha que $L(1 + it, \chi) = 0$ com $t \neq 0$, daí

$$\lim_{\sigma \rightarrow 1^+} L^3(\sigma, \chi_1) \cdot L^4(\sigma + it, \chi) \cdot L(\sigma + 2it, \chi^2) = 0$$

pois o polo simples de $L(s, \chi_1)$ seria superado pelo zero de $L(s, \chi)$, e $L(\sigma + 2it, \chi^2) \rightarrow L(1 + 2it, \chi^2)$ que é um complexo se $t \neq 0$. Desse modo deveríamos ter que

$$\lim_{\sigma \rightarrow 1^+} \log |L^3(\sigma, \chi_1) L^4(\sigma + it, \chi) L(\sigma + 2it, \chi^2)| = -\infty,$$

mas este logaritmo é não negativo por (*).

Se $t = 0$ este mesmo argumento se aplica, desde que $\chi^2 \neq \chi_1$. Neste caso $L(\sigma, \chi^2) \rightarrow L(1, \chi^2)$ que é ainda complexo.

Resumindo, já mostramos que se $\chi^2 \neq \chi_1$, então $L(1 + it, \chi) \neq 0$ para todo $t \in \mathbb{R}$, e se $\chi^2 = \chi_1$, então $L(1 + it, \chi) \neq 0$ para todo $t \in \mathbb{R}^*$.

Resta provar que se $\chi^2 = \chi_1$ então $L(1, \chi) \neq 0$. Chamemos

$$\Xi(s) = L(s, \chi_1) \cdot L(s, \chi),$$

temos que Ξ é analítica em $\Re s > 0$ se $L(1, \chi) = 0$. Em $\Re s > 1$ podemos escrever

$$\begin{aligned}
 \log \Xi(s) &= \sum_p \sum_{m \geq 1} \frac{1}{mp^{ms}} [\chi_1^m(p) + \chi^m(p)] \\
 &= \sum_{p \nmid q} \sum_{m \geq 1} \frac{1}{mp^{ms}} [1 + \chi^m(p)].
 \end{aligned}$$

Ora, $\chi^2 = \chi_1$ implica em que $\chi(p) = \pm 1$ se $p \nmid q$, logo

$$\log \Xi(s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

com $a_n \geq 0$. Esta última série não converge em $s = \frac{1}{\varphi(q)}$. De fato, para s real positivo maior que $\frac{1}{\varphi(q)}$ temos

$$\sum_{n \geq 1} \frac{a_n}{n^s} = \sum_{p \nmid q} \sum_{m \geq 1} \frac{a_{p^m}}{p^{ms}} > \sum_{p \nmid q} \frac{a_{p^{\varphi(p)}}}{p^{s\varphi(p)}}.$$

Como $p^{\varphi(q)} \equiv 1 \pmod{q}$ temos

$$a_{p^{\varphi(q)}} = \frac{1 + \chi(p)^{\varphi(q)}}{\varphi(q)} = \frac{2}{\varphi(q)}.$$

Daí

$$\sum_{n \geq 1} \frac{a_n}{n^s} > \frac{2}{\varphi(q)} \sum_{p \nmid q} \frac{1}{p^{\varphi(q)s}} \rightarrow \infty \text{ quando } s \rightarrow \frac{1}{\varphi(q)}.$$

Dizemos que $\sigma_0 > 0$ é a abscissa de convergência da série $\sum_{n \geq 1} \frac{b_n}{n^s}$ quando a série converge em $\Re s > \sigma_0$ e não converge em $\Re s > \sigma_0 - \varepsilon$ para qualquer $\varepsilon > 0$. Pelo anterior a abscissa de convergência σ_0 de nossa série $\sum_{n \geq 1} \frac{a_n}{n^s}$ é maior do que ou igual a $\frac{1}{\varphi(q)}$, e para $\Re s \geq \delta > \sigma_0$ a série $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge uniformemente, pois $a_n \geq 0$. Em particular a igualdade

$$\Xi(s) = \exp\left(\sum_{n \geq 1} \frac{a_n}{n^s}\right)$$

é válida em $\Re s > \sigma_0$.

Enunciamos agora o lema de Landau, que será demonstrado na seguinte seção:

Lema A.36. (Landau). Se $a_n \geq 0$ e $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ tem abscissa de convergência finita σ_0 , então f não admite extensão analítica a nenhuma vizinhança de $s = \sigma_0$.

Usando o lema acima podemos completar a demonstração. Como $\sigma_0 \geq \frac{1}{\varphi(q)} > 0$, em particular $\log \Xi$ não pode possuir extensão analítica em torno de $s = \sigma_0 > 0$. Mas Ξ é holomorfa em $\Re s > 0$ se $L(1, \chi) = 0$, e,

para \tilde{s} real com $\tilde{s} > \sigma_0$, temos $\log \Xi(\tilde{s}) = \sum_{n \geq 1} \frac{a_n}{n^{\tilde{s}}} > 0$, donde $|\Xi(\tilde{s})| > 1$.

Assim, $|\Xi(\sigma_0)| \geq 1$ (e em particular $|\Xi(\sigma_0)| \neq 0$), e portanto (qualquer ramo de) $\log \Xi$ admite extensão analítica em torno de $s = \sigma_0 > 0$, o que é uma contradição. Logo devemos ter $L(1, \chi) \neq 0$. \square

Corolário A.37. *Temos que*

$$\lim_{x \rightarrow \infty} \frac{\pi(x; q, \ell)}{x / \log x} = \frac{1}{\varphi(q)}.$$

DEMONSTRAÇÃO: Este limite é equivalente a $\lim_{x \rightarrow \infty} \frac{\psi(x; s, \ell)}{x} = \frac{1}{\varphi(q)}$. Pela fórmula de decomposição $g(s) - \frac{1}{\varphi(q)} \frac{1}{(s-1)}$ possui continuação analítica sobre $\Re s = 1$, pois $-\frac{L'(s, \chi_1)}{L(s, \chi_1)} - \frac{1}{s-1}$ possui tal extensão e $\sum_{\chi \neq \chi_1} \overline{\chi(\ell)} \frac{L'(s, \chi)}{L(s, \chi)}$ também possui. Pelo teorema A.20 temos o limite de $\psi(x; q, \ell)$ \square

A.4 O Lema de Landau

Fixemos como notação $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ em $\Re s > \sigma_0$, onde σ_0 será abscissa de convergência da série, e $a_n \geq 0$. Então a série converge uniformemente em $\Re s \geq \delta > \sigma_0$ e portanto

$$f'(s) = - \sum_{n \geq 1} \frac{a_n \log n}{n^s},$$

e esta última série tem a mesma abscissa de convergência σ_0 , convergindo uniformemente em $\Re s \geq \delta > \sigma_0$. Em particular podemos aplicar derivações sucessivas à fórmula do somatório para obter as derivadas de f em $\Re s > \sigma_0$. A função f é evidentemente analítica em $\Re > \sigma_0$.

Lema A.38. (Landau). *Se σ_0 é finito, então f não admite extensão analítica a nenhuma vizinhança de $s = \sigma_0$.*

Equivalentemente, se σ é finito, $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge em $\Re s > \sigma$ e a função f admite continuação analítica em torno de $s = \sigma$, então a série $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge em $\Re s > \sigma - \varepsilon$ para algum $\varepsilon > 0$.

DEMONSTRAÇÃO: Mostraremos a segunda forma do lema. Seja $a = 1 + \sigma$, daí f é analítica em a e portanto

$$f(s) = \sum_{k \geq 0} \frac{f^{(k)}(a)}{k!} (s - a)^k,$$

sendo esta série absolutamente convergente num disco aberto de centro em a e raio maior que 1, pois f é analítica em σ .

Temos que

$$f^{(k)}(a) = (-1)^k \sum_{n \geq 1} \frac{a_n (\log n)^k}{n^a},$$

logo

$$f(s) = \sum_{k \geq 0} \sum_{n \geq 1} \frac{a_n (\log n)^k}{n^a k!} (a - s)^k \quad (*)$$

neste disco. Como o raio de convergência é maior que 1, para algum $\varepsilon > 0$ teremos a expressão (*) válida com $s = \sigma - \varepsilon$, logo $a - s = 1 + \varepsilon > 0$, e desta forma os termos na dupla série (*) são não negativos, permitindo a troca dos somatórios. Obtemos

$$\begin{aligned} f(\sigma - \varepsilon) &= \sum_{n \geq 1} \frac{a_n}{n^a} \sum_{k \geq 0} \frac{((1 + \varepsilon) \log n)^k}{k!} \\ &= \sum_{n \geq 1} \frac{a_n}{n^a} e^{(1 + \varepsilon) \log n} = \sum_{n \geq 1} \frac{a_n}{n^{\sigma - \varepsilon}}, \end{aligned}$$

isto é, a série $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge para $s = \sigma - \varepsilon$, logo também converge em $\Re s > \sigma - \varepsilon$. \square

A.5 Bibliografia

- [1] Apostol, T., *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- [2] Edwards, H.M., *Riemann's Zeta Function*, Academic Press, New York, 1974.
- [3] Landau, E., *Handbuch der Lehre von der Verteilung der Primzahlen*, em dois volumes Teubner, Leipzig, 1909.

- [4] Korevaar, J., *On Newman's Quick Way to the Prime Number Theorem*, The Mathematical Intelligencer, 4 (1982), 108–115.
- [5] Newman, D.J., *Simple Analytic Proof of the Prime Number Theorem*, American Mathematical Monthly 87 (1980), 693–696.
- [6] Serre, J.-P., *A course in arithmetic*, Springer-Verlag, New York, 1973.
- [7] Widder, D.V., *The Laplace Transform*, Princeton University Press, Princeton, 1946.
- [8] Wiener, N., *Tauberian Theorems*, Annals of Mathematics 33 (1932), 1–100.

Apêndice B

Sequências Recorrentes

(Publicado originalmente por Carlos Gustavo Moreira na Revista da Olimpíada Regional de Matemática de Santa Catarina, no. 4, 53–69)

Sequências recorrentes são sequências x_0, x_1, x_2, \dots em que cada termo é determinado por uma dada função dos termos anteriores. Dado um inteiro positivo k , uma *sequência recorrente de ordem k* é uma sequência em que cada termo é determinado como uma função dos k termos anteriores:

$$x_{n+k} = f(x_{n+k-1}, x_{n+k-2}, \dots, x_{n+1}, x_n), \quad \forall n \in \mathbb{N}.$$

Com essa generalidade, o estudo geral de sequências recorrentes se confunde em larga medida com a teoria dos Sistemas Dinâmicos, e o comportamento de tais sequências pode ser bastante caótico e de descrição muito difícil, mesmo qualitativamente. Um caso particular muito importante ocorre quando a função f é linear: existem constantes c_1, c_2, \dots, c_n com

$$x_{n+k} = c_1 x_{n+k-1} + c_2 x_{n+k-2} + \dots + c_k x_n, \quad \forall n \in \mathbb{N}.$$

Tais sequências são conhecidas como sequências recorrentes lineares, e generalizam simultaneamente as progressões geométricas, aritméticas e os polinômios. Estas sequências serão o objeto principal dessas notas. Não obstante, algumas recorrências não-lineares serão consideradas, como a recorrência $x_{n+1} = x_n^2 - 2$, que tem grande interesse do ponto de vista de sistemas dinâmicos e por suas aplicações à Teoria dos Números.

Essas notas, adaptadas do texto de um mini-curso dado por um dos autores (Carlos Gustavo T. de A. Moreira) na II Bienal da SBM, são ins-

piradas no excelente livreto “Sucesiones Recurrentes”, de A. Markushévich [98], publicado na coleção “Lecciones populares de matemáticas”, da editora MIR, no qual o autor aprendeu bastante sobre o tema no início de sua formação matemática. A seção B.4, onde é deduzida a fórmula para o termo geral de uma sequência recorrente linear, é adaptada do artigo “Ecuaciones de recorrência”, de Héctor Soza Pollman, publicado no número 9 da revista Eureka! (de fato, o artigo original submetido à revista enunciava esta fórmula sem demonstração, a qual foi incluída no artigo pelo autor destas notas, que é um dos editores da Eureka!).

B.1 Sequências Recorrentes Lineares

Uma sequência $(x_n)_{n \in \mathbb{N}}$ é uma sequência recorrente linear de ordem k (onde k é um inteiro positivo) se existem constantes (digamos reais ou complexas) c_1, c_2, \dots, c_k tais que

$$x_{n+k} = \sum_{j=1}^k c_j x_{n+k-j} = c_1 x_{n+k-1} + c_2 x_{n+k-2} + \dots + c_k x_n, \quad \forall n \in \mathbb{N}.$$

Tais sequências são determinadas pelos seus k primeiros termos x_0, \dots, x_{k-1} .

Os exemplos mais simples (e fundamentais, como veremos a seguir) de sequências recorrentes lineares são as progressões geométricas: se $x_n = a \cdot q^n$ então $x_{n+1} = qx_n$, $\forall n \in \mathbb{N}$, donde (x_n) é uma sequência recorrente linear de ordem 1.

Se (x_n) é uma progressão aritmética, existe uma constante r tal que $x_{n+1} - x_n = r$, $\forall n \in \mathbb{N}$, donde $x_{n+2} - x_{n+1} = x_{n+1} - x_n$, $\forall n \in \mathbb{N}$, e logo $x_{n+2} = 2x_{n+1} - x_n$, $\forall n \in \mathbb{N}$, ou seja, (x_n) é uma sequência recorrente linear de ordem 2.

