Teoria Aritmética dos Números

Jair Donadelli

3 de dezembro de 2017

Sumário

O que é?

Teoria dos Números é uma disciplina da matemática dedicada principalmente ao estudo das propriedades dos números inteiros, em geral, e dos números primos, em particular, bem como as propriedades dos objetos obtidos a partir dos números inteiros (e.g., números racionais) ou de generalizações dos números inteiros (e.g., inteiros algébricos). Propriedades de números reais e números complexos são estudados em *Análise Real* e *Análise Complexa*.

Aritmética é como é chamada a parte elementar da Teoria dos Números, cujos temas são estudados sem se recorrer a métodos analíticos, algébricos ou geométricos. São estudados questões de divisibilidade, o algoritmo de Euclides para calcular o maior divisor comum, a fatoração de inteiros em números primos, os números perfeitos e congruências. Resultados importantes típicos são o teorema de Wilson, o pequeno teorema de Fermat, o teorema de Euler , o teorema chinês do resto e a lei da reciprocidade quadrática. Também, costumam aparecer sob essa designação as propriedades de funções multiplicativos como a função de Moebius e de função de Euler.

A primeira descoberta histórica de natureza aritmética foi a Tábula de Plimpton 322, 1800 aC. O início do estudo sistemático tem como principal marco *Os Elementos* de Euclides (300 aC) e o nascimento da Teoria dos Números moderna tem como principal marco inicial *Disquisitiones Arithmeticae* de Gauss (1801). Durante o período entre esses dois marcos há contribuições importantes devidas a Fermat e Euler, principlamente. Com o tempo *Aritmética* também adquiriu outros significados como em *Aritmética de Peano* e *Aritmética de ponto flutuante*. O uso do termo *Aritmética* para designar o mesmo que *Teoria dos Números* recuperou algum terreno na segunda metade do século 20, em parte devido à influência francesa[1].

Pra que serve?

Os números estão na base da civilização, faz parte da cultura dos povos e, segundo historiadores, já se contava na Idade da Pedra.

Números estão na base da construção do conhecimento matemático, em particular, o conjunto dos números naturais, em alguns aspectos, é a peça mais básica da matemática pois você pode construir os demais conjuntos numéricos a partir de números naturais

$$\mathbb{N} \xrightarrow{-} \mathbb{Z} \xrightarrow{\div} \mathbb{Q} \xrightarrow{\epsilon} \mathbb{R} \xrightarrow{i} \mathbb{C}$$

daí você pode chegar ao cálculo, à topologia e outras disciplinas da Matemática. Por outro lado, a Teoria dos Números utiliza técnicas dessas disciplinas (álgebra, análise, geometria e topologia, lógica e a

[1] Serre, Jean-Pierre. Cours d'arithmétique. Presses Universitaires de France - PUF - ISBN: 9782130418351

ciência da computação) para resolver as questões que lhes são próprias, e muitas vezes direciona desenvolvimentos nestes campos.

Teoria dos Números é um ótimo lugar para aprender a ler e escrever provas. É uma rica fonte de conjecturas que são fáceis de enunciar e muito difíceis de provar. É uma área que lida com problemas de entendimento simples, são acessíveis pois envolvem elementos que são familiares, embora as soluções nem sempre são simples, exigem engenhosidade, em muitos casos, são muito difíceis, embora os números inteiros sejam familiares e suas propriedades parecerem simples, é sim um assunto muito profundo.

Por exemplo, aqui estão alguns problemas que permanecem sem solução (um número primo é um número inteiro maior que 1, cujos divisores positivos são 1 e o próprio número). Note-se que estes problemas são simples de enunciar

- (conjectura de Goldbach) Todo inteiro $n > 2$ par é soma de dois primos?
- (conjectura dos primos gêmeos) Há um número infinito de primos gêmeos? (primos gêmeos diferem por 2, como 11 e 13)
- A sequência de números de Fibonacci tem infinitos números primos?
- Existem infinito primos de Mersenne (da forma $2^p + 1$, com p primo)?
- $n^2 - n + 41$ é primo para n de 1 até 40, há infinitos primos dessa forma?
- Há um primo entre n^2 e $(n+1)^2$?
- Há uma quantidade infinita de números perfeitos? (perfeito se é a soma de seus divisores, $6 = 3 + 2 + 1$ por exemplo)
- Existe um número ímpar perfeito?
- Existe um algoritmo eficiente para fatorar inteiros?
- (Conjectura de Collatz — conjectura $3n + 1$) Comece com qualquer inteiro n. Obtenha um novo número inteiro m dividindo na metade n, se for par, ou tomando $3n + 1$, se for ímpar. Repita, se m é par, tome a metade, senão tome $3m + 1$. E assim por diante. É verdade que este procedimento iterativo sempre resuta em 1, independente do valor inicial?
- (Problema de Catalan Os números 8 e 9 são as únicas duas potências consecutivas? Ou seja, as únicas soluções nos naturais para $x^a - y^b = 1$, $x, y, a, b > 1$, são $x = 3$, $a = 2$, $y = 2$ e $b = 3$?

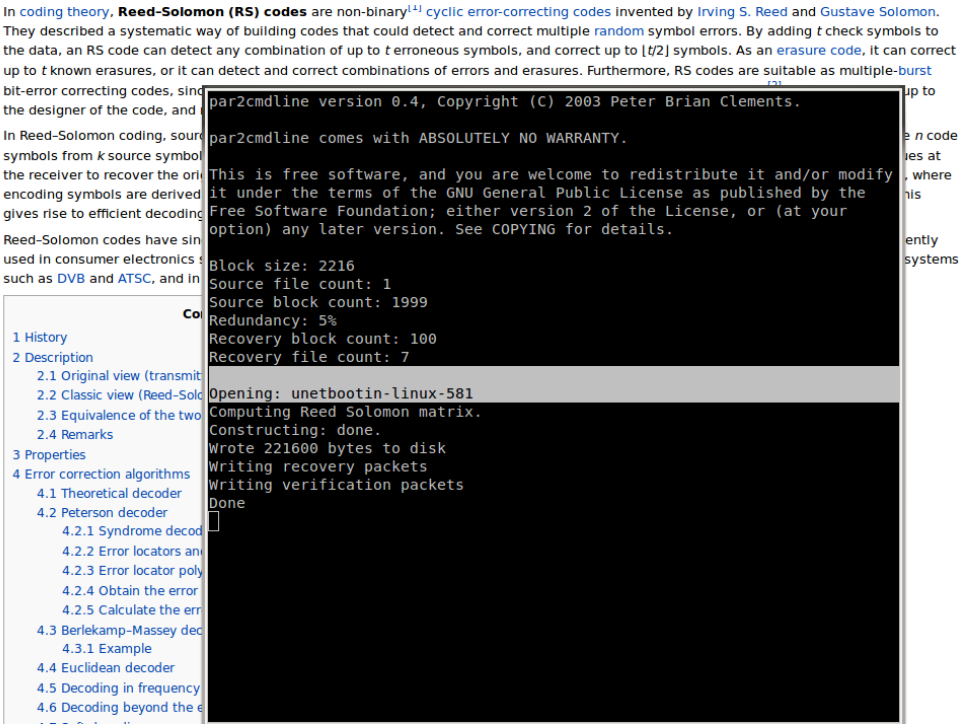
- (Conjectura dos números palíndromos) Escolha um inteiro. Inverta seus dígitos e adicione ao resultado o inteiro original. Se o resultado não é um palíndromo, repita o processo. Será que todos os números inteiros, eventualmente, tornam-se palíndromos por este processo?

- Existem inifinitos primos com todos os dígitos iguais a 1?

- (Hipótese de Riemann) Essa não dá pra descrever de modo simples!!! Mas pra motivar, se você resolver o problema, ganha US$1.000.000,00.