Se $x_n = P(n)$ onde P é um polinômio de grau k , então (x_n) satisfaz a recorrência linear de ordem $k+1$ dada por

$$x_{n+k+1} = \sum_{j=0}^k (-1)^j \binom{k+1}{j+1} x_{n+k-j}, \quad \forall n \in \mathbb{N}. \quad (*)$$

Isso é evidente se $k=0$ (isto é, se P é constante), pois nesse caso $(*)$ se reduz a $x_{n+1} = x_n$, $\forall n \in \mathbb{N}$, e o caso geral pode ser provado por indução: se P é um polinômio de grau $k \geq 1$ então $Q(x) = P(x+1) -$

$P(x)$ é um polinômio de grau $k - 1$, donde $y_n = x_{n+1} - x_n = Q(n)$ satisfaz a recorrência $y_{n+k} = \sum_{j=0}^{k-1} (-1)^j \binom{k}{j+1} y_{n+k-1-j}$, $\forall n \in \mathbb{N}$, donde

$$x_{n+k+1} - x_{n+k} = \sum_{j=0}^{k-1} (-1)^j \binom{k}{j+1} (x_{n+k-j} - x_{n+k-j-1}), \quad \forall n \in \mathbb{N},$$

e logo

$$\begin{aligned} x_{n+k+1} &= \sum_{j=0}^k (-1)^j \left(\binom{k}{j+1} + \binom{k}{j} \right) x_{n+k-j} \\ &= \sum_{j=0}^k (-1)^j \binom{k+1}{j+1} x_{n+k-j}, \quad \forall n \in \mathbb{N}. \end{aligned}$$

Um outro exemplo é dado por sequências do tipo $x_n = (an + b) \cdot q^n$, onde a, b e q são constantes. Temos que $x_{n+1} - qx_n = (a(n+1) + b)q^{n+1} - q(an + b) \cdot q^n = q^{n+1}(a(n+1) + b - (an + b)) = aq^{n+1}$ é uma progressão geométrica de razão q , e logo $x_{n+2} - qx_{n+1} = q(x_{n+1} - qx_n)$, donde $x_{n+2} = 2qx_{n+1} - q^2x_n$, $\forall n \in \mathbb{N}$, e portanto (x_n) é uma sequência recorrente linear de ordem 2.

Vamos agora considerar a famosa e popular sequência de Fibonacci, dada por $F_0 = 0$, $F_1 = 1$ e $F_{n+2} = F_{n+1} + F_n$, $\forall n \in \mathbb{N}$. Seus primeiros termos são $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, $F_7 = 13$, $F_8 = 21, \dots$. Mostraremos na próxima seção como achar uma fórmula explícita para seu termo geral F_n em função de n , o que será generalizado para sequências recorrentes lineares quaisquer, e veremos algumas de suas propriedades aritméticas.

Antes disso porém, concluiremos esta seção com alguns fatos gerais sobre sequências recorrentes lineares, que serão úteis nas seções subsequentes.

O conjunto das sequências que satisfazem uma dada recorrência linear

$$x_{n+k} = \sum_{j=1}^k c_j x_{n+k-j}, \quad \forall n \in \mathbb{N}$$

é um *espaço vetorial*, isto é, dadas duas sequências (y_n) e (z_n) que satisfazem esta recorrência (ou seja, $y_{n+k} = \sum_{j=1}^k c_j y_{n+k-j}$ e $z_{n+k} =$

$\sum_{j=1}^k c_j z_{n+k-j}$, $\forall n \in \mathbb{N}$) e uma constante a , a sequência (w_n) dada por

$w_n = y_n + az_n$ satisfaz a mesma recorrência: $w_{n+k} = \sum_{j=1}^k c_j w_{n+k-j}$, $\forall n \in \mathbb{N}$.

É bastante usual, dada uma sequência (x_n) , estudar a sequência obtida pela soma de seus n primeiros termos $s_n = \sum_{k \leq n} x_k$. Se (x_n) é uma sequência recorrente linear, (s_n) também é. De fato, $s_{n+1} - s_n = \sum_{k \leq n+1} x_k - \sum_{k \leq n} x_k = x_{n+1}$, $\forall n \in \mathbb{N}$. Se $x_{n+k} = \sum_{j=1}^k c_j x_{n+k-j}$, temos

$s_{n+k+1} - s_{n+k} = \sum_{j=1}^k c_j (s_{n+k+1-j} - s_{n+k-j})$, $\forall n \in \mathbb{N}$, donde

$$s_{n+k+1} = (1 + c_1)s_{n+k} + \sum_{j=1}^{k-1} (c_{j+1} - c_j)s_{n+k-j} - c_k s_n = \sum_{i=1}^{k+1} d_i s_{n+k+1-i}$$

onde $d_1 = 1 + c_1$, $d_i = c_i - c_{i-1}$ para $2 \leq i \leq k$ e $d_{k+1} = -c_k$, $\forall n \in \mathbb{N}$, e portanto (s_n) é uma sequência recorrente linear de ordem $k + 1$.

B.2 A Sequência de Fibonacci

A sequência de Fibonacci é definida por $F_0 = 0$, $F_1 = 1$ e $F_{n+2} = F_{n+1} + F_n$, $\forall n \in \mathbb{N}$. Queremos achar uma fórmula explícita para F_n em função de n . Para isso usaremos uma ideia que será bastante útil também no caso geral: procuraremos progressões geométricas que satisfazem a mesma recorrência que (F_n) : se $x_n = a \cdot q^n$ com a e q não nulos satisfaz $x_{n+2} = x_{n+1} + x_n$, $\forall n \in \mathbb{N}$, teremos $a \cdot q^{n+2} = a \cdot q^{n+1} + a \cdot q^n = a \cdot q^n(q + 1)$, donde $q^2 = q + 1$. Temos assim dois valores possíveis para q : as duas raízes da equação $q^2 - q - 1 = 0$, que são $\frac{1+\sqrt{5}}{2}$ e $\frac{1-\sqrt{5}}{2}$. Assim, sequências da forma $a \left(\frac{1+\sqrt{5}}{2}\right)^n$ e da forma $b \left(\frac{1-\sqrt{5}}{2}\right)^n$ satisfazem a recorrência acima, bem como sequências da forma $y_n = a \left(\frac{1+\sqrt{5}}{2}\right)^n + b \left(\frac{1-\sqrt{5}}{2}\right)^n$, pela observação da seção anterior.

Basta agora encontrar valores de a e b tais que $y_0 = 0$ e $y_1 = 1$ para que tenhamos $y_n = F_n$ para todo n (de fato, teríamos $y_0 = F_0$, $y_1 = F_1$ e, por indução se $k \geq 2$ e $y_n = F_n$ para todo $n < k$, temos

$y_k = y_{k-1} + y_{k-2} = F_{k-1} + F_{k-2} = F_k$). Para isso, devemos ter:

$$\begin{cases} a + b = 0 \\ a \left(\frac{1+\sqrt{5}}{2} \right) + b \left(\frac{1-\sqrt{5}}{2} \right) = 1 \end{cases}$$

e portanto $a = \frac{1}{\sqrt{5}}$ e $b = -\frac{1}{\sqrt{5}}$. Mostramos assim que

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right), \quad \forall n \in \mathbb{N}.$$

É curioso que na fórmula do termo geral de uma sequência de números inteiros definida de modo tão simples quanto (F_n) apareçam números irracionais.

Provaremos a seguir uma identidade útil sobre números de Fibonacci:

Proposição B.1. $F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$, $\forall m, n \in \mathbb{N}$, $n \geq 1$.

DEMONSTRAÇÃO: Sejam $y_m = F_{m+n}$ e $z_m = F_m F_{n-1} + F_{m+1} F_n$. Temos que (y_n) e (z_n) satisfazem a recorrência $x_{n+2} = x_{n+1} + x_n$, $\forall n \in \mathbb{N}$. Por outro lado, $y_0 = F_n$, $y_1 = F_{n+1}$, $z_0 = 0 \cdot F_{n-1} + 1 \cdot F_n = F_n = y_0$ e $z_1 = 1 \cdot F_{n-1} + 1 \cdot F_n = F_{n+1} = y_1$, e portanto, como antes, $z_n = y_n$, $\forall n \in \mathbb{N}$. \square

Podemos usar este fato para provar o seguinte interessante fato aritmético sobre a sequência (F_n) , que pode ser generalizado para as chamadas sequências de Lucas, as quais são úteis para certos testes de primalidade:

Teorema B.2. $\text{mdc}(F_m, F_n) = F_{\text{mdc}(m,n)}$, $\forall m, n \in \mathbb{N}$.

DEMONSTRAÇÃO: Observemos primeiro que $\text{mdc}(F_n, F_{n+1}) = 1$, $\forall n \in \mathbb{N}$. Isso vale para $n = 0$ pois $F_1 = 1$ e, por indução,

$$\text{mdc}(F_{n+1}, F_{n+2}) = \text{mdc}(F_{n+1}, F_{n+1} + F_n) = \text{mdc}(F_{n+1}, F_n) = 1.$$

Além disso, se $m = 0$, $\text{mdc}(F_m, F_n) = \text{mdc}(0, F_n) = F_n = F_{\text{mdc}(m,n)}$, $\forall n \in \mathbb{N}$, e se $m = 1$, $\text{mdc}(F_m, F_n) = \text{mdc}(1, F_n) = 1 = F_1 = F_{\text{mdc}(m,n)}$, $\forall n \in \mathbb{N}$. Vamos então provar o fato acima por indução em m . Suponha

que a afirmação do enunciado seja válida para todo $m < k$ (onde $k \geq 2$ é um inteiro dado) e para todo $n \in \mathbb{N}$. Queremos provar que ela vale para $m = k$ e para todo $n \in \mathbb{N}$, isto é, que $\text{mdc}(F_k, F_n) = F_{\text{mdc}(k,n)}$ para todo $n \in \mathbb{N}$. Note que, se $n < k$, $\text{mdc}(F_k, F_n) = \text{mdc}(F_n, F_k) = F_{\text{mdc}(n,k)} = F_{\text{mdc}(k,n)}$, por hipótese de indução. Já se $n \geq k$, $F_n = F_{(n-k)+k} = F_{n-k}F_{k-1} + F_{n-k+1}F_k$, e logo $\text{mdc}(F_k, F_n) = \text{mdc}(F_k, F_{n-k}F_{k-1} + F_{n-k+1}F_k) = \text{mdc}(F_k, F_{n-k}F_{k-1}) = \text{mdc}(F_k, F_{n-k})$ (pois $\text{mdc}(F_k, F_{k-1}) = 1$) $= F_{\text{mdc}(k,n-k)} = F_{\text{mdc}(k,n)}$. \square

Corolário B.3. *Se $m \geq 1$ e m é um divisor de n então F_m divide F_n . Além disso, se $m \geq 3$ vale a recíproca: se F_m divide F_n então m divide n .*

B.3 A Recorrência $x_{n+1} = x_n^2 - 2$

Consideremos as sequências $(x_n)_{n \in \mathbb{N}}$ de números reais que satisfazem a recorrência $x_{n+1} = x_n^2 - 2$, $\forall n \in \mathbb{N}$. Suponha que $x_0 = \alpha + \alpha^{-1}$ para um certo α (real ou complexo). Então podemos provar por indução que $x_n = \alpha^{2^n} + \alpha^{-2^n}$, $\forall n \in \mathbb{N}$. De fato, se vale a fórmula para x_n , teremos

$$\begin{aligned} x_{n+1} &= x_n^2 - 2 = (\alpha^{2^n} + \alpha^{-2^n})^2 - 2 = \alpha^{2^{n+1}} + 2 + \alpha^{-2^{n+1}} - 2 \\ &= \alpha^{2^{n+1}} + \alpha^{-2^{n+1}}. \end{aligned}$$

Se $|x_0| > 2$, temos $x_0 = \alpha + \alpha^{-1}$ para $\alpha = \frac{x_0 + \sqrt{x_0^2 - 4}}{2} \in \mathbb{R}$.

Se $|x_0| \leq 2$, vale a mesma fórmula para α , mas nesse caso α é um número complexo de módulo 1, e pode ser escrito como $\alpha = e^{i\theta} = \cos \theta + i \sin \theta$. Nesse caso, $x_n = e^{2^n i\theta} + e^{-2^n i\theta} = (\cos(2^n \theta) + i \sin(2^n \theta)) + (\cos(2^n \theta) - i \sin(2^n \theta)) = 2 \cos(2^n \theta)$.

Podemos ver isso de outra forma: se $|x_0| \leq 2$, escrevemos $x = 2 \cos \theta$, com $\theta \in [0, \pi]$. Podemos mostrar então por indução que $x_n = 2 \cos(2^n \theta)$, para todo $n \in \mathbb{N}$. De fato, $x_{n+1} = x_n^2 - 2 = 4 \cos^2(2^n \theta) - 2 = 2(2 \cos^2(2^n \theta) - 1) = 2 \cos(2^{n+1} \theta)$, pois $\cos(2x) = 2 \cos^2 x - 1$, $\forall x \in \mathbb{R}$. Podemos usar esta expressão para obter diversos tipos de comportamento possível para uma tal sequência (x_n) . Se $x_0 = 2 \cos \theta$ e θ/π é racional e tem representação binária periódica de período m então $(x_n) = (2 \cos(2^n \theta))$ é periódica de período m . Por outro lado, podemos

ter $x_0 = 2 \cos \theta$ onde θ/π tem representação binária como

$$0,0100011011000001010011100101110111\dots$$

em que todas as sequências finitas de zeros e uns aparecem em algum lugar (isso acontece para a “maioria” dos valores de θ).

Nesse caso, a sequência $(x_n) = (2 \cos(2^n \theta))$ é *densa* em $[-2, 2]$, isto é, qualquer ponto de $[-2, 2]$ pode ser aproximado por elementos de (x_n) , com erro arbitrariamente pequeno.

No caso em que x_0 é um inteiro, a sequência (x_n) pode ter propriedades aritméticas muito interessantes. Em particular, se $x_0 = 4$ (e logo $x_n = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$, $\forall n \in \mathbb{N}$) vale o famoso critério de Lucas-Lehmer para testar a primalidade de números de Mersenne: se $n \geq 3$ então $2^n - 1$ é primo se e somente se $2^n - 1$ é um divisor de x_{n-2} (por exemplo, $2^3 - 1 = 7$ é primo e é um divisor de $x_{3-2} = x_1 = x_0^2 - 2 = 4^2 - 2 = 14$).

B.4 Fórmulas Gerais para Recorrências Lineares

Considere a equação

$$(2) \quad a_k x_{n+k} + a_{k-1} x_{n+k-1} + \dots + a_0 x_n = 0, \quad n \geq 0$$

em que a_0, \dots, a_k são constantes, e os valores de x_i são conhecidos para $i = 0, \dots, k-1$. Supondo que a equação (2) admite uma solução do tipo: $x_n = \lambda^n$, em que λ é um parâmetro, e substituindo em (2) temos

$$a_k \lambda^{n+k} + a_{k-1} \lambda^{n+k-1} + \dots + a_0 \lambda^n = 0.$$

Dividindo por λ^n , obtemos a *equação característica* associada à equação (2)

$$a_k \lambda^k + a_{k-1} \lambda^{k-1} + \dots + a_0 \lambda^0 = 0.$$

Vamos mostrar que se esta equação tem as raízes complexas $\lambda_1, \dots, \lambda_r$ com multiplicidades $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}$, respectivamente, então as soluções de (2) são exatamente as sequências (x_n) da forma $x_n = Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \dots + Q_r(n)\lambda_r^n$, onde Q_1, \dots, Q_r são polinômios com grau(Q_i) $< \alpha_i$, $1 \leq i \leq r$ (em particular, se λ_i é uma raiz simples então Q_i é constante).

Seja $P(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_0$ um polinômio.

Definição B.4. Dizemos que $(x_n)_{n \in \mathbb{N}}$ satisfaz a propriedade $\text{Rec}(P(x))$ se

$$a_k x_{n+k} + a_{k-1} x_{n+k-1} + \cdots + a_0 x_n = 0 \quad \forall n \in \mathbb{N}$$

Não é difícil verificar os seguintes fatos:

- (i) Se (x_n) e (y_n) satisfazem $\text{Rec}(P(x))$ e $c \in \mathbb{C}$ então $(z_n) = x_n + cy_n$ satisfaz $\text{Rec}(P(x))$.
- (ii) Se $Q(x) = b_r x^r + b_{r-1} x^{r-1} + \cdots + b_0$ e (x_n) satisfaz $\text{Rec}(P(x))$ então (x_n) satisfaz $\text{Rec}(P(x)Q(x))$
(isso segue de $\sum_{j=0}^r b_j (a_k x_{n+j+k} + a_{k-1} x_{n+j+k-1} + \cdots + a_0 x_{n+j}) = 0$, $\forall n \in \mathbb{N}$)
- (iii) (x_n) satisfaz $\text{Rec}(P(x))$ se e só se $(y_n) = (x_n/\lambda^n)$ satisfaz $\text{Rec}(P(\lambda x))$ (substitua $x_{n+j} = \lambda^{n+j} y_{n+j}$ em $\sum_{j=0}^k a_j x_{n+j} = 0$).
- (iv) Se $s_n = \sum_{k=0}^n x_k$ então (x_n) satisfaz $\text{Rec}(P(x))$ se e só se (s_n) satisfaz $\text{Rec}((x-1)P(x))$ (escreva $x_{n+j+1} = s_{n+j+1} - s_{n+j}$ e substitua em $\sum_{j=0}^n a_j x_{n+j+1} = 0$).

Por (iii), para ver que, para todo polinômio $Q(x)$ de grau menor que m , $x_n = Q(n)\lambda^n$ satisfaz $\text{Rec}((x-\lambda)^m)$, basta ver que $(y_n) = (Q(n))$ satisfaz $\text{Rec}((x-1)^m)$, o que faremos por indução. Isso é claro que $m=1$, e em geral, se $z_n = y_{n+1} - y_n = Q(n+1) - Q(n)$, como $\tilde{Q}(x) = Q(x+1) - Q(x)$ tem grau menor que $m-1$, (z_n) satisfaz $\text{Rec}((x-1)^{m-1})$ (por hipótese de indução), e logo, por (iv), (y_n) satisfaz $\text{Rec}((x-1)^m)$. Essa observação, combinada com (ii) e (i), mostra que se $P(x) = (x-\lambda_1)^{\alpha_1}(x-\lambda_2)^{\alpha_2}(x-\lambda_3)^{\alpha_3} \cdots (x-\lambda_r)^{\alpha_r}$, e grau(Q_i) $< \alpha_i$ para $1 \leq i \leq r$ então $x_n = \sum_{i=1}^r Q_i(n)\lambda_i^n$ satisfaz $\text{Rec}(P(x))$.

Para ver que se (x_n) satisfaz $\text{Rec}(P(x))$ então x_n é da forma acima, usaremos indução novamente.

Supomos $\lambda_1 \neq 0$ e tomamos $y_n = x_n/\lambda_1^n$, $z_n = y_{n+1} - y_n$, para $n \geq 0$.

Por (iii) e (iv), z_n satisfaz $\text{Rec}(P(\lambda_1 x)/(x-1))$ e portanto, por hipótese de indução, $z_n = \tilde{Q}_1(x) + \tilde{Q}_2(x)(\lambda_2/\lambda_1)^n + \cdots + \tilde{Q}_r(x)(\lambda_r/\lambda_1)^n$, onde $\text{grau}(\tilde{Q}_i) < \alpha_i$ para $2 \leq i \leq r$ e $\text{grau}(\tilde{Q}_1) < \alpha_1 - 1$.

Para terminar, vamos mostrar se existem polinômios P_1, P_2, \dots, P_k tais que $y_{n+1} - y_n = P_1(n) + P_2(n)\beta_2^n + \cdots + P_k(n)\beta_k^n$ (onde $1, \beta_2, \dots, \beta_k$ são complexos distintos e $P_i \neq 0, \forall i \geq 2$) então $y_n = \tilde{P}_1(n) + \tilde{P}_2(n)\beta_2^n + \cdots + \tilde{P}_k(n)\beta_k^n$, onde $\tilde{P}_1, \dots, \tilde{P}_k$ são polinômios com $\text{grau } \tilde{P}_i = \text{grau } P_i$ para $i \geq 2$ e $\text{grau } \tilde{P}_1 = \text{grau } P_1 + 1$, por indução na soma dos graus dos polinômios P_i , onde convencionamos que o grau do polinômio nulo é -1 (no nosso caso temos $\beta_i = \lambda_i/\lambda_1$, e como $x_n = \lambda_1^n y_n$ o resultado segue imediatamente).

Para provar essa afirmação observamos inicialmente que, se a soma dos grau de P_i é -1 , então $y_{n+1} - y_n = 0, \forall n$, e logo, y_n é constante. Em geral, consideramos 2 casos:

- (a) $P_1(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_0, c_m \neq 0$. Nesse caso definimos $\tilde{y}_n = y_n - \frac{c_m n^{m+1}}{m+1}$, e temos $\tilde{y}_{n+1} - \tilde{y}_n = Q_1(n) + P_2(n)\beta_1^n + \cdots + P_k(n)\beta_k^n$, com $\text{grau}(Q) < m$. Por hipótese de indução, \tilde{y}_n (e logo y_n) é da forma desejada.
- (b) $P_2(x) = d_s x^s + d_{s-1} x^{s-1} + \cdots + d_0, d_s \neq 0$. Nesse caso, definimos $\tilde{y}_n = y_n - \frac{d_s n^s \lambda_2^n}{\lambda_2 - 1}$, e temos $\tilde{y}_{n+1} - \tilde{y}_n = P_1(n) + Q(n)\beta_2^n + P_3(n)\beta_3^n + \cdots + P_k(n)\beta_k^n$, com $\text{grau}(Q) < s$. Por hipótese de indução, \tilde{y}_n (e logo y_n) é da forma desejada.

Vimos na primeira parte da demonstração acima que a sequência (x_n) satisfaz $\text{Rec}(P(x))$, onde $P(x) = (x - \lambda_1)^{\alpha_1} (x - \lambda_2)^{\alpha_2} \cdots (x - \lambda_r)^{\alpha_r}$ sempre que $x_n = Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n$, onde Q_1, Q_2, \dots, Q_r são polinômios com $\text{grau}(Q_j) < \alpha_j, \forall j \leq r$. Vamos apresentar um argumento alternativo, motivado por conversas do autor com Bruno Fernandes Cerqueira Leite, para mostrar que todas as sequências que satisfazem as recorrência são dessa forma.

Cada polinômio $Q_i(n)$ tem α_i coeficientes (dos monômios cujos graus são $0, 1, 2, \dots, \alpha_i - 1$). Como o espaço vetorial das sequências satisfazendo $\text{Rec}(P(x))$ tem dimensão $\text{grau}(P(x)) = \sum_{i=1}^r \alpha_i$, basta ver que há unicidade na representação de uma sequência na forma cima. Para isso, devemos mostrar que, se $\lambda_1, \lambda_2, \dots, \lambda_r$ são números complexos distintos e Q_1, Q_2, \dots, Q_r são polinômios tais que $Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n = 0, \forall n \in \mathbb{N}$, então $Q_j \equiv 0, \forall j \leq r$.

Vamos supor por absurdo que não seja assim. Supomos sem perda de generalidade que, para certos s e t com $1 \leq s \leq t \leq r$, $|\lambda_1| = |\lambda_i| > |\lambda_j|$, $\forall i \leq t$, $j > t$, e $\text{grau}(Q_1) = \text{grau}(Q_i) > \text{grau}(Q_j)$, se $i \leq s < j \leq t$. Se os polinômios Q_j não são todos nulos, temos Q_1 não nulo. Seja d o grau de Q_1 . Se $|\lambda_j| < |\lambda_1|$ então $\lim_{n \rightarrow \infty} \frac{Q_j(n)\lambda_j^n}{n^d \lambda_1^n} = 0$, e se $|\lambda_i| = |\lambda_1|$ e $\text{grau}(Q) < d$, também temos $\lim_{n \rightarrow \infty} \frac{Q(n)\lambda_i^n}{n^d \lambda_1^n} = 0$. Portanto, se $Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n = 0$, $\forall n \in \mathbb{N}$ e o coeficiente de n^d em Q_i é a_i para $i \leq s$, dividindo por $n^d \lambda_1^n$ e tomando o limite, temos

$$\lim_{n \rightarrow \infty} \left(a_1 + \sum_{2 \leq i \leq s} a_i \left(\frac{\lambda_i}{\lambda_1} \right)^n \right) = 0,$$

donde

$$\begin{aligned} 0 &= \lim_{n \rightarrow \infty} \left(\frac{1}{n} \sum_{k=1}^n \left(a_1 + \sum_{2 \leq i \leq s} a_i \left(\frac{\lambda_i}{\lambda_1} \right)^k \right) \right) \\ &= \lim_{n \rightarrow \infty} \left(a_1 + \frac{1}{n} \sum_{k=1}^n \sum_{2 \leq i \leq s} a_i \left(\frac{\lambda_i}{\lambda_1} \right)^k \right) \\ &= a_1 + \sum_{2 \leq i \leq s} a_i \cdot \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \left(\frac{\lambda_i}{\lambda_1} \right)^k \\ &= a_1 + \sum_{2 \leq i \leq s} a_i \cdot \lim_{n \rightarrow \infty} \left(\frac{1}{n} \cdot \frac{(\lambda_i/\lambda_1)^{n+1} - (\lambda_i/\lambda_1)}{(\lambda_i/\lambda_1) - 1} \right) = a_1, \end{aligned}$$

pois, para $2 \leq i \leq s$, $\lambda_i/\lambda_1 \neq 1$ é um complexo de módulo 1, donde

$$\left| \frac{(\lambda_i/\lambda_1)^{n+1} - (\lambda_i/\lambda_1)}{(\lambda_i/\lambda_1) - 1} \right| \leq \frac{2}{|(\lambda_i/\lambda_1) - 1|},$$

e logo

$$\lim_{n \rightarrow \infty} \frac{1}{n} \left(\frac{(\lambda_i/\lambda_1)^{n+1} - (\lambda_i/\lambda_1)}{(\lambda_i/\lambda_1) - 1} \right) = 0.$$

Entretanto, isso é um absurdo, pois $\text{grau}(Q_1) = d$, e logo $a_1 \neq 0$.

Exemplo B.5. A sequência $x_n = \sin(n\alpha)$ satisfaz uma recorrência linear.

SOLUÇÃO: De fato,

$$\begin{cases} x_{n+1} = \sin(n\alpha + \alpha) = \sin(n\alpha) \cos \alpha + \cos(n\alpha) \sin \alpha \\ x_{n+2} = \sin(n\alpha + 2\alpha) = \sin(n\alpha) \cos 2\alpha + \cos(n\alpha) \sin 2\alpha \end{cases}$$

$$\Rightarrow x_{n+2} - \frac{\sin 2\alpha}{\sin \alpha} x_{n+1} = (\cos 2\alpha - \frac{\sin 2\alpha}{\sin \alpha} \cos \alpha) x_n$$

ou seja, $x_{n+2} = 2 \cos \alpha \cdot x_{n+1} - x_n$. Note que x_n não parece ser da forma geral descrita nesta seção, mas de fato

$$x_n = \frac{e^{in\alpha} - e^{-in\alpha}}{2i} = \frac{1}{2i} (\cos \alpha + i \sin \alpha)^n - \frac{1}{2i} (\cos \alpha - i \sin \alpha)^n$$

(observe que $\cos \alpha + i \sin \alpha$ e $\cos \alpha - i \sin \alpha$ são as raízes de $x^2 - 2 \cos \alpha \cdot x + 1$). \square

Observação B.6. Se (x_n) satisfaz $\text{Rec}((x-1)P(x))$, onde $P(x) = a_n x^k + \dots + a_0$, então, se definirmos $y_n = a_k x_{n+k} + a_{k-1} x_{n+k-1} + \dots + a_0 x_n$, teremos $y_{n+1} = y_n$, $\forall n \in \mathbb{N}$, ou seja, y_n é constante. Assim, $a_k x_{n+k} + \dots + a_0 x_n$ é um invariante da sequência x_n , o que é um fato útil para muitos problemas envolvendo recorrências (veja, por exemplo, os exemplos a seguir).

Vamos agora ver um problema resolvido em que se usam estimativas assintóticas de sequências recorrentes para provar um resultado de Teoria dos Números:

Exemplo B.7 (Problema 69 da Revista Eureka! 14). Sejam a e b inteiros positivos tais que $a^n - 1$ divide $b^n - 1$ para todo inteiro positivo n .