A Teoria dos Números é considerada uma disciplina desafiadora e instigante, ademais, tem algumas grandes aplicações: a criptografia de chave pública (RSA é o mais famoso), a construção de grafos expansores, a Teoria de Códigos, etc. Todo sistema digital está baseado nos números inteiros. Duas aplicações modernas são: códigos corretores de erros e criptografia de chave pública.

Códigos corretores de erros: fazem parte do nosso cotidiano de várias formas, e.g., ao falar pelo telefone, ao ouvir um CD de música, ao assistir um filme em DVD ou navegar pela Internet. Códigos corretores de erros são usados frequentemente em aplicações militares para proteção contra interferência inimiga intencional. Quando queremos transmitir uma informação através de um canal de comunicação (linha telefônica, DVD, internet) podem ocorrer ruídos, o que acaba provocando erros na informação inicial. Detectar tais erros e, se possível, corrigi-los é o objetivo dos códigos corretores de erros. A Álgebra, a Combinatória e a Teoria de Números são ferramentas fundamentais no estudo da Teoria de Códigos.



Criptografia RSA:

1. Escolha dois números primos p e q, por exemplo, $\boxed{p = 3 \text{ e } q = 11}$
2. Compute $n = p * q$, no exemplo $\boxed{n = 33}$
3. Compute $\phi(n) = (p-1) * (q-1)$, $\boxed{\phi(33) = 20}$
4. Escolha $e \in \{2, 3, \ldots \phi(n)\}$ com e e n coprimos, $\boxed{e = 7}$
5. Compute d tal que $(d * e) \div \phi(n)$ deixa resto 1, $\boxed{d = 3}$
6. **Chave pública** (e, n), $\boxed{(7, 33)}$
7. **Chave privada** (d, n), $\boxed{(3, 33)}$

Para criptografar convertemos a mensagem num inteiro m e calculamos $c = m^e \pmod{n}$, $\boxed{m = 2,\ c = 29}$.
Para decodificar, calculamos $c^d \pmod{n}$, $\boxed{m = 29^3 \pmod{33} = 2}$.

A conversão pra inteiro não é problema, informação é normavelmente codificada em computador usando um sistema de numeração:

String: teoria aritmética dos números

ASCII (decimal): 116 101 111 114 105 97 32 97 114 105 116 109 101 116 105 99 97 32 100 111 115 32 110 117 109 101 114 111 115

Binário: 01110100 01100101 01101111 01110010 01101001 01100001 00100000 01100001 01110010 01101001
01110100 01101101 01100101 01110100 01101001 01100011 01100001 00100000 01100100 01101111 01110011
00100000 01101110 01110101 01101101 01100101 01110010 01101111 01110011
Hexadecimal: 74 65 6F 72 69 61 20 61 72 69 74 6D 65 74 69 63 61 20 64 6F 73 20 6E 75 6D 65 72 6F 73
Texto comum: teoria aritmética dos números
Texto criptografado (representado em hex): c40bd12d61340e76830f00de6e590e
98f58cacf59b314d791824c280943770d4984caca3543496c543459d0051a299f57ce6
03aeff7745572ec659159ab0613e0a9ed6d5accb2f7588c60b7aaf13b05df9f4a51735b
0ca71d52922a94e9dff1f271285c3defad9fb5605f9e4c9e58c26898e40f47c078f328b7
3814ed6c6555b

> "I was interviewed in the Israeli Radio for five minutes and I said that more than 2000 years ago, Euclid proved that there are infinitely many primes. Immediately the host interrupted me and asked: 'Are there still infinitely many primes?"' Noga Alon

0 Preliminares: partição e relação de equivalência

0.1 Partição

Uma família (finita) de conjuntos $\mathscr{A} = \{A_1, A_2, \ldots, A_n\}$ **particiona** o conjunto X se seus elementos são não-vazio, disjuntos e a união deles é X, isto é,

$$A_i \neq \emptyset \text{ para todo } i \tag{1}$$

$$A_i \cap A_j = \emptyset \text{ para todo } i \neq j, \quad \text{e} \tag{2}$$

$$A_1 \cup A_2 \cup \cdots \cup A_n = X. \tag{3}$$

Dizemos que $\mathscr{A}$ é uma **partição** X. Notemos que $A_i \subset X$ para todo i. A definição é a mesma no caso em que $\mathscr{A}$ não é finito.

Exemplo 1. *Sejam R_0, R_1 e R_2 subconjuntos de $\mathbb{N}$ definidos por*

$$R_i = \{n : \ n \textit{ dividido por } 3 \textit{ deixa resto } i\}$$

$\{R_0, R_1, R_2\}$ *é uma partição de* $\mathbb{N}$.

0.2 Relação de equivalência

Uma **relação binária** R sobre um conjunto A é um conjunto de pares ordenados de elementos de A, em outras palavras, é um subconjunto $R \subset A \times A$.
Notação: Escrevemos aRb com o significado de $(a, b) \in R$.

Exemplo. $<\subset \mathbb{N}\times\mathbb{N}$ *é uma relação binária e* $(2,3)\in <$, *mas usamos escrever* $2<3$.

Uma relação binária $\sim$ sobre um conjunto A é de **equivalência** se valem as propriedades

reflexiva $a\sim a$ para todo $a\in A$;

simétrica se $a\sim b$, então $b\sim a$ para todos $a,b\in A$;

transitiva se $a\sim b$ e $b\sim c$, então $a\sim c$ para todos $a,b,c\in A$;

Exemplo.

1. $=$ *é uma relação de equivalência em* $\mathbb{N}$.
2. $\leq$ *não é uma relação de equivalência em* $\mathbb{N}$.
3. *Se T e S são triângulos no plano e $T\cong S$ se os triângulos são semelhantes, então $\cong$ é relação de equivalência sobre o conjunto de todos os triângulos no plano.*
4. *Semelhança de matriz é uma relação de equivalência sobre o conjuntos de todas as matrizes quadradas de ordem n de números reais.*
5. $\subset$ *não é relação de equivalência sobre o conjunto das partes de A.*

Exemplo. *Seja* $\{R_0,R_1,R_2\}$ *a partição de* $\mathbb{N}$ *dada no exemplo 1. Definimos* $\sim$ *sobre* $\mathbb{N}$ *por*

$$a\sim b \text{ se existe } i\in\{0,1,2\} \text{ tal que } a,b\in R_i$$

ou seja, a e b pertencem a um mesmo conjunto da partição.

Exercício 2. *Se $\mathscr{A}$ é uma partição de X então a relação definida por*

$$a\sim b \text{ se, e só se, } a\in A \text{ e } b\in A, \text{ para algum } A\in\mathscr{A}$$

é uma relação de equivalência.

Solução. Sejam $\mathscr{A}$, X e $\sim$ como no enunciado e vamos provar que $\sim$ é uma relação binária reflexiva, simétrica e transitiva.

Para todo $a\in X$, $a\in A$ para algum $A\in\mathscr{A}\,S$ pois $\mathscr{A}$ é partição; da definição temos $a\sim a$, logo a relação $\sim$ é reflexiva.

Se $a\sim b$ então $a\in A$ e $b\in A$, para algum $A\in\mathscr{A}$, mas também, $b\sim a$. Logo a relação $\sim$ é simétrica.

Finalmente, se $a\sim b$ então $a\in A$ e $b\in A$, para algum $A\in\mathscr{A}$, e se $b\sim c$ então $b\in B$ e $c\in B$, para algum $B\in\mathscr{A}$. Portanto $b\in A\cap B$.

Como $\mathscr{A}$ é partição $A\cap B=\emptyset$ ou $A=B$. Vale a segunda opção. De $a,c\in A$ temos $a\sim c$. Logo a relação $\sim$ é transitiva. □

Classe de equivalência

Seja $\sim$ uma relação de equivalência sobre o conjunto X e $a \in X$

$$[a] := \{b \in X : b \sim a\}$$

é o subconjunto de X formado por todos os elementos equivalentes a a, chamado de **classe de equivalência** de a. O elemento dentro dos colchetes é chamado de **representante** da classe.