Prove que existe $k \in \mathbb{N}$ tal que $b = a^k$.

SOLUÇÃO: (DE ZOROASTRO AZAMBUJA NETO, RIO DE JANEIRO-RJ)
Suponha por absurdo que b não seja uma potência de a .

Então existe $k \in \mathbb{N}$ tal que $a^k < b < a^{k+1}$. Consideremos a sequência

$x_n = \frac{b^n - 1}{a^n - 1} \in \mathbb{N}$, $\forall n \geq 1$. Como $\frac{1}{a^n - 1} = \frac{1}{a^n} + \frac{1}{a^{2n}} + \cdots = \sum_{j=1}^{\infty} \frac{1}{a^{jn}}$, temos

$$\begin{aligned} x_n &= \sum_{j=1}^{\infty} \frac{b^n}{a^{jn}} - \frac{1}{a^n - 1} \\ &= \left(\frac{b}{a}\right)^n + \left(\frac{b}{a^2}\right)^n + \cdots + \left(\frac{b}{a^k}\right)^n + \frac{b^n}{a^{kn}(a^n - 1)} - \frac{1}{a^n - 1}. \end{aligned}$$

Note que como $\frac{b^n}{a^{kn}(a^n - 1)} = \frac{(b/a^{k+1})^n}{1 - a^{-n}}$ e $\frac{1}{a^n - 1}$ tendem a 0 quando n cresce, se definimos

$$y_n = \left(\frac{b}{a}\right)^n + \left(\frac{b}{a^2}\right)^n + \cdots + \left(\frac{b}{a^k}\right)^n = \sum_{j=1}^k \left(\frac{b}{a^j}\right)^n,$$

temos que

$$x_n - y_n = \frac{b^n}{a^{kn}(a^n - 1)} - \frac{1}{a^n - 1}$$

tende a 0 quando n tende a infinito. Por outro lado, como y_n é uma soma de k progressões geométricas de razões b/a^j , $1 \leq j \leq k$, y_n satisfaz a equação de recorrência $c_0 y_{n+k} + c_1 y_{n+k-1} + \cdots + c_k y_n = 0$, $\forall n \geq 0$, onde

$$c_0 x^k + c_1 x^{k-1} + \cdots + c_{k-1} x + c_k = a^{k(k+1)/2} \left(x - \frac{b}{a}\right) \left(x - \frac{b}{a^2}\right) \cdots \left(x - \frac{b}{a^k}\right)$$

Note que todos os c_i são inteiros. Note também que

$$\begin{aligned} &c_0 x_{n+k} + c_1 x_{n+k-1} + \cdots + c_k x_n \\ &= c_0 (x_{n+k} - y_{n+k}) + c_1 (x_{n+k-1} - y_{n+k-1}) + \cdots + c_k (x_n - y_n) \end{aligned}$$

tende a 0 quando n tende a infinito, pois $x_{n+j} - y_{n+j}$ tende a 0 para todo j com $0 \leq j \leq k$ (e k está fixo). Como os c_i e os x_n são todos inteiros, isso mostra que $c_0 x_{n+k} + c_1 x_{n+k-1} + \cdots + c_k x_n = 0$ para todo n grande.

Agora, como

$$x_n = y_n + \left(\frac{b}{a^{k+1}}\right)^n + \frac{b^n}{a^{(k+1)n}(a^n - 1)} - \frac{1}{a^n - 1},$$

temos

$$c_0 x_{n+k} + c_1 x_{n+k-1} + \cdots + c_k x_n = \sum_{j=0}^k c_j \left(\left(\frac{b}{a^{k+1}} \right)^{n+k-j} + z_{n+k-j} \right),$$

onde

$$z_m = \frac{b^m}{a^{(k+1)m}(a^m - 1)} - \frac{1}{a^m - 1}.$$

Note que

$$\sum_{j=0}^k c_j \left(\frac{b}{a^{k+1}} \right)^{n+k-j} = P \left(\frac{b}{a^{k+1}} \right) \cdot \left(\frac{b}{a^{k+1}} \right)^n,$$

onde

$$\begin{aligned} P(x) &= c_0 x^k + c_1 x^{k-1} + \cdots + c_{k-1} x + c_k \\ &= a^{k(k+1)/2} \left(x - \frac{b}{a} \right) \left(x - \frac{b}{a^2} \right) \cdots \left(x - \frac{b}{a^k} \right), \end{aligned}$$

donde $P \left(\frac{b}{a^{k+1}} \right) \neq 0$. Por outro lado, para todo j com $0 \leq j \leq k$,

$$\frac{z_{n+k-j}}{\left(\frac{b}{a^{k+1}} \right)^n} = \frac{(b/a^{k+1})^{k-j}}{a^{n+k-j} - 1} - \frac{1}{(a^{k-j} - a^{-n})(b/a^k)^n},$$

que tende a 0 quando $n \rightarrow \infty$, donde $w_n = \left(\sum_{j=0}^k c_j x_{n+k-j} \right) / \left(\frac{b}{a^{k+1}} \right)^n$

tende a $P \left(\frac{b}{a^{k+1}} \right) \neq 0$, o que é um absurdo, pois, como vimos antes, w_n é igual a 0 para todo n grande. \square

Veremos a seguir dois problemas resolvidos que envolvem sequências recorrentes, que foram propostos na OBM e na IMO, respectivamente:

Exemplo B.8 (Problema 5 da XIII OBM Sênior). *Seja Q_0 o quadrado de vértices $P_0 = (1, 0)$, $P_1 = (1, 1)$, $P_2 = (0, 1)$ e $P_3 = (0, 0)$. Seja A_0 o interior desse quadrado. Para cada $n \in \mathbb{N}$, P_{n+4} é o ponto médio do segmento $\overline{P_n P_{n+1}}$, Q_n é o quadrilátero de vértices P_n, P_{n+1}, P_{n+2} e P_{n+3} e A_n é o interior de Q_n . Encontre a interseção de todos os A_n .*

SOLUÇÃO:

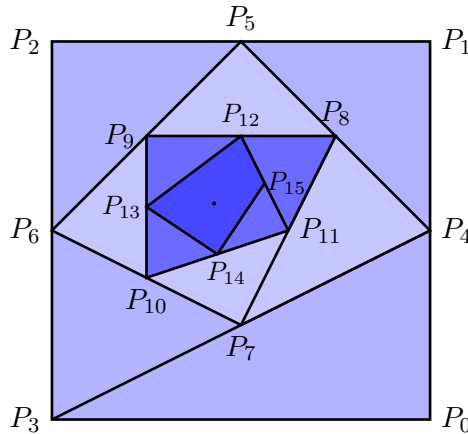
Primeira solução: temos

$$P_{n+4} = \frac{P_n + P_{n+1}}{2}$$

Portanto $P_{n+1} + 2P_{n+2} + 2P_{n+3} + 2P_{n+4} = P_n + 2P_{n+1} + 2P_{n+2} + 2P_{n+3}$, logo $P_n + 2P_{n+1} + 2P_{n+2} + 2P_{n+3} = P_0 + 2P_1 + 2P_2 + 2P_3 = (3, 4)$, para todo $n \in \mathbb{N}$ (note que $2x^4 - x - 1 = (x - 1)(2x^3 + 2x^2 + 2x + 1)$), donde, como A_n é sempre convexo,

$$\begin{aligned} \left(\frac{3}{7}, \frac{4}{7} \right) &= \frac{P_n + 2P_{n+1} + 2P_{n+2} + 2P_{n+3}}{7} \\ &= \frac{3}{7} \left(\frac{1}{3}P_n + \frac{2}{3}P_{n+1} \right) + \frac{4}{7} \left(\frac{P_{n+2} + P_{n+3}}{2} \right) \end{aligned}$$

sempre pertence ao interior de A_n . Se mostrarmos que o diâmetro (maior distância entre 2 pontos) de A_n tende a 0, teremos mostrado que a interseção de todos os A_n é $\left\{ \left(\frac{3}{7}, \frac{4}{7} \right) \right\}$.



Para isso, note que o diâmetro de $ABCD$ é

$$\text{diam}(ABCD) = \max \{ \overline{AB}, \overline{AC}, \overline{AD}, \overline{BC}, \overline{BD}, \overline{CD} \}$$

e

$$\begin{aligned}
P_{n+4} &= \frac{P_n + P_{n+1}}{2}, & P_{n+5} &= \frac{P_{n+1} + P_{n+2}}{2}, & P_{n+6} &= \frac{P_{n+2} + P_{n+3}}{2}, \\
P_{n+7} &= \frac{P_{n+3} + P_{n+4}}{2} = \frac{2P_{n+3} + P_n + P_{n+1}}{4} & e \\
P_{n+8} &= \frac{P_{n+4} + P_{n+5}}{2} = \frac{P_n + 2P_{n+1} + P_{n+2}}{4}.
\end{aligned}$$

Assim,

$$\begin{aligned}
\overline{P_{n+5}P_{n+6}} &= |P_{n+6} - P_{n+5}| = \left| \frac{P_{n+3} - P_{n+1}}{2} \right| = \frac{1}{2} \overline{P_{n+1}P_{n+3}} \\
\overline{P_{n+5}P_{n+7}} &= |P_{n+7} - P_{n+5}| = \left| \frac{2P_{n+3} + P_n - P_{n+1} - 2P_{n+2}}{4} \right| \\
&\leq \frac{1}{2} |P_{n+3} - P_{n+2}| + \frac{1}{4} |P_n - P_{n+1}| = \frac{\overline{P_{n+2}P_{n+3}}}{4} + \frac{\overline{P_nP_{n+1}}}{2}, \\
\overline{P_{n+5}P_{n+8}} &= |P_{n+8} - P_{n+5}| = \left| \frac{P_n - P_{n+2}}{4} \right| = \frac{\overline{P_nP_{n+2}}}{4}, \\
\overline{P_{n+6}P_{n+7}} &= |P_{n+7} - P_{n+6}| = \left| \frac{P_n + P_{n+1} - 2P_{n+2}}{4} \right| \\
&\leq \frac{|P_n - P_{n+2}|}{4} + \frac{|P_{n+1} - P_{n+2}|}{4} = \frac{1}{4} \overline{P_nP_{n+2}} + \frac{1}{4} \overline{P_{n+1}P_{n+2}}, \\
\overline{P_{n+6}P_{n+8}} &= |P_{n+8} - P_{n+6}| = \left| \frac{P_n + 2P_{n+1} - P_{n+2} - 2P_{n+3}}{4} \right| \\
&\leq \frac{1}{2} |P_{n+1} - P_{n+3}| + \frac{1}{4} |P_n - P_{n+2}| = \frac{1}{2} \overline{P_{n+1}P_{n+3}} + \frac{1}{4} \overline{P_nP_{n+2}}, \\
\overline{P_{n+7}P_{n+8}} &= |P_{n+8} - P_{n+7}| = \left| \frac{P_{n+2} + P_{n+1} - 2P_{n+3}}{4} \right| \\
&\leq \frac{|P_{n+2} - P_{n+3}|}{4} + \frac{|P_{n+1} - P_{n+3}|}{4} \\
&= \frac{1}{4} \overline{P_{n+2}P_{n+3}} + \frac{1}{4} \overline{P_{n+1}P_{n+3}}.
\end{aligned}$$

Portanto $\text{diam}(P_{n+5}P_{n+6}P_{n+7}P_{n+8}) \leq \frac{3}{4} \text{diam}(P_nP_{n+1}P_{n+2}P_{n+3})$,
donde

$$\text{diam}(P_{5k}P_{5k+1}P_{5k+2}P_{5k+3}) \leq \left(\frac{3}{4}\right)^k \text{diam}(P_0P_1P_2P_3) = \sqrt{2} \cdot \left(\frac{3}{4}\right)^k,$$

que tende a 0, o que implica o nosso resultado.

Segunda solução: podemos escrever $P_n = Q_0 + Q_1\alpha^n + Q_2\beta^n + Q_3\gamma^n$, onde $1, \alpha, \beta$ e γ são as raízes de $x^4 - \left(\frac{x+1}{2}\right) = 0$, ou seja, α, β e γ são raízes de $2x^3 + 2x^2 + 2x + 1 = 0$ (pois $(x-1)(2x^3 + 2x^2 + 2x + 1) = 2x^4 - x - 1$). Temos $P(x) = 2x^3 + 2x^2 + 2x + 1 = 2(x-\alpha)(x-\beta)(x-\gamma)$. Como $P(0) = 1$, $P(-1) = -1$ e $P\left(-\frac{1}{2}\right) = \frac{1}{4}$ podemos supor que $-1 < \alpha < -\frac{1}{2}$, logo $\beta\gamma = -1/2\alpha < 1$ e $\beta + \gamma = -1 - \alpha \in (-1, 0)$, donde $(\beta + \gamma)^2 - 4\beta\gamma = 1 + 2\alpha + \alpha^2 + \frac{2}{\alpha} < 0$ pois $\alpha < 0 \implies \alpha + \frac{1}{\alpha} \leq -2$ e $|\alpha| < 1 \implies \alpha^2 < 1$. Assim, $(\beta - \gamma)^2 < 0$, donde β e γ são complexos conjugados, e $|\beta| = |\gamma| = \sqrt{\beta\gamma} < 1$. Portanto, P_n tende a Q_0 quando n cresce, e logo a interseção de todos os A_n deve ser Q_0 .

Para calcular Q_0 , observe que:

$$\begin{cases} Q_0 + Q_1 + Q_2 + Q_3 = P_0 \\ Q_0 + Q_1\alpha + Q_2\beta + Q_3\gamma = P_1 \\ Q_0 + Q_1\alpha^2 + Q_2\beta^2 + Q_3\gamma^2 = P_2 \\ Q_0 + Q_1\alpha^3 + Q_2\beta^3 + Q_3\gamma^3 = P_3 \end{cases}$$

assim

$$\begin{aligned} & 7Q_0 + Q_1(1 + 2\alpha + 2\alpha^2 + 2\alpha^3) + Q_2(1 + 2\beta + 2\beta^2 + 2\beta^3) \\ & \quad + Q_3(1 + 2\gamma + 2\gamma^2 + 2\gamma^3) = P_0 + 2P_1 + 2P_2 + 2P_3 \\ \implies & 7Q_0 = P_0 + 2P_1 + 2P_2 + 2P_3 \quad (*) \\ \implies & Q_0 = \frac{P_0 + 2P_1 + 2P_2 + 2P_3}{7} = \left(\frac{3}{7}, \frac{4}{7}\right) \end{aligned}$$

onde em $(*)$ usamos o fato de α, β e γ serem raízes de $2x^3 + 2x^2 + 2x + 1$. \square

Exemplo B.9 (Problema 3 da XLI IMO, Coreia do Sul). *Seja $n \geq 2$ um inteiro. Existem n pulgas numa reta horizontal, nem todas no mesmo ponto. Para um dado número real positivo ℓ , define-se um salto da seguinte maneira:*

- *Escolhem-se duas pulgas quaisquer nos pontos A e B , com o ponto A à esquerda do ponto B ;*
- *A pulga que está em A salta até o ponto C da reta, à direita de B , tal que $\frac{BC}{AB} = \ell$.*

Determine todos os valores de ℓ para os quais, dado qualquer ponto M na reta e quaisquer posições iniciais das n pulgas, existe uma sucessão finita de saltos que levam todas as pulgas para pontos à direita de M .

SOLUÇÃO: A resposta é: para $\ell \geq \frac{1}{(n-1)}$.

Devemos demonstrar duas coisas:

- (a) que, para $\ell \geq \frac{1}{(n-1)}$, existe uma sequência infinita de movimentos que vai levando as pulgas cada vez mais para a direita, ultrapassando qualquer ponto prefixado M ;
- (b) que, para $\ell < \frac{1}{(n-1)}$ e para qualquer posição inicial das pulgas, existe um ponto M tal que as pulgas em um número finito de movimentos jamais alcançam ou ultrapassam M .

Começaremos pelo item (b). Sejam x_1, x_2, \dots, x_n as posições iniciais das pulgas, com $x_1 \leq x_2 \leq \dots \leq x_n$, de tal forma que x_n é a posição da pulga mais à direita. Seja

$$P = \left(\frac{1}{1 - (n-1)\ell} \right) \cdot (x_n - \ell \cdot x_1 - \ell \cdot x_2 - \dots - \ell \cdot x_{n-1}).$$

O ponto P claramente está à direita de todas as pulgas.

Sejam x'_1, \dots, x'_n as novas posições após alguns movimentos e definamos

$$P' = \left(\frac{1}{1 - (n-1)\ell} \right) \cdot (x'_n - \ell \cdot x'_1 - \ell \cdot x'_2 - \dots - \ell \cdot x'_{n-1}).$$

Afirmamos então que $P' \leq P$, o que conclui a demonstração, pois isso mostra que as pulgas nunca passarão do ponto P .

Para provar esta afirmação, basta considerar o que ocorre após um movimento.

Se a pulga que estava em x_i pula sobre a pulga que estava em x_n então $x'_n - x_n = \ell \cdot (x_n - x_i)$ e $x'_n - \ell \cdot x_n = x_n - \ell \cdot x_i$ e $P' = P$.

Vamos ver que qualquer outro caso é ainda mais favorável. Suponhamos que a pulga que estava em x_i pula sobre a pulga que estava em x_j . Se a pulga que pulou continua atrás de x_n , temos $x'_n = x_n$ e $x'_1 + \dots + x'_{n-1} > x_1 + \dots + x_{n-1}$, donde $P' < P$. Se ela passa de x_n , teremos $x'_n = x_j + \ell(x_j - x_i) \implies x'_n - \ell x_n < x'_n - \ell x_j = x_j - \ell x_i < x_n - \ell x_i$, donde novamente temos $P' < P$.

Vamos agora ao item (a): Seja $P = x_n - \ell(x_1 + x_2 + \cdots + x_{n-1})$ se, em cada movimento, a pulga mais à esquerda pula sobre a pulga mais à direita, temos $x'_n = x_n + \ell(x_n - x_1) \implies x'_n - \ell x_n = x_n - \ell x_1$. Assim, se as novas posições são $x'_1 = x_2, \dots, x'_{n-1} = x_n$ e $x'_n = x'_n - \ell(x'_1 + x'_2 + \cdots + x'_{n-1})$, temos $P' = P$, donde P é uma constante. Podemos supor sem perda de generalidade que P é positivo (escolhendo a origem, por exemplo, em $\frac{x_1 + \cdots + x_{n-1}}{n-1}$; note que então teremos sempre $\frac{x_1 + \cdots + x_{n-1}}{n-1} \geq 0$). Temos então

$$\begin{aligned} \frac{1}{n-1} \sum_{j=1}^{n-1} (x_n - x_j) &= x_n - \frac{1}{n-1} (x_1 + \cdots + x_{n-1}) \\ &\geq x_n - \ell(x_1 + \cdots + x_{n-1}) = P \end{aligned}$$

e assim

$$x_n - x_1 \geq \frac{1}{n-1} \sum_{j=1}^{n-1} (x_n - x_j) \geq P \implies x'_n - x_n = \ell(x_n - x_1) \geq \frac{P}{n-1},$$

donde o ponto mais à direita caminha pelo menos $\frac{P}{n-1}$ para a direita a cada passo, logo tende a infinito. Como o ponto mais à direita após $n-1$ passos será o ponto mais à esquerda, todos os pontos tendem a infinito (para a direita). \square

Observação B.10. Na estratégia descrita na solução do item (a), o ponto mais à esquerda se torna sempre o mais à direita, donde podemos definir $x_{n+1} = x'_n = x_n + \ell(x_n - x_1)$, e teríamos simplesmente $x'_j = x_{j+1}$, $\forall j$. Reduzimos então a análise dessa estratégia ao estudo da recorrência linear $x_{n+1} = (1 + \ell)x_n - \ell x_1$, cujo polinômio característico é $P(x) = x^{n+1} - (1 + \ell)x^n + \ell$, do qual 1 é raiz, donde, como $\frac{P(x)}{x-1} = x^n - \ell(x^{n-1} + x^{n-2} + \cdots + x + 1)$, a expressão $y_m = x_m - \ell(x_{m-1} + x_{m-2} + \cdots + x_{m-n+1} + x_{m-n})$ é um invariante da recorrência, isto é, $y_{m+1} = y_m \forall m$, donde y_m é constante. Daí vem nossa fórmula para P .

Concluimos com o problema a seguir, que é uma interessante aplicação de sequências recorrentes à trigonometria.

Exemplo B.11. *Prove que os ângulos agudos de um triângulo retângulo de lados 3, 4 e 5 são irracionais quando expressos em graus (i.e., são múltiplos irracionais de π).*

SOLUÇÃO: Considere a sequência $x_n = \frac{(2+i)^n - (2-i)^n}{2i}$. Temos $x_0 = 0$, $x_1 = 1$ e, como $2+i$ e $2-i$ são raízes da equação $x^2 - 4x + 5 = 0$, (x_n) satisfaz a recorrência $x_{n+2} = 4x_{n+1} - 5x_n$. Daí segue que x_{n+2} é congruente a $-x_{n+1}$ módulo 5 para todo $n \geq 1$, donde x_n é congruente a $(-1)^{n+1}$ para todo $n \geq 1$, e logo x_n não é múltiplo de 5 para nenhum $n \geq 1$. Em particular, $x_n \neq 0$, para todo $n \geq 1$. Assim, $1 \neq \frac{(2+i)^n}{(2-i)^n} = (\frac{2+i}{2-i})^n = (\frac{3}{5} + \frac{4}{5}i)^n$, para todo $n \geq 1$. Se $\theta = \cos^{-1}(3/5)$, $\frac{3}{5} + \frac{4}{5}i = e^{i\theta}$, donde $(\frac{3}{5} + \frac{4}{5}i)^n = e^{in\theta} \neq 1$, para todo $n \geq 1$, o que implica que θ/π é irracional (de fato, se $\theta/\pi = p/q$, teríamos $e^{2iq\theta} = e^{2ip\pi} = 1$). \square

Observação B.12. *Para uma versão mais geral deste problema, veja o Problema 88 proposto na Eureka! 17, p. 60, por Carlos Gustavo Moreira e José Paulo Carneiro, e a solução de seus autores publicada na Eureka! 20, pp. 52–53.*

Problemas Propostos

B.1. *Seja $x_0 \geq 3$ um inteiro ímpar.*

- (i) *Prove que se p é um número primo então existe no máximo um valor de $n \in \mathbb{N}$ tal que p divide x_n .*
- (ii) *Prove que se p é um fator primo de x_n então $p > n$.*

Dica: Considere a sequência $x_n \bmod p$.

Esse exercício pode ser generalizado para outras recorrências. Nesse caso particular da recorrência $x_{n+1} = x_n^2 - 2$ é possível mostrar um resultado mais forte: se p é um fator primo de x_n então $p \geq 2^{n+2} - 1$ (note que quando $p = 2^q - 1$ é primo, com $q \geq 3$ e $n = q - 2$, vale a igualdade $p = 2^{n+2} - 1$ e $p \mid x_n$, pelo critério de Lucas-Lehmer enunciado acima).

B.2. *Seja $\{a_n\}$ uma sequência estritamente crescente de inteiros que satisfazem a recorrência*

$$a_n = 4a_{n-1} - a_{n-2} \quad \text{para } n > 2 \quad \text{e} \quad a_4 = 194.$$

Encontrar a_5 .

Dica: Encontrar a_4 em função de a_0 e a_1 , escrever uma equação linear cujas soluções são $a_0 = 56t - 2$ e $a_1 = 15t + 4$, como $a_0 < a_1$ então $t \leq 0$, por último demonstrar que se t é negativo então a sequência em algum momento começará a decrescer.

B.3 (OIbM1998). *Seja λ a solução positiva da equação $x^2 - 1998x - 1 = 0$. Defina a sequência $\{x_i\}$ tal que $x_0 = 1$ e $x_{n+1} = \lfloor \lambda x_n \rfloor$ para todo $n \in \mathbb{N}$. Calcule o resto da divisão de x_{1998} por 1998.*

B.4. *Demonstrar que $\text{mdc}(\frac{F_{np}}{F_n}, p^2) = p$.*

A sequência de Lucas é definida por $L_0 = 2$, $L_1 = 1$ e $L_{n+2} = L_{n+1} + L_n$ para $n \geq 0$.

B.5. *Seja $p > 5$ um primo e n um inteiro par, demonstrar que*

1. *Se $L_n \equiv 2 \pmod{p}$, então $L_n \equiv 2 \pmod{p^2}$;*
2. *Se $L_n \equiv -2 \pmod{p}$, então $L_n \equiv -2 \pmod{p^2}$;*

B.6. *Seja r um inteiro positivo, demonstrar que*

$$L_{5^r} \equiv L_{5^{r-1}} \pmod{5^r}.$$

B.7. *Seja n um inteiro par positivo tal que $L_n \equiv 2 \pmod{p}$, onde p é um primo ímpar. Demonstrar que*

$$L_{n+1} \equiv 1 \pmod{p}.$$

B.8. *Resolver a recorrência*

$$a_{n+1} = 5a_n^3 - 3a_n, \quad n \geq 0$$

com condição inicial $a_0 = 1$.

B.9. *Demonstrar que*

$$L_n^2 = 5F_n^2 + 4(-1)^n$$

B.10. *Demonstrar que*

$$F_n = 1 + \binom{n-2}{1} + \binom{n-3}{2} + \cdots + \binom{n-j}{j-1} + \binom{n-j-1}{j}$$

onde j é o maior inteiro que é menor do que ou igual a $(n-1)/2$.

B.11. *Demonstrar que*

$$\binom{n}{1}F_1 + \binom{n}{2}F_2 + \binom{n}{3}F_3 + \cdots + \binom{n}{n-1}F_{n-1} + \binom{n}{n}F_n = F_{2n}.$$

B.12. *Demonstrar que $L_n^2 - 2L_{2n} = 5F_n^2$.*

B.13. *Demonstrar que*

$$\frac{F_{n(2k+1)}}{F_n} = \sum_{i=0}^{k-1} (-1)^{in} L_{(2k-2i)t} + (-1)^{kt}$$

e

$$\frac{F_{2nk}}{F_n} = \sum_{i=0}^{k-1} (-1)^{in} L_{(2k-2i-1)t}.$$

B.14. *Seja $\{a_n\}_{n \geq 1}$ uma sequência definida por*

$$a_1 = 2, \quad a_2 = 8, \quad a_{n+2} = 3a_{n+1} - a_n + 5(-1)^n \text{ para } n \geq 1.$$

Mostrar que se a_n é um número primo, então n tem que ser uma potência de 3.

B.15. *A sequência $\{b_n\}$ é definida por*

$$b_0 \in [0, 1], \quad b_{n+1} = 1 - |1 - 2b_n|.$$

Mostrar que a sequência é periódica se, e somente se, x_0 é irracional.

B.16. *A sequência $\{x_n\}_{n \geq 1}$ é definida por*

$$x_1 = x_2 = 1, \quad x_{n+2} = 14x_{n+1} - x_n - 4 \quad (n = 1, 2, \dots)$$

Mostrar que x_n é sempre um quadrado perfeito.

B.17. *Seja $\{x_n\}_{n \geq 1}$ uma sequência de números inteiros positivos tal que*

$$0 < x_{n+1} - x_n \leq 2010 \quad \text{para todo } n \in \mathbb{N}.$$

Mostrar que existem infinitos pares (a, b) de inteiros positivos tais que $b > a$ e $x_a \mid x_b$.

B.18. *A sequência $\{a_n\}_{n \geq 1}$ é definida por*

$$a_1 = 1, \quad a_{n+1} = 2a_n + \sqrt{3a_n^2 + 1} \quad \text{para todo } n \geq 1$$

Mostrar que a_n é um número inteiro para todo n .