Por transitividade, qualquer elemento da classe pode ser seu representante. Seja $b \in X$ com $b \sim a$. Para todo $c \in [a]$ vale $c \sim a$, portanto, $c \sim b$, logo $c \in [b]$. Reciprocamente, se $c \in [b]$ então $c \in [a]$, por argumento análogo. Assim $[a] = [b]$. Também, se $[a] = [b]$ então de $a \in [a]$ temos $a \in [b]$, portanto $a \sim b$. Com isso provamos

$$a \sim b \Leftrightarrow [a] = [b]. \tag{4}$$

O que podemos dizer no caso $[a] \neq [b]$? Imediatamente, por (4) que $a \not\sim b$. Para qualquer $c \in X$, se $c \sim a$ então $b \not\sim c$, caso contrário teríamos uma contradição pela transitividade, de modo que $[a] \cap [b] = \emptyset$.

Concluindo, dos parágrafos precedentes temos que para as classes de equivalência vale um dos casos: para quaisquer $a, b \in X$

1. $[a] = [b]$, ou
2. $[a] \cap [b] = \emptyset$.

O **conjunto quociente** de X pela relação de equivalência $\sim$ é o conjunto das classes de equivalência da relação

$$X/\sim := \{[a] : a \in X\}. \tag{5}$$

Exercício 3. *Prove que $X/\sim$ é uma partição de X.*

Exemplo. *No caso de exemplo 1*

$$R_0 = [0] = \{0, 3, 6, 9, 12, 15, \ldots\}$$

$$R_1 = [1] = \{1, 4, 7, 10, 13, 16, \ldots\}$$

$$R_2 = [1] = \{2, 5, 8, 11, 14, 17, \ldots\}$$

Observemos que $[0] = [3] = [6]$. *O Teorema da Divisão (que veremos com detalhe nesse curso) garante que* $R_0 \cup R_1 \cup R_2 = \mathbb{N}$.

Exercício 4. *Considere a relação* $\mathbf{Z} \subset \mathbb{N} \times \mathbb{N}$ *definida por*

$$(a, b)\mathbf{Z}(n, m) \text{ se, e só se } a + m = b + n \tag{6}$$

Para cada (a,b) definimos a classe de equivalência de (a,b) por

$$[(a,b)] := \{(n,m) \in \mathbb{N} \times \mathbb{N} \colon (a,b)\mathbf{Z}(n,m)\}. \tag{7}$$

Por exemplo, $[(1,2)] = \{(0,1),(1,2),(2,3),(3,4),\ldots\}$ *e* $[(5,2)] = \{(3,0),(4,1),(5,2),(6,3),\ldots\}$. *Também definimos uma soma de classes de equivalência por*

$$[(a,b)] + [(n,m)] := [(a+n, b+m)]. \tag{8}$$

1. *Prove que* $\mathbf{Z}$ *é uma relação de equivalência.*

2. *Verifique que* $[(1,2)] + [(5,2)] = [(0,1)] + [(3,0)]$.

3. *Generalizando o item anterior prove que a soma de conjuntos definida acima é compatível com a relação de equivalência, isto é, a soma não depende dos representantes de cada classe de equivalência envolvida.*

Definimos um produto de classes de equivalência por

$$[(a,b)] \cdot [(n,m)] := [(an+bm, am+bn)]. \tag{9}$$

Prove que tal operação é compatível com a relação de equivalência, isto é, ela não depende dos representantes de cada classe de equivalência envolvida.

Observação 5. *Os exercícios 2 e 3 nos dizem que partição e relação de equivalência são definições equivalentes.*

Exercícios

1. Verifique se são relações de equivalência:

   (a) Em $\mathbb{R}$, $x \sim y$ se $x - y \in \mathbb{Q}$.

   (b) Em $\mathbb{R}$, $x \sim y$ se $x \leq y$.

   (c) Em $\mathbb{R}$, $x \sim y$ se $|x - y| \leq 1$.

   (d) Em X não vazio, $x \sim y$ para todo $x, y \in X$.

   (e) Em $\mathbb{R}^2$, $P \sim Q$ se a reta $\overline{PQ}$ passa pela origem.

   (f) Em $[-1,1]$, $x \sim y$ se $\sin^2(x) + \cos^2(y) = 1$.

2. Suponha que $\sim$ é uma relação simétrica e transitiva sobre o conjunto X. Se $a \sim b$, então $b \sim a$ por simetria e, então, $a \sim a$ por transitividade, assim a propriedade reflexiva é dispensável na definição de relação de equivalência, pois é consequência das outras duas. O que está errado?

Este primeiro contato com a Teoria dos Números é por meio da Teoria Elementar dos Números. Através desta disciplina introduziremos propriedades interessantes e notáveis dos números inteiros.

Começamos este texto com uma apresentação axiomática dos números naturais seguido do estudo de suas propriedades. Mais adiante construímos o conjunto dos inteiros e partimos para seu estudo e de suas propriedades.

1 Números Naturais e Indução Matemática

Os axiomas de Peano apareceram na publicação de 1889 *Arithmetic principia: novo methodo exposita* — *Novo método de exposição dos princípios da Aritmética*. Esses axiomas formalizavam a ideia de que todos os números naturais podem ser obtidos a partir do número 1 pela soma sucessiva da unidade. O grande mérito de Guiseppe Peano (1858-1932) foi a constatação de que *a partir de quatro axiomas pode-se conceituar ou deduzir todas as definições e propriedades dos números naturais*, como por exemplo: adição, multiplicação e relação de ordem. Na realidade, os axiomas conhecidos como *Axiomas de Peano* foram enunciados pela primeira vez por Dedekind um ano antes, em 1888. Dedekind usou de modo informal a teoria dos conjuntos, Peano, trabalhando de modo independente, não construiu sua teoria dentro da teoria dos conjuntos. Apresentamos a seguir uma breve exposição dos axiomas de Peano.

Axiomas de Peano. Vamos começar um estudo aritmético do conjunto $\mathbb{N}$ dos números naturais com uma abordagem formal a partir da construção lógica de $\mathbb{N}$. Consideremos conceitos elementares de teoria dos conjuntos e três conceitos primitivos: número natural, zero[2] e sucessor. O conjunto dos números naturais é caracterizado pelas seguintes propriedades:

1. Todo número natural possui um único sucessor, que também é um número natural.
2. Existe um único número natural que não é sucessor de nenhum outro. Este número é chamado de *zero* e é representado pelo símbolo 0.
3. Números naturais diferentes possuem sucessores diferentes.
4. **Axioma da Indução:** se um conjunto de números naturais contém o número 0 e, além disso, contém o sucessor de cada um dos seus elementos, então esse conjunto coincide com o conjunto dos números naturais.

Ou seja, $0 \in \mathbb{N}$ e existe uma função injetiva $s\colon \mathbb{N} \to \mathbb{N} \setminus \{0\}$, que associa a cada $n \in \mathbb{N}$ um elemento $s(n) \in \mathbb{N}$, chamado de sucessor de n. O axioma da Indução fica escrito assim

[2] Hmmmm! vou usar o zero como natural! Perdoem-me os puristas, espero que não desistam aqui, mas isso simplifica muito a apresentação pelo modo que foi estruturado este texto.

Axioma da Indução: *Para todo X, se $X \subset \mathbb{N}$ é um subconjunto tal que*

1. $0 \in X$ *e*

2. $\forall n,\ n \in X \Rightarrow s(n) \in X$,

então $X = \mathbb{N}$.

Exercício 6. *Nenhum número é sucessor dele mesmo*

Solução. Seja X o conjunto dos números naturais n tais que $n \neq s(n)$.

$0 \in X$ pelo axioma 2.

$n \in X \Rightarrow n \neq s(n)$; pelo axioma 3, $s(n) \neq s(s(n))$, portanto, $s(n) \in X$.