B.19. *A sequência $\{a_n\}_{n \geq 1}$ é definida por $a_1 = 1$*

$$a_{n+1} = \frac{a_n}{2} + \frac{1}{4a_n} \quad \text{para } n \in \mathbb{N}.$$

Mostrar que $\sqrt{\frac{2}{2a_n^2 - 1}}$ é um número inteiro positivo para $n > 1$.

B.20 (Banco-IMO1988). *Seja α a maior raiz real da equação $x^3 - 3x^2 + 1 = 0$. Prove que $\lfloor \alpha^{1988} \rfloor$ é divisível por 17.*

B.21 (OBM2011). *Seja $(x_n)_{n \geq 0}$ uma sequência de números inteiros não todos nulos que satisfaz uma recorrência linear de ordem k para um certo inteiro positivo k fixado, i.e., existem constantes reais c_1, c_2, \dots, c_k tais que $x_{n+k} = \sum_{r=1}^k c_r x_{n+k-r}$ para todo $n \geq 0$. Suponha que k é o menor inteiro positivo com esta propriedade. Prove que $c_j \in \mathbb{Z}$ para todo j com $1 \leq j \leq k$.*

Apêndice C

Qual o próximo destino?

Ao completarmos este breve passeio pelo mundo inteiro, surge a natural pergunta: o que mais resta explorar? Nós, autores, confrontados com a tarefa de oferecer um panorama geral de uma área tão rica e diversa como a Teoria dos Números, tivemos que fazer algumas difíceis escolhas sobre o que incluir e omitir: o bom senso dita que há limites para o que se pode dizer neste confinado espaço sem que o livro se transformasse numa massa disforme percorrendo sobre tudo e que a ninguém serviria.

Assim, vários tópicos importantes, muitos dos quais particularmente caros a estes autores, acabaram por não tomar vida neste manuscrito. Como solução remedial, este epílogo visa a indicar algumas destas direções ocultadas, sugestões de possíveis itinerários pelos quais o leitor possa se aventurar, neste que é o fascinante mundo da Teoria dos Números.

C.1 Alguns comentários e sugestões

C.1.1 Fundamentos

O leitor terá notado que começamos o livro já supondo que ele conhecesse bem os números naturais e os reais. Não discutimos a axiomatização dos naturais, tema que desviaria o rumo do livro. Muitos livros de matemática, como [91], discutem tais sistemas de axiomas. O axioma mais interessante para os naturais é o da indução, que apresentamos no início do livro e que toma como implícito o conceito de conjunto (e por-

tanto pelo menos uma parte da teoria dos conjuntos). Na verdade tanto os naturais quanto os reais podem ser construídos dentro da teoria dos conjuntos, conforme discutido em vários livros introdutórios de teoria dos conjuntos (como [65]). Uma construção bem diferente dos inteiros e dos reais é feita via jogos combinatórios e números surreais por John Conway em [37].

A discussão de problemas sobre os naturais (ou os inteiros) é muitas vezes melhor entendida com recurso a números reais ou complexos. Há vários exemplos disso neste livro. Esta prática não é apenas uma ajuda para a intuição dos matemáticos, uma espécie de figura explicativa: em [114], Paris e Harrington exibem um problema de enunciado finitário que não admite demonstração na aritmética de Peano, isto é, não admite uma demonstração finitária, sem falar de conjuntos infinitos.

C.1.2 Leis de Reciprocidade

A lei de reciprocidade quadrática de Gauß é apenas uma das várias leis de reciprocidade na natureza. O próprio Gauß enunciou a lei de reciprocidade biquadrática (para quartas potências), enquanto seu aluno Eisenstein foi responsável pela reciprocidade cúbica. Tais resultados envolvem a aritmética de inteiros algébricos, a saber a de $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$; enunciados e provas de tais leis de reciprocidade podem ser vistas em [77].

A lei de reciprocidade geral é a chamada *reciprocidade de Artin*, principal resultado da *Teoria de Corpos de Classe*, que descreve as extensões abelianas (i.e. extensões galoisianas cujo grupo de Galois é abeliano) de um corpo de números em termos dos completamentos p -ádicos deste corpo (ver abaixo). Tal descrição está intimamente ligada às leis de reciprocidade como acima discutidas e é, por assim dizer, a “explicação” de tais fenômenos. A prova usual da reciprocidade de Artin, utilizando cohomologia Galoisiana, pode ser vista em [31]. Em [112], o leitor poderá ver uma prova totalmente elementar (mas elaborada) deste resultado.

C.1.3 Inteiros p -ádicos

Como vimos, o lema de Hensel (Lema 2.21) permite, sob certas condições, encontrar uma sequência de soluções r_n para as equações diofantinas $f(x) \equiv 0 \pmod{p^n}$, p primo, “compatíveis entre si” no sentido que $r_{n+1} \equiv r_n \pmod{p^n}$ para todo n . Por exemplo, se $p = 5$ e $f(x) = x^2 - 6$,

uma tal sequência de “soluções coerentes”, escritas na base $p = 5$, é dada por

$$\begin{aligned} r_0 &= 1 \\ r_1 &= r_2 = 1 + 3 \cdot 5 \\ r_3 &= 1 + 3 \cdot 5 + 4 \cdot 5^3 \\ r_4 &= 1 + 3 \cdot 5 + 4 \cdot 5^3 + 2 \cdot 5^4 \\ &\vdots \end{aligned}$$

Tal sequência pode ser simbolicamente representada pela seguinte “expansão infinita na base 5”

$$r = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + \dots$$

de modo que r é uma “raiz quadrada de 6”. Uma expressão como r acima é um exemplo de um número 5-*ádico*.

Em 1902, Kurt Hensel introduziu, para todo primo p , o anel \mathbb{Z}_p dos *números p -ádicos* como o anel cujos elementos são tais expansões (formais) infinitas na base p , com a soma e a multiplicação feitas da “maneira usual”. Este anel é um domínio e seu corpo de frações é denotado \mathbb{Q}_p . Por exemplo, no anel \mathbb{Z}_5 , 6 é um quadrado perfeito pois $r^2 = 6$. Em \mathbb{Z}_2 temos a “soma da PG”

$$1 + 2 + 2^2 + 2^3 + \dots = \frac{1}{1-2} = -1$$

Embora isto possa a princípio parecer apenas um artifício formal, a simplicidade e elegância obtidas ao considerarmos esta nova formulação consolidou estes novos objetos como protagonistas na Teoria dos Números contemporânea. Um dos resultados clássicos é o chamado *princípio local-global* ou *princípio de Haß*, que norteia boa parte do desenvolvimento da teoria. Neste contexto, temos por exemplo o *teorema de Haß-Minkowski*, que afirma que uma forma quadrática

$$a_1x_1^2 + a_2x_2^2 + \dots + a_nx_n^2 \quad a_i \in \mathbb{Q}$$

possui um zero não trivial $(r_1, \dots, r_n) \neq (0, \dots, 0)$ sobre \mathbb{Q} (i.e. $r_i \in \mathbb{Q}$) se, e só se, ela possui zeros não triviais sobre \mathbb{R} e sobre \mathbb{Q}_p para todo primo p . Boas exposições deste e outros resultados encontram-se nos livros [130] e [18].

C.1.4 Geometria Diofantina

Um dos casamentos mais fortuitos do século XX foi o da Teoria dos Números com a Geometria Algébrica, dando origem à chamada *Geometria Diofantina*. O último capítulo, sobre curvas elípticas, é um pequeno aperitivo desta nova área, responsável talvez pela resolução da maior quantidade de problemas célebres em Teoria dos Números nos últimos anos, tais como as conjecturas de Weil (que, dentre várias outras consequências, fornece estimativas assintóticas para o número de soluções em um corpo finito de um sistema de equações polinomiais), a conjectura de Mordell (toda curva sobre \mathbb{Q} com gênero maior ou igual a 2 possui um número finito de pontos racionais) e o último teorema de Fermat.

Infelizmente mesmo uma introdução a esta fascinante área da Matemática foge completamente do escopo deste livro. Textos sobre a aritmética de curvas elípticas, como os listados abaixo, são um bom ponto de partida; mas eventualmente o leitor interessado por enveredar nesta direção precisará se familiarizar com a linguagem de *esquemas*, introduzida por Alexander Grothendieck nos anos 60. Uma boa introdução a esta linguagem é o livro de Mumford [110], mas que não traz aplicações aritméticas. O livro [92], embora mais técnico, foi escrito com aplicações aritméticas em mente e é uma de nossas recomendações.

C.2 Sugestões Bibliográficas

C.2.1 Textos Gerais

- K. F. Ireland and M. I. Rosen, *A classical introduction to modern number theory* [77] (um ótimo texto geral).
- J. P. Serre, *Cours d'arithmétique* [130] (texto relativamente curto, com muito bom gosto, contendo uma excelente introdução à aritmética p -ádica e às formas modulares).

C.2.2 Textos sobre Teoria Analítica dos Números

- A. E. Ingham, *The distribution of prime numbers* [76].
- H. Davenport, *Multiplicative number theory* [48].
- H. Rademacher, *Topics in analytic number theory* [123].

- T. M. Apostol, *Introduction to analytic number theory*, [5].
- T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory* [6] (excelente introdução às formas modulares com aplicações para partições e aproximações diofantinas).
- H. Iwaniec e E. Kowalski, *Analytic Number Theory* [78] (provavelmente o mais completo dos textos sobre Teoria Analítica dos Números).

C.2.3 Textos sobre Aproximações Diofantinas

Mencionamos inicialmente dois excelentes textos gerais sobre o assunto.

- J. W. S. Cassels, *An introduction to Diophantine approximation* [28] (um excelente texto geral sobre o assunto).
- W. M. Schmidt, *Diophantine approximation* [128] (outro texto geral, também excelente).
- Baker, Alan, *Transcendental number theory* [10] (um ótimo texto sobre aplicações de aproximações diofantinas à teoria da transcendência).
- Bugeaud, Yann, *Approximation by algebraic numbers* [25] (este livro, assim como o capítulo VIII de [128], trata de uma extensão da teoria clássica: ao invés de aproximarmos por racionais agora aproximamos por algébricos)

C.2.4 Textos sobre Teoria Algébrica dos Números

- J. Neukirch, *Algebraic Number Theory* [112] (uma das melhores e mais completas introduções à Teoria Algébrica dos Números, uma obra de arte!).
- Z. I. Borevitch e I. R. Shafarevitch, *Number theory* [18] (excelente texto sobre Teoria Algébrica dos Números especialmente do ponto de vista local)
- J-P. Serre, *Local Fields* [131].

- S. S. Shatz, *Profinite groups, Arithmetic, and Geometry* [133].
- *Algebraic number theory; proceedings of an instructional conference*, Editado por J. W. S. Cassels e A. Fröhlich [31] (este texto, como os dois anteriores, são mais avançados e cobrem a chamada Teoria de Corpos de Classe, que generaliza a reciprocidade quadrática de Gauß).

C.2.5 Textos sobre Curvas Elípticas e Geometria Diofantina

1. J. H. Silverman e J. Tate, *Rational Points on Elliptic Curves* [143] (assim como o próximo item, excelente introdução à aritmética de curvas elípticas).
2. A. W. Knap, *Elliptic Curves* [82].
3. J. W. S. Cassels, *Lectures on Elliptic Curves* [30].
4. J. H. Silverman, *The Arithmetic of Elliptic Curves* [141] (o texto clássico sobre o assunto).
5. D. Husemöller, *Elliptic Curves* [74].
6. D. Lorenzini, *An Invitation to Arithmetic Geometry* [93] (uma das mais acessíveis introduções à geometria diofantina, com a demonstração devida a Stepanov e Bombieri das conjecturas de Weil para curvas).
7. Q. Liu, *Algebraic Geometry and Arithmetic Curves* [92] (a melhor introdução à Geometria Algébrica para aplicações aritméticas).
8. J. H. Silverman e M. Hindry, *Diophantine Geometry: An Introduction* [142] (uma excelente exposição da prova “elementar”, devida a Vojta e Bombieri, da conjectura de Mordell)

Bibliografia

- [1] L. M. Adleman, C. Pomerance e R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. (2) 117 (1983), 173–206.
- [2] L. Adleman e M. Huang, *Primality testings and two dimensional Abelian varieties over finite fields*, Lecture Notes in Mathematics 1512 (1992).
- [3] M. Agrawal, N. Kayal e N. Saxena, *PRIMES is in P*, Ann. of Math. (2) 160 (2004), no. 2, 781–793; disponível também em <http://www.cse.iitk.ac.in/users/manindra/algebra/primality.pdf>
- [4] W. R. Alford, A. Granville e C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) 140 (1994), 703–722.
- [5] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag (1976).
- [6] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory* Graduate Texts in Mathematics v. 41 (1989).
- [7] A. Arbieto, C. Matheus e C. G. Moreira, *Aspectos Ergódicos da Teoria dos Números*, XXVI Colóquio Brasileiro de Matemática, IMPA (2007).
- [8] E. Bach, *Explicit bounds for primality testing and related problems*, Math. of Comp. 55 (1990), 355–380.
- [9] M. Beck, E. Pine, W. Tarrant, K. Yarbrough. *New Integer representations as the Sum of Three Cubes*, Math. of Comp. 76 (2007), 1683–1690.

- [10] A. Baker, *Transcendental number theory*, Cambridge University Press, London-New York, 1975. x+147 pp.
- [11] R. C. Baker, G. Harman e J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. 83 (2001), 532–562.
- [12] S. Barnard, e J. M. Child, *Higher Algebra*, Macmillam & Co. (1959).
- [13] A. Beiler, *Recreations in theory of Numbers*, Dover Publications (1964).
- [14] D. J. Bernstein, *Detecting perfect powers in essentially linear time*, Math. Comp., 67:223 (1998) 1253–1283.
- [15] D. J. Bernstein, *Proving primality in essentially quartic random time*, Math. Comp. 76 (2007), no. 257, 389–403.
- [16] P. Berrizbeitia, *Sharpening “PRIMES is in P” for a large family of numbers*, Math. Comp. 74 (2005), no. 252, 2043–2059.
- [17] N. Beskin, *Fracções contínuas*, Editora MIR, Moscou 1980.
- [18] Z. I. Borevitch e I. R. Shafarevitch, *Number theory*, Pure and applied mathematics 20, Academic Press (1966).
- [19] R. P. Brent, G. L. Cohen e H. J. J. te Riele, *Improved techniques for lower bounds for odd perfect numbers*, Math. Comp. 57 (1991), 857–868.
- [20] J. Brillhart, D. H. Lehmer e J. L. Selfridge, *New primality criteria and factorizations of $2m \pm 1$* , Math. Comp. 29 (1975), 620–647.
- [21] E. Bombieri, *Continued fractions and the Markoff tree*, Exp. Math. 25 (2007), 187–213.
- [22] J. W. Bruce, *A really trivial proof of the Lucas-Lehmer test*, Amer. Math. Monthly 100 (1993), no. 4, 370–371.
- [23] V. Brun, *La série $\frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{29} + \frac{1}{31} + \frac{1}{41} + \frac{1}{43} + \frac{1}{59} + \frac{1}{61} + \dots$ où les dénominateurs sont nombres premiers jumeaux est convergente ou finie*, Bull. Sci. Math., (2) 43 (1919), 100-104, 124-128.

- [24] V. Brun, *Le crible d'Ératosthène et le théorème de Goldbach*, Videnskabs-selskabet i Kristiania Skrifter I, Matematisk-Naturvidenskabelig Klasse No. 3 (1920) pp. 1-36.
- [25] Y. Bugeaud, *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics, 160. Cambridge University Press, Cambridge, 2004.
- [26] C. Caldwell, *The Largest Known Primes*, disponível eletronicamente em <http://primes.utm.edu/largest.html>
- [27] R. Carmichael, *The theory of numbers*, Dover Publications (1914).
- [28] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathematics and Mathematical Physics 45, Hafner Publishing Co. (1972)
- [29] J. W. S. Cassels, *Some metrical theorems in Diophantine approximation I*, Proc. Camb. Phil. Soc. 46 (1950), 209–218.
- [30] J. W. S. Cassels, *Lectures on Elliptic Curves* (London Mathematical Society Student Texts), Cambridge University Press (1991).
- [31] J. W. S. Cassels e A. Fröhlich (editores), *Algebraic number theory; proceedings of an instructional conference*, Academic Press (1967).
- [32] Q. Cheng, *Primality proving via one round of ECPP and one iteration in AKS*, J. Cryptology 20 (2007), no. 3, 375–387.
- [33] Y. Cheng, *Explicit estimate on primes between consecutive cubes*, Rocky Mountain J. Math 40, no. 1, 1–47 (2010). Também em <http://arxiv.org/abs/0810.2113v1>.
- [34] M. Cipolla, *Sui numeri composti P , che verificano la congruenza di Fermat $a^{P-1} \equiv 1 \pmod{P}$* , Annali di Matematica (3) 9, 1904, 139–160.
- [35] M. Clausen e U. Baum, *Fast Fourier Transforms*, BI-Wiss.-Verlag (1993).
- [36] H. Cohn, *A short proof of the simple continued fraction expansion of e* , Am. Math. Monthly 113, 57–62 (2006).

- [37] J. H. Conway, *On Numbers and Games*, Academic Press.
- [38] J. H. Conway e R. K. Guy, *The Book of Numbers*, Springer-Verlag (1996).
- [39] G. Cornell, J. H. Silverman e G. Stevens, *Modular Forms and Fermat's Last Theorem*, Springer-Verlag (2009).
- [40] S. C. Coutinho, *Números inteiros e criptografia RSA*, Coleção Computação e Matemática, SBM e IMPA (2000).
- [41] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arithmetica 2: 23–46 (1936).
- [42] R. Crandall e B. Fagin, *Discrete weighted transforms and large-integer arithmetic*, Math. Comp. 62 (1994), no. 205, 305–324.
- [43] R. Crandall e J. Papadopoulos, *On the implementation of AKS-class primality tests*, <http://www.apple.com/acg/pdf/aks3.pdf>
- [44] R. Crandall e C. Pomerance, *Prime Numbers — A Computational Perspective*, segunda edição, Springer (2005).
- [45] T. W. Cusick e M. E. Flahive, *The Markoff and Lagrange spectra*, Math. Surveys and Monographs, no. 30, A.M.S. (1989).
- [46] Lorenzo J. Díaz, Danielle de Rezende Jorge, *Uma introdução aos Sistemas Dinâmicos via Frações Contínuas*. 26º Colóquio Brasileiro de Matemática. IMPA, 2007. 211 p.
- [47] I. Damgård, P. Landrock e C. Pomerance, *Average case error estimates for the strong probable prime test*, Math. Comp. 61 (1993), no. 203, 177–194.
- [48] H. Davenport, *Multiplicative number theory*, Graduate texts in mathematics 74, Springer (1967).
- [49] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly, vol.80 (1973), pp. 233–269. (Reimpresso como apêndice em M. Davis, *Computability and Unsolvability*, Dover reprint 1982.)

- [50] H. G. Diamond, J. Pintz, *Oscillation of Mertens' product formula* Journal de théorie des nombres de Bordeaux 21, no. 3 (2009), 523–533.
- [51] P. Erdős, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. 35 (1949), 374–384.
- [52] P. Erdős e M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. 62 (1940), 738–742.
- [53] P. Erdős e C. Pomerance, *On the number of false witnesses for a composite number*, Math. Comp. 46 (1986), 259–279.
- [54] E. Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, Invent. Math. 79 (1985), no. 2, 383–407.
- [55] G. Frobenius, *Über die Markoffschen Zahlen*, Preuss. Akad. Wiss. Sitzungsberichte (1913), 458–487; disponível também em G. Frobenius, *Gesammelte Abhandlungen*, vol. 3, Springer (1968), 598–627.
- [56] M. Fürer, *Faster Integer Multiplication*, Proceedings of the thirty-ninth annual ACM symposium on Theory of computing, June 11–13, 2007, San Diego, California, USA.
- [57] D. A. Goldston, J. Pintz e C. Y. Yıldırım, *Primes in tuples I*, Ann. of Math. 170, 819–862 (2009). Também em [arxiv:math/0508185](#).
- [58] D. A. Goldston, J. Pintz e C. Y. Yıldırım, *Primes in tuples II*, Acta Math. 204, no. 1, 1–47 (2010). Também em [arxiv:0710.2728](#).
- [59] S. Goldwasser e J. Kilian, *Almost all primes can be quickly certified*, Proc. of Ann. IEEE Symp. on Foundations of Computer Science (1986), 316–329.
- [60] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete mathematics*, segunda edição, Addison-Wesley (1994).
- [61] J. Grantham, *There are infinitely many Perrin pseudoprimes*, J. Number Theory 130, no. 5, 1117–1128 (2010).

- [62] B. Green e T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math. 167, no. 2 (2008), 481–548.
- [63] R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag (1994).
- [64] M. Hall, *On the sum and product of continued fractions*, Annals of Math., Vol. 48, (1947), pp. 966–993.
- [65] P. R. Halmos, *Naive Set Theory*, Undergraduate Texts in Mathematics, Springer-Verlag.
- [66] Hardy, G. H., *On Dirichlet's Divisor Problem*, Proc. London Math. Soc.(2) 15 (1917), 1–25.
- [67] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers*, quinta edição, Oxford University Press (1979).
- [68] H. Helfgott, *Major arcs for Goldbach's problem*, preprint em <http://arxiv.org/pdf/1305.2897.pdf>.
- [69] G. H. Hardy e J. E. Littlewood, *Some problems of 'partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. 44 (1923), 1–70.
- [70] G. H. Hardy e S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. 17 (1918), 75–115.
- [71] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. 37 (1986), 27–38.
- [72] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.
- [73] L. K. Hua, *Introduction to number theory*, Springer-Verlag (1982).
- [74] D. Husemöller, *Elliptic Curves* (Graduate Texts in Mathematics, Vol.111), Springer-Verlag.
- [75] M. N. Huxley, *Exponential Sums and Lattice Points III*, Proc. London Math. Soc.(3) 87 (2003), 591–609.

- [76] A. E. Ingham, *The distribution of prime numbers*, Cambridge Tracts in Mathematics and Mathematical Physics 30, Cambridge University Press (1990) (publicado originalmente em 1932).
- [77] K. F. Ireland and M. I. Rosen, *A classical introduction to modern number theory*, Springer-Verlag (1982).
- [78] H. Iwaniec e E. Kowalski, *Analytic Number Theory*, Colloquium Publications, Vol. 53, AMS (2004).
- [79] A. Khintchine, *Zur metrischen Theorie der diophantischen Approximationen*, Math. Z. 24 (1926), no. 1, 706–714.
- [80] S. H. Kim e C. Pomerance, *The probability that a random probable prime is composite*, Math. Comp. 53 (1989), no. 188, 721–741.
- [81] V. Klee e S. Wagon, *Old and new unsolved problems in plane geometry and number theory*, The Dolciani Mathematical Expositions 11, MAA (1991).
- [82] A. W. Knap, *Elliptic Curves* (Mathematical Notes, 40), Princeton University Press (1992).
- [83] D. E. Knuth, *The Art of computer Programming*, vol. 2 (Seminumerical Algorithms), Addison Wesley (1998).
- [84] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner (1909). Reprinted: Chelsea (1953).
- [85] L. Larson, *Problem-solving through problems*, Springer-Verlag (1990).
- [86] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. 31 (1930), 419–448. Reimpresso em *Selected Papers*, (ed. D. McCarthy), vol 1, Ch. Babbage Res. Center, St. Pierre, Manitoba, Canada, 11–48 (1981).
- [87] F. Lemmermeyer, *The Euclidean Algorithm in Algebraic Number Fields*, Exposition. Math. 13, no.5, 385–416 (1995).
- [88] H. W. Lenstra Jr., *Primality testing with cyclotomic rings*, não publicado (2002).

- [89] H. W. Lenstra Jr. e C. Pomerance, *Primality testing with Gaussian periods*, manuscrito, exposto em XXIII Journées Arithmétiques Graz (2003), 6–12 julho (2003); preprint disponível em <http://www.math.dartmouth.edu/~carlp/aks102309.pdf>.
- [90] Y. Lequain, *Aproximação de um número real por números racionais*, 19º Colóquio Brasileiro de Matemática (1993).
- [91] E. L. Lima, Curso de Análise, vol. 1, Projeto Euclides.
- [92] Q. Liu, *Algebraic Geometry and Arithmetic Curves* (Oxford Graduate Texts in Mathematics).
- [93] D. Lorenzini, *An Invitation to Arithmetic Geometry* (Graduate Studies in Mathematics, Vol 7) AMS (1996).
- [94] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 184–240 e 289–321.
- [95] H. Maier, *Primes in short intervals*, Michigan Math. J. 32 (1985), 221–225.
- [96] A. Markov, *A new sequence of minima in the geometry of numbers*, Math. Ann. 15 (1879), 381–406.
- [97] A. Markov, *Sur les formes quadratiques binaires indéfinies*, Math. Ann. 15 (1879), 381–406.
- [98] A. I. Markushévich, *Sucesiones recurrentes*, Editorial MIR, Moscou 1974.
- [99] Martín-López E., Laing A., Lawson T., Alvarez R., *Experimental realization of Shor's quantum factoring algorithm using qubit recycling*, Nature Photonics 6, (2012) 773–776
- [100] W. de Melo e B. F. Svaiter, *The cost of computing integers*, Proc. AMS 124 (1996), no. 5, 1377–1378.
- [101] G. L. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. Sys. Sci. 13 (1976), 300–317.
- [102] W. H. Mills, *A prime representing function*, Bull. Amer. Math. Soc., 53 (1947), 604.

- [103] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series 33, Princeton University Press (1980).
- [104] R. A. Mollin, *Prime-producing polynomials*, Amer. Math. Monthly 104 (1997), 529–544.
- [105] C. G. Moreira e N. C. Saldanha, *Primos de Mersenne (e outros primos muito grandes)*, texto para o 22o Colóquio Brasileiro de Matemática, IMPA, 1999.
- [106] C. G. Moreira, *O teorema de Ramsey*, Revista Eureka! 6, 23–29.
- [107] C. G. Moreira, *On asymptotic estimates for arithmetic cost function*, Proc. AMS 125 (1997), 347–353.
- [108] C. G. Moreira, *Geometric properties of the Markov and Lagrange spectra*. Preprint-IMPA-2009.
- [109] Y. Motohashi, *An overview of the sieve method and its history*, Sugaku Expositions 21, 1–32 (2008). Também em <http://arxiv.org/abs/math/0505521>.
- [110] D. Mumford (com contribuições de E. Arbarello), *The Red Book of Varieties and Schemes*, Springer.
- [111] T. Nagell, *On a special class of Diophantine equation of the second degree*, Ark. Mat. 3 (1954), 51–65.
- [112] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften 322, Springer-Verlag (1999).
- [113] I. Niven e M. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley and Sons (1991).
- [114] Paris e Harrington, *An incompleteness in PA* in Barwise, *Handbook of Mathematical Logic*, North Holland.
- [115] J. Pintz, *Very large gaps between consecutive primes*, J. Number Theory 63 (1997), no. 2, 286–301.
- [116] A. Politi, J. C. F. Matthews, J. L. O’Brien, *Shor’s Quantum Factoring Algorithm on a Photonic Chip*, Science 4 September 2009: Vol. 325. no. 5945, p. 1221.