Pelo axioma da indução $X = \mathbb{N}$. □

s é bijetiva:

Exercício 7. *Todo natural, exceto o zero, é sucessor de algum número natural.*

Solução. Seja S o conjunto de todos os naturais que são sucessores de outro natural. Definimos $X := \{0\} \cup S$. Então $X \subset \mathbb{N}$ e $0 \in X$.

Seja $n \in X$, vamos mostrar que $s(n) \in X$. Se $n \neq 0$ então $n = s(m)$ e $s(n) = s(s(m))$ (ax. 3); como o natural $s(n)$ é sucessor de alguém (a saber, de $s(m)$) ele está em S, logo $s(n) \in X$. Se $n = 0$, então $s(0) \in S$, portanto, $s(0) \in X$.

Pelo axioma da indução $X = \mathbb{N}$, portanto, $S = \mathbb{N} \setminus \{0\}$. □

Denota-se $1 := s(0)$, $2 := s(1) = s(s(0))$, $3 := s(2) = s(s(s(0)))$ e assim vai.

1.1 Operações aritméticas

Adição: Para cada $m \in \mathbb{N}$, <u>somar m</u> é definido por

1. $m + 0 = m$;

2. $m + s(n) = s(m + n)$.

De modo que

$$m + 1 = m + s(0) = s(m + 0) = s(m). \tag{10}$$

Daí $1 + 1 = s(1) = 2$. Notemos que $s(1) = 2$ é uma definição enquanto que $1 + 1 = 2$ é um teorema.

Fixado $m \in \mathbb{N}$, notemos que se

$$X_m := \{n \in \mathbb{N}\colon\ m+n \text{ está definido }\}$$

então pelo Axioma da Indução $X_m = \mathbb{N}$ pois

a. $0 \in X_m$

b. se $m+n$ está definido então $s(m+n) \in \mathbb{N}$ logo $m+s(n)$ está definido.

$X_m = \mathbb{N}$ vale para todo natural m, portanto, $m+n$ está definido para todo par de número naturais.

Observação: *$+$ é uma operação binária $+\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ e escrevemos $a+b$ para denotar $+(a,b)$. A rigor, a demonstração acima tem o problema de que "está definido" usando em X_n não tem significado preciso. É possíver provar que $f\colon \mathbb{N}\to\mathbb{N}$ que satisfaça $f(0)=m$ e $f(s(n))=s(f(n))$ existe e é única, ou seja, a soma é a única operação binária sobre $\mathbb{N}$ que satisfaz os itens 1 e 2 acima.*

Multiplicação: Para $m \in \mathbb{N}$, multiplicar por m é definido por

1. $m \cdot 0 = 0$
2. $m \cdot s(n) = m \cdot n + m$.

Exercício 8. *Mostre que $m \cdot n$ está definido para todo par m, n de números naturais.*

Observação: *$\cdot$ é uma operação binária $\cdot\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ e escrevemos $a\cdot b$ para denotar $\cdot(a,b)$. Como na observação anterior, é possíver provar que $f\colon \mathbb{N}\to\mathbb{N}$ que satisfaça $f(0)=m$ e $f(s(n))=s(f(n))$ existe e é única, ou seja, amultiplicação é a única operação binária sobre $\mathbb{N}$ que satisfaz os itens 1 e 2 acima.*

A adição e a multiplicação de números naturais têm as seguintes propriedades.

Teorema 9. *Sejam a,b,c,m,n,p números naturais quaisquer*

1. *(adição é associativa)* $(a+b)+c = a+(b+c)$

   Demonstração. Dados a e b, seja $X := \{c\colon\ (a+b)+c = a+(b+c)\}$.

   Se $c=0$, então $(a+b)+0 = a+b$ e $a+(b+0) = a+b$, portanto $0 \in X$.

   Seja $c \in X$. Então $(a+b)+s(c) = s((a+b)+c) = s(a+(b+c))$. Usando a definição de soma duas vezes $s(a+(b+c)) = a+s(b+c) = a+(b+s(c))$. Portanto $s(c) \in X$. Pelo axioma da indução $X = \mathbb{N}$. □

2. *(adição é comutativa)* $a+b = b+a$

Demonstração. Começamos com o caso $a = 1$. Lembremos de (10) que $s(b) = b + 1$. Seja $X = \{b\colon s(b) = 1 + b\}$. Verifique que $0 \in X$. Se $b \in X$ então $s(b) = 1 + b$, logo $s(s(b)) = s(1 + b) = 1 + s(b)$, logo $s(b) \in X$, portanto $X = \mathbb{N}$. Com isso $b + 1 = 1 + b$ para todo natural b.

Agora, $Y := \{a\colon a + b = b + a(\forall b)\}$. $0, 1 \in Y$. Se $a \in Y$ então $s(a) + b = (a + 1) + b = a + (1 + b) = a + s(b) = s(a + b) = s(b + a)$. Agora, $s(b + a) = b + s(a)$, portanto, $s(a) \in X$. Assim $Y = \mathbb{N}$. □

3. *(elemento neutro da adição)* 0 *é o único natural tal que* $a + 0 = 0 + a = a$

   Demonstração. Que $a + 0 = 0 + a$ segue da comutatividade. Falta provar que 0 é o único natural com essa propriedade. Seja u tal que $a + u = u + a = a$ para todo natural a. Tomando $a = 0$, $u + 0 = 0$ portanto $u = 0$. □

4. *(lei de cancelamento da adição)* $a + c = b + c \Rightarrow a = b$

   Demonstração. Exercício: dado que

   $$a + s(c) = b + s(c) \Rightarrow s(a + c) = s(b + c) \Rightarrow a + c = b + c$$

   justifique a última implicação e complete a demonstração. □

5. *Se* $a + b = 0$ *então* $a = b = 0$.

   Demonstração. Se $a + b = 0$ e $b \neq 0$ então existe um natural c tal que $b = s(c)$ e $a + s(c) = 0$. Da definição de soma $s(a + c) = 0$, que contradiz o axioma 2. Analogamente, se $a \neq 0$ então derivamos uma contradição. Portanto, $a = b = 0$. □

6. *(elemento neutro da multiplicação)* $m \cdot 1 = 1 \cdot m = m$ *e* 1 *é único com essa propriedade.*

   Demonstração. Exercício. □

7. *(multiplicação é associativa)*$(m \cdot n) \cdot p = m \cdot (n \cdot p)$.

   Demonstração. Exercício. □

8. *(multiplicação é comutativa)* $m \cdot n = n \cdot m$.

   Demonstração. Veja exercício 13 a seguir. □

9. *(lei de cancelamento da multiplicação)* $mp = np$ *e* $p \neq 0 \Rightarrow m = n$.

Demonstração. Exercício. □

10. *(multiplicação é distributiva com respeito a adição)* $(a+b)\cdot m = a\cdot m + b\cdot m$.

    Demonstração. Exercício. □

11. *Se* $m\cdot n = 0$ *então* $m = 0$ *ou* $n = 0$.

    Demonstração. Se $m\cdot n = 0$ e $n \neq 0$. Então $n = s(p)$ para algum natural p. Então $m\cdot n = m\cdot s(p) = mp + m = 0$. Pelo item 5 $mp = m = 0$, assim $m = 0$. Analogamente, se $m \neq 0$ deduzimos que $n = 0$. □

12. *Se* $m\cdot n = 1$ *então* $m = n = 1$.