- [117] D. H. J. Polymath, *Deterministic methods to find primes*, preprint, <http://polymathprojects.files.wordpress.com/2010/07/polymath.pdf>; veja também <http://polymathprojects.org/2009/08/09/research-thread-ii-deterministic-way-to-find-primes/> e http://michaelnielsen.org/polymath1/index.php?title=Finding_primes
- [118] C. Pomerance, *A new lower bound for the pseudoprimes counting function*, Illinois J. Math, 26, 1982, 4–9.
- [119] C. Pomerance, *Primality testing: variations on a theme of Lucas*, disponível eletronicamente em <http://cm.bell-labs.com/cm/ms/who/carlp/PS/primalitytalk5.ps>
- [120] C. Pomerance, J. L. Selfridge e S. S. Wagstaff Jr., *The pseudoprimes to 25.109*, Math. Comp. 35 (1980), 1003–1026.
- [121] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory 12 (1980), 128–138.
- [122] H. Rademacher, *On the partition function $p(n)$* , Proc. London Math. Soc. (2) 43 (1937), 241–254.
- [123] H. Rademacher, *Topics in analytic number theory*, Grundlehren der mathematischen Wissenschaften 169, Springer-Verlag (1973).
- [124] P. Ribenboim, *The New Book of Prime Number Records*, terceira edição, Springer-Verlag (1995).
- [125] P. Ribenboim, *Selling primes*, Math. Mag. 68 (1995), 175–182. Traduzido como *Vendendo primos*, Rev. Mat. Univ. 22/23 (1997), 1–13.
- [126] H. Riesel, *Naagra stora primtal* (sueco: *Alguns primos grandes*), Elementa 39 (1956), 258–260.
- [127] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Progress in Mathematics, Birkhauser Boston, vol. 57 (1985) e vol. 126 (1994).
- [128] W. M. Schmidt, *Diophantine approximation*, Lecture Notes in Mathematics 785, Springer-Verlag (1980).

- [129] A. Selberg, *An elementary proof of the prime number theorem*, Ann. of Math. 50 (1949), 305–13.
- [130] J. P. Serre, *Cours d'arithmétique*, Presses Universitaires de France (1970).
- [131] J-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag.
- [132] J.P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) 40 (2003), no. 4, 429–440.
- [133] S. S. Shatz, *Profinite groups, Arithmetic, and Geometry*, Annals of Mathematical Studies 67, Princeton University Press.
- [134] A. Shen e N. K. Vereshchagin, *Basic Set Theory*, AMS, 2002.
- [135] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. 26 (5), 1484-1509 (1997). Também em [arXiv:quant-ph/9508027v2](#).
- [136] M. Shub e S. Smale, *On the intractability of Hilbert's Nullstellensatz and algebraic version of “ $NP = P$ ”*, Duke Math J. 81 (1995), 47–54.
- [137] W. Sierpinski, *Sur un problème concernant les nombres $k \cdot 2n + 1$* , Elem. Math. 15 (1960) 73–74. Corrigendum: Elem. Math. 17 (1963), 85.
- [138] W. Sierpinski, *Elementary theory of numbers*, P. W. N. Poland (1964).
- [139] W. Sierpinski, *250 Problems in Elementary Number Theory*, Elsevier (1970).
- [140] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag (1995).
- [141] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics 106, Springer (2009).
- [142] J. H. Silverman e M. Hindry, *Diophantine Geometry: An Introduction* (Graduate Texts in Mathematics), Springer-Verlag.

- [143] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag (1994).
- [144] R. Solovay e V. Strassen, *A fast Monte-Carlo test for primality*, SIAM Journal on Computing 6 (1977), 84–86.
- [145] E. M. Stein, e R. Shakarchi, *Fourier analysis, an introduction*, Princeton University Press (2003).
- [146] R. Taylor e A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 (1995), no. 3, 553–572.
- [147] H. F. Trotter, *On the norms of units in quadratic fields*, Proc. Amer Math. Soc. 22 (1969), 198–201.
- [148] S. Vajda, *Fibonacci and Lucas Number and the golden section*, John Willey & Sons (1989).
- [149] A. I. Vinogradov *On the remainder in Merten's formula* (Russian), Dokl. Akad. Nauk SSSR 148 (1963), 262–263.
- [150] E. Westzynthius, *Über die Verteilung der Zahlen die zu den n ersten Primzahlen teilerfremd sind*, Comm. Phys. math. Helsingfors 5 (1931), no. 5, 1–37.
- [151] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443–551.
- [152] H. Wilf, *What is an answer?*, Am. Math. Monthly 89 (1982), 289–292.
- [153] H. C. Williams e H. Dubner, *The primality of $R1031$* , Math. Comp., 47 (1986), 703–711.
- [154] J. Young e A. Potler, *First occurrence of primes gaps*, Math. Comp. 52 (1989), 221–224.
- [155] Y. Zhang, *Bounded gaps between primes*, aceito para publicação no Ann. of Math.. Mais informações disponíveis em <http://annals.math.princeton.edu/articles/7954>.

Índice Remissivo

- algoritmo
 - da divisão para polinômios, 59
 - complexidade, 372
 - das divisões sucessivas, 19
 - de Euclides, 19, 24, 111, 261
 - de Fürer, 371
 - de Karatsuba, 363
 - de Miller-Rabin, 335
 - de Shor, 55
 - determinístico polinomial, 54
 - probabilístico, 335
 - usando FFT, 364
- anel, 47, 167
 - integralmente fechado, 280
 - comutativo, 47
 - de inteiros algébricos, 279
 - de inteiros ciclotômicos, 257
 - dos inteiros módulo n , 41
 - noetheriano, 289
- base integral, 280
- bases, 38
- binômio de Newton, 9, 48
- caráteres, 439
- coeficiente binomial, 6, 9, 45
- coeficiente multinomial, 9
- congruência, 34
 - em $\mathbb{Z}[\sqrt{d}]$, 254
 - módulo um ideal, 286
- de grau dois, 87
- de grau superior, 100
- em $\mathbb{Z}[i]$, 241
- conjectura
 - de Goldbach, 321
 - de Artin, 76
 - de Catalan, 171
 - de Euler, 148, 155
 - de Hardy-Littlewood, 312
 - de Taniyama, Shimura e Weil, 160
 - sobre números perfeitos, 353
 - sobre primos, 319
- conjuntos
 - de Cantor, 128
 - mensuráveis, 153
- constante
 - de Artin, 76
 - de Euler-Mascheroni, 206, 210, 223, 322
 - de Mertens, 210
- corpo, 47, 167
- criptografia RSA, 53, 329
- critério
 - de divisibilidade, 39
 - de Eisenstein, 66, 68
 - de Euler, 88
 - de primalidade $n - 1$, 357
 - de primalidade de Morrison, 360

curvas elípticas, 164, 402

descenso infinito de Fermat, 155

desigualdade das médias aritmética e geométrica, 10

discriminante, 281, 415

divisão euclidiana, 18

de polinômios, 59

em inteiros de Eisenstein, 252

em $\mathbb{Z}[i]$, 244

domínio, 47, 286

euclidiano, 253

de Dedekind, 292

de ideais principais, 285, 300

não euclideano, 302

elemento

algébrico, 265

integral, 275

equação

de Markov, 128, 158

de Pell, 166

de Pell-Dirichlet, 177

de Ramanujan-Nagell, 262

diofantina, 133

diofantina linear, 80

módulo m , 80

espaço projetivo, 402

espectro

de Lagrange, 127

de Markov, 128

extensão

de anéis, 276

finita, 276

simples, 267

fórmula

de Moivre, 273

fatoração única

de polinômios, 64

em \mathbb{Z} , 26

em ideais primos, 293

em inteiros de Eisenstein, 251

em inteiros de Gauß, 247

fatoração canônica, 27

de n fatorial, 30

fórmula

de Euler, 426

de inversão de Möbius, 194, 195

para primos, 324

fração contínua

de π , 109, 118

de \sqrt{A} , 173

de e , 118, 130

frações contínuas

aproximações, 119, 382

periódicas, 118, 125

função

λ de Carmichael, 78

ζ de Riemann, 212, 422

Λ de von Magoldt, 428

$[x]$ teto, 18

$[x]$ piso, 18

μ de Möbius, 193

ω número de divisores primos, 219

Ω número de divisores primos com multiplicidade, 219

π de quantidade de números primos, 201, 308, 420

ψ de Tchebyshev, 428

σ soma dos divisores, 189, 217

- σ_k soma das k -ésimas potências dos divisores, 30, 189
- τ custo aritmético, 231
- φ de Euler, 49, 212
- \wp de Weierstraß, 412
- d número de divisores, 30, 189, 221
- p número de partições, 225
- duplamente periódica, 409
- geratriz de $p(n)$, 227
- Li logaritmo integral, 309
- monótona, 189
- multiplicativa, 188
- totalmente multiplicativa, 188
- funções aritméticas
 - estimativas, 188
- grau
 - de extensão de corpos, 264
 - de polinômio, 59
- grupo, 46
 - abeliano, 47
 - cíclico, 75
 - de caracteres, 437, 439
 - de classe, 298
 - de unidades, 43, 245
- hipótese de Riemann, 77, 196, 310
- ideal, 284
 - primo, 286
 - fracionário, 293
 - maximal, 286
 - principal, 285
- identidade de Euler, 145
- identidades de Newton, 274
- imersão, 269
- inteiro
 - algébrico, 275
 - de Eisenstein, 251
 - de Gauß, 240
- inverso multiplicativo, 43
- irredutível
 - elemento, 245
 - associado, 245
 - em inteiros de Eisenstein, 252
 - em inteiros de Gauß, 249
 - polinômio, 63
- L -séries de Dirichlet, 442
- lema
 - de Gauß, 65, 92
 - de Hensel, 101
 - de Landau, 447, 448
 - de Thue, 143, 155
- máximo divisor comum, 18, 21
 - de polinômios, 62
- método
 - de Newton, 346, 373
 - do crivo, 314
 - geométrico, 136
- mínimo múltiplo comum, 18, 24
 - de polinômios, 63
- número
 - algébrico, 265
 - composto, 22
 - primo, 22
 - de Brier, 323
 - de Liouville, 399
 - de Riesel, 323
 - de Sierpinski, 323
 - livre de quadrados, 83, 219
- números

- amigos, 197
- de Fermat, 99
- primos entre si, 18, 213
- de Carmichael, 331
- norma, 167, 240, 251, 271
 - de um ideal, 295
- ordem
 - de e , 124, 400
 - de um número algébrico, 400
 - de um número real, 123, 130
 - de uma sequência recorrente, 451
 - lexicográfico, 264
 - módulo um número, 68
 - normal de uma função, 221
 - parcial, 7
 - total, 8, 263
- polinômio, 58
 - irredutível, 63
 - simétrico elementar, 263
 - característico, 293
 - ciclotômico, 320
 - mônico, 59
 - minimal, 265
 - primitivo, 65
 - simétrico, 263
- polinômios
 - homogêneos, 403
- ponto racional, 142
- postulado de Bertrand, 204
- primos, 22, 308
 - distribuição dos, 308
 - conjectura de Goldbach, 321
 - conjecturas, 319
 - de Wieferich, 160
 - de Fermat generalizado, 339
 - de Mersenne, 350
 - de Sophie Germain, 311
 - estimativas, 200
 - fatoriais, 376
 - gêmeos, 311
 - ideais, 286
 - infinitude, 27, 203
 - primoriais, 375
- princípio
 - da boa ordenação, 7
 - da casa dos pombos, 10
 - da indução finita, 3
 - das gavetas de Dirichlet, 10
- problema
 - décimo de Hilbert, 133
 - de Waring, 147
 - dos divisores de Dirichlet, 224
- pseudoprímo, 330
 - de Perrin, 279
 - forte, 332
- raiz primitiva, 68
- reciprocidade quadrática, 90, 257
- relação
 - de divisibilidade, 15
 - de equivalência, 41
 - de ordem, 7
- resíduo quadrático, 87
- reticulado, 152, 408
- sequência
 - de Farey, 32
 - de Lucas, 356
 - de Perrin, 278
 - recorrente, 355, 451
 - linear, 457

- de Fibonacci, 5, 8, 32, 157, 256, 262, 278, 454
- símbolo
 - de Jacobi, 94
 - de Legendre, 88
- sistema completo de restos, 48
- sistema completo de invertíveis, 48
- soma
 - de dois quadrados, 153
 - de Gauß, 258
 - dos inversos dos primos, 209
 - dos inversos dos quadrados, 210
 - harmônica, 32, 207
- somas
 - de dois quadrados, 142
 - de quatro quadrados, 147, 154
 - de três cubos, 165
 - de três quadrados, 149
- teorema
 - dos três quadrados, 149
 - chinês dos restos, 81, 86, 250, 306
 - da base integral, 282
 - das unidades de Dirichlet, 305
 - de Goldston, Pintz e Yıldırım, 322
 - de Bachet-Bézout, 20, 63, 246, 268
 - de Brun, 311
 - de Chebyshev, 200, 204
 - de Chevalley-Warning, 103
 - de Dirichlet, 115, 126, 319, 421
 - de Erdős, Ginzburg e Ziv, 104
 - de Euler-Fermat, 50
 - para inteiros de Gauß, 250
 - de Green Tao, 322
 - de Hurwitz-Markov, 119
 - de Ikehara-Wiener, 435
 - de Khintchine, 390
 - de Ko Chao, 171
 - de Kronecker, 303, 385
 - de Lagrange, 51, 78, 343
 - de Legendre, 138, 150
 - de Lucas-Lehmer, 353, 361
 - de Lucas-Lehmer-Riesel, 362
 - de Mills, 326
 - de Minkowski, 152
 - de Mordell-Weil, 408
 - de Nagell-Trotter, 178
 - de Pólya-Vinogradov, 260
 - de Proth, 339
 - de Ramsey, 13
 - de Roth, 400
 - de Sophie Germain, 311
 - de uniformização, 416
 - de Weyl, 387
 - de Wilson, 44, 61, 330
 - de Wolstenholme, 44
 - do elemento primitivo, 269
 - dos números primos, 309, 421, 437
 - fundamental da aritmética, 26
 - pequeno de Fermat, 50
 - Schinzel, 217
 - Sierpiński, 216
 - Tauberianos, 431
 - último de Fermat, 160, 311, 402

ternas pitagóricas, 134
teste de primalidade, 329
 AKS, 340
 baseados em $n - 1$, 337
 de Miller-Rabin, 335
 Lucas-Lehmer, 353
 Pépin, 339
 Pocklington, 338
traço, 271
transformação de Gauss, 111
transformada
 de Fourier discreta, 366
 de Laplace, 435
 de Mellin, 435
triplas pitagóricas, 134
truque do determinante, 277,
 280