    Demonstração. Se $m = 0$ ou $n = 0$ então $m\cdot n = 0$ pela definição de produto. Portanto, existem naturais a e b tais que $m = s(a)$ e $n = s(b)$. Assim $s(a)s(b) = 1$, porém $1 = s(a)s(b) = (a+1)(b+1) = ab + a + b + 1$. Usando a lei de cancelamento, item 4, $ab + a + b = 0$, portanto $ab = a + b = 0$. De $a + b = 0$ temos $a = b = 0$, pelo item 5, logo $m = n = 1$. □

1.2 Relação de ordem ≤

Para $a, b \in \mathbb{N}$ escrevemos

$$a \leq b$$

se existe um natural m tal que

$$a + m = b.$$

Escrevemos $a < b$ caso $m \neq 0$. Ainda $a \geq b$ denota $b \leq a$ e $a > b$ denota $b < a$. A relação ≤ é

reflexiva $\forall a \in \mathbb{N}$, $a \leq a$, pois

$$a = a + 0;$$

antissimétrica $\forall a, b \in \mathbb{N}$, se $a \leq b$ e $b \leq a$ então $b = a$, pois existem naturais m, n

$$\begin{aligned} a \leq b &\Rightarrow a + m = b \\ b \leq a &\Rightarrow b + n = a \end{aligned}$$

portanto $(a+m)+n = a$, donde $a+(m+n) = a$ por associatividade da soma, pela lei cancelativa da soma $m + n = 0$; disso sabemos que $m = n = 0$ (teo. 9, item 5);

transitiva $\forall a,\ b,\ c \in \mathbb{N}$, se $a \leq b$ e $b \leq c$ então $a \leq c$, pois

$$\begin{aligned} a \leq b \quad &\Rightarrow \quad a + m = b \\ b \leq c \quad &\Rightarrow \quad b + n = c \end{aligned}$$

portanto $(a+m)+n = c$, donde $a+(m+n) = c$ e por definição de $\leq$ temos $a \leq c$.

Teorema 10. *Para quaisquer $a, b \in \mathbb{N}$, $a \leq b$ ou $b \leq a$.*

Demonstração. Para um dado natural b definimos

$$X_b := \{n\colon\ n \leq b\} \cup \{n\colon\ b \leq n\}.$$

Vamos mostrar que $X_b = \mathbb{N}$, assim $a \in X_b$ portanto $a \leq b$ ou $b \leq a$.

Como $0 \leq b$ temos $0 + b = b$, portanto, $0 \in X_b$.

Seja $n \in X_b$, então $n \leq b$ ou $b \leq n$. Se $n \leq b$ então existe r tal que $n + r = b$. Caso $r = 0$, de $n = b$ temos $s(n) = b + 1 \in X_b$ pois $b \leq b + 1$. Caso $r \neq 0$ existe u tal que $r = s(u)$. De $n + s(u) = b$ temos $s(n) + u = b$, portanto $b \leq s(n)$, logo $s(n) \in X_b$.

Se $b \leq n$, então $b + t = n$ para algum t, donde $s(n) = s(b + t) = b + s(t)$, isto é, $b \leq s(n)$ portanto $s(n) \in X_b$.

Pelo axioma da indução $X_b = \mathbb{N}$. □

Exercício 11 (Lei da tricotomia em $\mathbb{N}$)**.** *Para quaisquer $a, b \in \mathbb{N}$, vale uma e só uma das relações*

$$a = b,\ a < b,\ b < a$$

Solução. Dados naturais a e b, pelo teorema acima $a \leq b$ ou $b \leq a$. Logo existem $n, m \in \mathbb{N}$ tais que $a + n = b$ ou $b + m = a$. Se $a \neq b$ então $n, m \neq 0$, portanto $a < b$ ou $b < a$.

Agora, se $a < b$ e $b < a$ então $a + n = b$ e $b + m = a$ para n e m naturais diferentes de 0. De $a + n = b$ e $b + m = a$ concluímos que $(b + m) + n = b$ (substituindo a segunda na primeira); pela associativa $b + (m + n) = b$, pela cancelativa, $m + n = 0$ e pelo item 5 do teorema 9 $m = n = 0$. Uma contradição.

Se $a < b$ e $a = b$ então $a + n = b$ e $a = b$ para n natural diferente de 0. De $a + n = b$ e $a = b$ concluímos que $a + n = a$, portanto, $n = 0$. Uma contradição.

Se $a < b$ e $a = b$ então $a + n = b$ e $a = b$ para n natural diferente de 0. De $a + n = b$ e $a = b$ concluímos que $a + n = a$, portanto, $n = 0$. Uma contradição.

Desse modo vale exclusivamente um de $a = b,\ a < b,\ b < a$. □

Exercício 12. *Mostre que $\leq$ é compatível com a adição, i.e.,*

$$a \leq b \Rightarrow a + c \leq b + c \qquad (\forall c) \tag{11}$$

e é compatível com a multiplicação, i.e.,

$$a \leq b \Rightarrow a \cdot c \leq b \cdot c \qquad (\forall c). \tag{12}$$

Exercício 13. *Deduza de* (11) *o item* 4 *do teorema* 9*.*

Exercício 14. *Se $a < b$ então $a+1 \leq b$. Prove a recíproca.*

Solução: Se $a < b$ então $a + r = b$ com $r \neq 0$. Existe n tal que $r = n+1$. Assim $a + (n+1) = b$, porém $a + (n+1) = a + (1+n) = (a+1) + n$ e de $(a+1) + n = b$ temos $a + 1 \leq b$. □

1.3 Subtração em $\mathbb{N}$

Definimos

$$b - a := c, \text{ sempre que } a \leq b \text{ em que } c \text{ é o natural tal que } a + c = b \tag{13}$$

c existe por definição de $\leq$. Portanto, para quaisquer a, b, c com $a \leq b$

$$b - a = c \Leftrightarrow b = a + c \tag{14}$$

Como $a \leq a$, está definido $a - a$ que, por (14), vale $a - a = 0$. Por definição $b = a + (b - a)$.

Proposição 15. *Para quaisquer a, b, c com $a \leq b$ vale*

$$c \cdot (b - a) = c \cdot b - c \cdot a$$

Demonstração. Primeiro, verifiquemos que $c \cdot b - c \cdot a$ está definido. De fato, pela compatibilidade da multiplicação com a relação de ordem, exercício 12, página 17, $a \leq b \Rightarrow a \cdot c \leq b \cdot c$. Agora, pela definição de $\leq$, existe um natural d tal que $a + d = b$, portanto, $c \cdot (a + d) = c \cdot b$; usando os itens 8, 10 e 8 do teorema 9

$$\begin{aligned} c \cdot (a + d) &= (a + d) \cdot c \\ &= a \cdot c + d \cdot c \\ &= c \cdot a + c \cdot d \end{aligned}$$

logo $c \cdot a + c \cdot d = c \cdot b$ e por (14)

$$c \cdot b - c \cdot a = c \cdot d$$

e a proposição segue do fato de que $d = b - a$ que decorre de (14) e da escolha de d. □

Exercícios

1. Prove os itens 6,7,9 e 10 do teorema 9.
2. Prove que a multiplicação tem 1 como único elemento neutro.
3. Seja $a \neq 0$. Mostre que a *potência* a^n está definida para todo $n \in \mathbb{N}$ se

$$\begin{aligned} a^0 &:= 1 \\ a^{s(n)} &:= a \cdot a^n \end{aligned}$$

4. Prove que $a \leq b \Rightarrow a^n \leq b^n$.
5. Mostre que o *fatorial,* $n!$, está definido para todo $n \in \mathbb{N}$ se

$$\begin{aligned} 0! &:= 1 \\ (n+1)! &:= (n+1) \cdot n! \end{aligned}$$

6. Sejam a, b, c naturais tais que esteja definido $a-(b-c)$. Mostre que $(a+c)-b$ está bem definido e $a-(b-c) = (a+c)-b$.
7. Sejam a, b, c naturais tais que $b+c \leq a$. Mostre que $a-(b+c)$ e $(a-b)-c$ estão bem definidos e $a-(b+c) = (a-b)-c$.
8. Sejam a, b, c naturais tais que $0 < c < b < a$. Mostre que $0 < b-c < a-c < a$.
9. Sejam a, b, c naturais tais que $a \leq c$ e $b \leq c$. Mostre que, se $c-a \leq c-b$ então $b \leq a$.
10. Sejam a, b, c, d naturais tais que $a \leq b$ e $c \leq d$. Mostre que $b-a \leq d-c \Leftrightarrow b+c \leq a+d$.
11. Mostre que $s(m-1) = m$ sempre que $m-1$ está definido.

1.4 Princípio da Boa Ordem (PBO)

Teorema 16 (PBO)**.** *Todo $A \subset \mathbb{N}$ não-vazio tem um **menor elemento**, ou seja, existe $a \in \mathbb{N}$ tal que*

$$\begin{aligned} &a \in A \\ &\forall x \in A,\ a \leq x. \end{aligned}$$

Demonstração. Se $0 \in A$ então 0 é o menor elemento de A pois $0 \leq n$ para todo natural n. De fato $0+n = n$, donde $0 \leq n$.

Supondo $0 \notin A$ definimos

$$X := \{n \in \mathbb{N}:\ \text{para todo } k \leq n,\ k \notin A\}$$

e notamos que $0 \in X$ (pois, $0 \notin A$). Se valer que $n \in X \Rightarrow n+1 \in X$ para todo natural n, então teremos $X = \mathbb{N}$, o que não é verdade (por quê?), portanto existe um natural m tal que $m \in X$ e $m+1 \notin X$.

De $m \in X$ temos que $n \notin A$ para todo $n \leq m$ e de $m+1 \in X$ temos $m+1 \in A$ e como não há p, $m < p < m+1$, $m+1$ é menor elemento de A. De fato,

$$x \in A \Rightarrow m < x$$

portanto, pelo exercício 14, pág. 18, $m+1 \leq x$. □

Exercício 17. *Prove que não existe natural p tal que $0 < p < 1$.*
Obs.: *$n < p < n+1$ denota: $n < p$ e $p < n+1$*

Solução: Se $p \in \mathbb{N}$ é tal que que $0 < p < 1$ então $A = \{x \in \mathbb{N} : 0 < x < 1\}$ é um subconjunto não vazio dos naturais. Tome $m := \min(A)$ dado pelo PBO.

De $0 < m$ temos $0 < m^2$ e de $m < 1$ temos $m^2 < m < 1$, portanto $m^2 \in A$ e $m^2 < \min(A)$, uma contradição. □

Exercício 18. *$A \subseteq \mathbb{N}$ é dito limitado superiormente se existir um natural n tal que*

$$\forall x \in A,\ x \leq n$$

e se n com a propriedade acima pertence a A ele é dito maior elemento de A.

Mostre que se A é limitado superiormente e não vazio então admite maior elemento.

Proposição 19. *Para toda função $f : \mathbb{N} \to \mathbb{N}$ não-crescente[3], existe um natural n_0 a partir do qual f é constante.*

Demonstração. A imagem da função, $\mathrm{Im}(f)$, é um subconjunto não vazio de naturais. Seja n_0 um natural tal que $f(n_0)$ é o menor elemento de $\mathrm{Im}(f)$. Como f é não-crescente $n > n_0 \Rightarrow f(n) \leq f(n_0)$, mas $f(n) \not< f(n_0)$ pois $f(n_0)$ é o menor elemento de $\mathrm{Im}(f)$, portanto $n > n_0 \Rightarrow f(n) = f(n_0)$. □

Corolário 20. *Se f é decrescente então $\mathrm{Im}(f)$ é finito.* □

1.5 Princípios de Indução

O axioma de indução tem um papel de fundamental não só na teoria dos números naturais como em toda matemática. É visto como um método de demonstração, conhecido como *Princípio de Indução Matemática* ou *Princípio de Indução Finita*, usualmente expresso da seguinte maneira

$P(n)$ é um predicado sobre $\mathbb{N}$

[3] $x < y \Rightarrow f(x) \geq f(y)$

Princípio da Indução Finita (PIF). *Se são satisfeitas as condições*

1. $P(0)$ *é verdadeiro, e*

2. *para todo* $k \geq 0$, *se* $P(k)$ *é verdadeiro então* $P(k+1)$ *é verdadeiro,*

então $P(n)$ *é verdadeiro para todo natural* n.

Esse princípio decorre facilmente do axioma da Indução se tomarmos X como o conjunto dos naturas para os quais o predicado é verdadeiro, isto é,

$$X = \{n \in \mathbb{N} \colon P(n) \text{ é verdadeiro}\}$$

da condição 1 temos $0 \in X$ da condição 2 temos que se $k \in X$ então $k+1 \in X$, portanto, $X = \mathbb{N}$.□

Princípio da Indução Finita generalizado (PIFg). *Seja a um número natural. Se*

1. $P(a)$ *é verdadeiro, e*

2. *para todo* $k \geq a$, *se* $P(k)$ *é verdadeiro então* $P(k+1)$ *é verdadeiro,*

então $P(n)$ *é verdadeiro para todo natural* $n \geq a$.

Esse princípio decorre do Princípio da Boa Ordem da seguinte forma: suponha que *não* vale a sentença "$P(n)$ é verdadeiro para todo natural $n \geq a$", logo

$$A := \{n \in \mathbb{N} \colon n \geq a \text{ e } P(n) \text{ não é verdadeiro}\}$$

é não vazio, portanto admite um menor elemento $b := \min A$.

$b > a$ (estrito pois $a \notin A$) logo b não é zero, portanto existe existe um natural c tal que $b = s(c) = c+1$, ainda $b > a \Rightarrow c \geq a$ mas como b é o menor elemento de A devemos ter $c \notin A$, ou seja, $P(c)$ é verdadeiro. Mas, isso implica (condição 2) que $P(c+1) = P(b)$ é verdadeiro, uma contradição.□

Exemplo. $2^n < n!$ *para todo* $n \geq 4$*:* $P(n)$ *é* $2^n < n!$ *que é verdadeiro para* $n = 4$ *(confira). Seja* k *um natural maior ou igual a* 4 *e assumamos que* $P(k)$ *é verdadeiro, ou seja*

$$2^k < k! \tag{15}$$

Pela escolha de k, $k > 1 \Rightarrow k+1 > 2 \Rightarrow (k+1)\cdot k! > 2 \cdot k!$, *portanto* $(k+1)! > 2 \cdot k!$ *e usando* (15) $(k+1)! > 2^{k+1}$. *Pelo PIFg,* $2^n < n!$ *para todo* $n \geq 4$.

Notemos que, da dedução acima, PBO⇒PIFg. Entretanto, PIFg⇒PIF, basta tomar $a = 0$ e provamos o PBO usando PIF, isto é, PIF⇒PBO, portanto

$$\text{PIF} \Rightarrow \text{PBO} \Rightarrow \text{PIFg} \Rightarrow \text{PIF}$$

tais princípios são equivalentes.

Princípio da Indução Finita, segunda forma (PIF2). *Seja a um número natural. Se*

1. *$P(a)$ é verdadeiro, e*
2. *$P(k)$ verdadeiro para todo $k \in \{a, a+1, \ldots, n\}$ implica $P(n+1)$ verdadeiro,*

então $P(n)$ é verdadeiro para todo natural $n \geq a$.

Exercícios

1. Seja a um número natural e P um predicado sobre $\mathbb{N}$. Verifique o seguinte Princípio de Indução: *Se*

   (1) $P(a)$ é verdadeiro, e

   (2) $P(b)$ verdadeiro para todo $b \in \{a, a+1, \ldots, k\}$ implica $P(k+1)$ verdadeiro,

   então $P(n)$ é verdadeiro para todo natural $n \geq a$.

2. Seja a_i uma sequência (estritamente) crescente de números naturais. Verifique o seguinte Princípio de Indução: *Se $P(n)$ é um predicado a respeito de $n \in \mathbb{N}$ de modo que*

   (1) $P(a_i)$ é verdadeiro para todo $i \in \mathbb{N}$ e

   (2) $P(j)$ verdadeiro implica $P(j-1)$ verdadeiro, para todo $j > a_1$

   então $P(n)$ é verdadeiro para todo $n \geq a_1$.

3. Descubra uma falha na prova: *todos os números naturais são iguais* Denotamos por $\max(a,b)$ o maior número natural dentre a e b. Vamos mostrar por indução que se $\max(a,b) = n$ então $a = b$.

   (a) Se $\max(a,b) = 0$ então $a = b = 0$.

   (b) Suponha que se $\max(a,b) = k-1$ então $a = b$.

   Vamos mostrar que

   $$\text{se } \max(a,b) = k+1 \text{ então } a = b.$$

   Suponha que $\max(a,b) = k+1$. Então $\max(a-1, b-1) = k$ e pela hipótese indutiva $a-1 = b-1$, portanto $a = b$.

4. Sejam $A_1, A_2, \ldots, A_n$ conjuntos e $n \geq 2$. Suponha que para dois conjuntos quaisquer A_i e A_j vale que $A_i \subseteq A_j$ ou $A_j \subseteq A_i$. Prove, por indução, um desses conjuntos é subconjunto de todos eles.

5. Prove, usando indução, que todo número natural, exceto o zero, pode ser expresso como soma de potências distintas de 2

6. Demonstre usando indução:

   (a) $9+9\cdot 10+9\cdot 10^2+\cdots+9\cdot 10^{n-1}=10^n-1$.

   (b) $1+3+5+\cdots+(2n-1)=n^2$.

   (c) $1+2+4+\cdots+2n=n(n+1)$

   (d) $2^n\leq 2^{n+1}-2^{n-1}-1$

   (e) $n!<n^n$, $n\geq 2$

   (f) $1^3+3^3+\cdots+(2n+1)^3=(n+1)^2(2n^2+4n+1)$

2 Divisibilidade em $\mathbb{N}$

Dizemos que o natural a **divide** o natural b, e escrevemos $a|b$, se existe um natural c tal que $b=a\cdot c$. Em símbolos essa definição é

$$a|b \Leftrightarrow \exists c\in\mathbb{N},\ b=a\cdot c$$

Notação: $\not|$ significa *não divide* e b é **múltiplo** de a significa $a|b$.

Observação. $0|0$ *pois* $0=0\cdot c$ *para todo* c, *mas* $0\not|b$ *caso* $b\neq 0$ *pois, nesse caso, não existe* c *tal que* $b=0\cdot c$. *Ainda* $a|0$.

Como o *menor ou igual*, o *divide* é uma relação sobre o conjunto $\mathbb{N}$ que satisfaz[4]

reflexiva $\forall a\in\mathbb{N}$, $\boxed{a|a}$, pois $a=a\cdot 1$;

antissimétrica $\forall a,\ b\in\mathbb{N}$, $\boxed{\text{se } a|b \text{ e } b|a \text{ então } b=a}$, pois de $a|b$ e $b|a$ ou $a=b=0$ ou $a,b\neq 0$ e existem naturais m,n

$$\begin{aligned} a|b &\Rightarrow a\cdot m=b\\ b|a &\Rightarrow b\cdot n=a \end{aligned}$$

portanto $(a\cdot m)\cdot n=a$, donde tiramos que $m\cdot n=1$ e disso sabemos que $m=n=1$ (teo. 9, item 12);

[4] toda relação reflexiva, antissimétrica e transitiva sobre um conjunto é chamada de *ordem parcial* sobre o conjunto.

transitiva $\forall a,\ b,\ c \in \mathbb{N}$, $\boxed{\text{se } a|b \text{ e } b|c \text{ então } a|c}$, pois

$$\begin{aligned} a|b &\Rightarrow a \cdot m = b \\ b|c &\Rightarrow b \cdot n = c \end{aligned}$$

portanto $(a \cdot m) \cdot n = c$, donde $a|c$.

Teorema 21. *Para quaisquer números naturais a, b, c, d*

1. $1|a$;
2. $a|b$ *e* $c|d \Rightarrow a \cdot c|b \cdot d$;
3. $a|(b+c) \Longrightarrow \big[a|b \Leftrightarrow a|c\big]$;
4. $c \leq b$ *e* $a|(b-c) \Longrightarrow \big[a|b \Leftrightarrow a|c\big]$;
5. $a|b$ *e* $a|c \Rightarrow a|(bx+cy)$ *para todos* $x,\ y \in \mathbb{N}$. *Também,* $a|b$ *e* $a|c \Rightarrow a|(bx-cy)$ *para todos* $x,\ y \in \mathbb{N}$ *pros quais* $bx \geq cy$;
6. $a|b$ *e* $b \neq 0 \Rightarrow a \leq b$.

Demonstração. 1. De $1 \cdot a = a$ segue que $1|a$.□

2. Se $a|b$ e $c|d$ então existem $m,\ n \in \mathbb{N}$ tais que

$$\begin{aligned} a \cdot m &= b \\ c \cdot n &= d \end{aligned}$$

de modo que $b \cdot d = (a \cdot m) \cdot (c \cdot n) = (a \cdot c) \cdot (m \cdot n)$, portanto $a \cdot c|b \cdot d$.□

3. Suponhamos que $a|(b+c)$, i.e, $a \cdot d = b + c$ para algum d. Se $a = 0$ então $b + c = 0$, então $b = c = 0$ e vale a conclusão. Seja $a \neq 0$.

   Se $a|b$, $a \cdot x = b$ para algum x, portanto $a \cdot d = a \cdot x + c$, assim $a \cdot x \leq a \cdot d$ e pela equação (14)

$$a \cdot d - a \cdot x = c$$

   como $a \neq 0$, $a \cdot x \leq a \cdot d \Rightarrow x \leq d$ e pela Proposição 15

$$a \cdot (d - x) = c$$

   donde concluímos que $a|c$.

   Acima provamos que $a|b \Rightarrow a|c$. Resta provar que $a|c \Rightarrow a|d$.

$$a|c \Rightarrow a \cdot y = c \Rightarrow a \cdot d = a \cdot y + b \Rightarrow a \cdot (d - y) = b \Rightarrow a|b$$

   pelas mesmas justificativas apresentadas acima.□

4. Exercício.

5. Se $a|b$ e $a|c$ então existem $m,\ n \in \mathbb{N}$ tais que

$$a \cdot m = b$$
$$a \cdot n = c$$

portanto, dados $x, y \in \mathbb{N}$

$$a \cdot m \cdot x = b \cdot x$$
$$a \cdot n \cdot y = c \cdot y$$

portanto

$$a \cdot m \cdot x + a \cdot n \cdot y = b \cdot x + c \cdot y \Leftrightarrow$$
$$a \cdot (m \cdot x + n \cdot y) = b \cdot x + c \cdot y$$

ou seja $a|(bx + cy)$.□

6. $a|b$ e $b \neq 0 \Rightarrow a \cdot c = b$ para algum $c \neq 0$; também, $c = d + 1$ para algum $d \in \mathbb{N}$. Portanto $a \cdot (d+1) = b$ o que implica em

$$a + a \cdot d = b$$

que equivale a $a \leq b$.

□

2.1 Algoritmo de divisão

Exercício 22. *Sejam a e b números naturais, $b \neq 0$. Então para algum natural q*

$$bq \leq a < b(q+1). \tag{16}$$

Solução. Se $a < b$ então $q = 0$ é o único natural que satisfaz (16). Se $a \geq b$ então definimos o conjunto

$$A := \{n \in \mathbb{N} :\ bn > a\}$$

que é não-vazio pois $a+1 \in A$ (verifique[5]), portanto tem um menor elemento $m > 0$ (pois $0 \notin A$); ademais m é sucessor de algum natural q, $m = q + 1$, $b(q+1) > a$ e, pela minimalidade de $q+1$, temos que $bq \leq a$. □

[5] $b \geq 1 \Rightarrow ba \geq a \Rightarrow ba + b \geq a + b > a$

Continuando nas hipóteses acima, se $bq \leq a$ então existe um natural r tal que

$$bq + r = a$$

e com $r < b$ pois, caso contrário, $r \geq b \Rightarrow bq + r \geq b(q+1) \Rightarrow a \geq b(q+1)$ contrariando (16).

Ademais, tais r e q são únicos. Por (14)

$$bq + r = a \Leftrightarrow r = a - bq$$

Admitamos que exista $r' \neq r$ com $r' = a - bq'$, $r = a - bq$ e $r' < r < b$. Então

$$bq' + r' = bq + r \Leftrightarrow$$
$$bq' = bq + r - r'$$

portanto $b|(bq + r - r')$ e pelo teorema 21, item 3, $b|(r - r')$ e pelo teorema 21, item 6, $b \leq r - r'$, contrariando $r < b$. Caso $r < r'$, por dedução análoga, também termina em contradição. Pela lei de tricotomia $r = r'$. Agora, se $r' = a - bq'$ e $r = a - bq$ e $r = r'$ então $q = q'$, ou seja, q também é único.

Em resumo, os naturais q e r cujas existência foi determinada acima são os únicos a satisfazerem $bq + r = a$. Provamos o seguinte teorema

Teorema 23 (**Algoritmo da divisão**, livro VII de *Elementos* de Euclides, 300 aC)**.** *Para todo natural a e todo natural $b \neq 0$ existe um único natural q e um único natural r com $r < b$ tal que*

$$a = bq + r. \tag{17}$$

Notação No teorema acima, caso $a = bq + r$

a é o **dividendo**, b é o **divisor**
$\lfloor a/b \rfloor := q$ é o **quociente** da divisão, quando $r = 0$ escrevemos apenas a/b
$a \bmod b := r$ é o **resto** é o resto.

Outra prova do teorema da divisão. Se $a < b$ então basta tomarmos $q = 0$ e, assim, $r = a$. Agora, para unicidade, se $q > 0$ então $q \geq 1$ (exercício 14), então $bq + r \geq b1 + r$ para todo r (exercício 12), ou seja, $a \geq b + r$ para todo r. Fazendo $r = 0$ temos $a \geq b$. Portanto q é único, e por conseguinte r também é único.

Se $a \geq b$, a ideia é considerar as sucessivas subtrações $a, a-b, a-2b, a-3b, \ldots$ enquanto estiver definida. Definimos o conjunto

$$R := \{n \in \mathbb{N} \colon a - bn \text{ está definido } \}. \tag{18}$$

e como $1 \in R$, $R \neq \emptyset$. Como $a - bn \leq a$ $(\forall n \in R)$ podemos definir q como o *maior* elemento de R, que existe pelo exercício 18, e $r := a - bq$.

Por (14)

$$bq + r = a \Leftrightarrow r = a - bq.$$

Caso $r \geq b$ deduzimos

$$\exists t,\ r + t = b \Leftrightarrow \exists t,\ bq + r + t = bq + b \Leftrightarrow \exists t,\ a + t = b(q+1)$$

portanto $q+1 \in R$, o que contraria o fato de q ser o maior elemento desse conjunto, portanto, $r < b$.

Para provar a unicidade, suponhamos que $r = a - bq$ e $r' = a - bq'$ e $r < r' < b$. Assim, $r' - r = b(q - q')$ e $b|(r - r')$ donde $b \leq r - r'$, um absurdo. Analogamente, não vale $r' < r$. Portanto $r = r'$, e disso $a - bq = a - bq'$, donde $q = q'$. □

Exemplo. *Do teorema temos que o resto da divisão de n por 2, para qualquer $n \in \mathbb{N}$, é 0 ou 1; quando o resto é 0 dizemos que n é um natural **par** e quando o resto é 1 dizemos que n é um natural **ímpar**. A característica de um número ser par ou ímpar é chamada de **paridade**.*

Exemplo. *Todo número natural pode ser escrito em uma (e só uma) das formas: $3q$, $3q+1$, $3q+2$.*

Exemplo. $253 = 50 \cdot 5 + 3$, *portanto, os naturais menores ou iguais a 253 e múltiplos não-nulos de 5 são:* $1 \cdot 5, 2 \cdot 5, 3 \cdot 5, \ldots, 49 \cdot 5, 50 \cdot 5$.

De um modo geral, se $b \leq a$ então a quantidade de naturais menores ou iguais a a que são *múltiplos não-nulos* de b é $\lfloor a/b \rfloor$.

Exercício 24. *Discuta a paridade da adição, do produto, da subtração e da potência de números naturais.*

Exercício 25. *Um número natural a é par se e somente se a^n é par para todo $n \in \mathbb{N} \setminus \{0\}$.*

Solução. Seja a um natural par. Então a^1 é par. Suponhamos que para $n > 1$ fixo, a^{n-1} é par, então $a^n = a^{n-1} \cdot a$ e por ser o produto de dois pares, a^n é par. Pelo PIFg a^n é par para todo $n \geq 1$.

Se a^n é par para todo $n \in \mathbb{N} \setminus \{0\}$, em particular a^1 é par. □

2.2 Representação — sistemas posicionais

No sistema decimal $253 = 200+50+3$ cada algarismo tem o seu valor e, além disso, um peso determinado pela posição; todo natural m é escrito como o numeral $d_n d_{n-1} \ldots d_1 d_0$ com $d_i \in \{0,1,2,3,4,5,6,7,8,9\}$ para todo i de modo que

$$m = d_n \cdot 10^n + d_{n-1} \cdot 10^{n-1} + \cdots + d_1 \cdot 10 + d_0$$

Exemplo. *No sistema binário os números são escritos com os algarismos 0 e 1 do sistema posicional de base 2*

$$253 = (11111101)_2 = 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

Em computação $\{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}$ *são os algarismos do sistema posicional de base* 16

$$253 = (FD)_{16} = 15 \cdot 16^1 + 13 \cdot 16^0$$

Teorema 26. *Seja* $b > 1$ *um natural e* $R = \{0,1,\ldots,b-1\}$. *Para todo natural* m *existem natural* n *e únicos* $d_i \in R$ *para* $0 \leq i \leq n$, *tais que*

$$m = d_n \cdot b^n + d_{n-1} \cdot b^{n-1} + \cdots + d_1 \cdot b + d_0 \tag{19}$$

com $d_n \neq 0$, *exceto quando* $m = 0$.

Demonstração. Se $m = 0$ então $n = 0$ e $d_0 = 0$; se $m = 1$ então $n = 0$ e $d_0 = 1$. Seja $m > 1$ um natural e assumamos que todo natural menor que m pode ser representado de forma única como em (19).

Usando o algoritmo de divisão para dividir m por b temos que existem q e r únicos tais que

$$m = bq + r,\ r < b$$

e pela hipótese de indução, pois $q < m$ (justifique), existem $e_0, e_1, \ldots, e_{n'-1}, e_{n'}$ únicos tais que

$$q = e_{n'} \cdot b^{n'} + \cdots + e_1 \cdot b + e_0$$

para algum n'. Assim

$$bq + r = e_{n'} \cdot b^{n'+1} + \cdots + e_1 \cdot b^2 + e_0 b + r$$

de modo que, fazendo

$$d_0 = r$$
$$d_i = e_{i-1} \text{ para } 1 \leq i \leq n$$

e depois disso fazendo $n = n' + 1$, o resultado segue pela segunda forma do PIF. □

A representação (19) dada no teorema acima é chamada de **expansão relativa à base** b. Quando $b = 10$, essa expansão é chamada **expansão decimal**, quando $b = 2$, ela toma o nome de **expansão binária** e quando $b = 16$ **expansão hexadecimal**.

A expansão numa dada base $b > 1$ nos fornece um método para representar os números naturais. Para tanto, escolhemos um conjunto $S = \{s_0, s_1, \ldots, s_{b-1}\}$ com b símbolos e $s_0 = 0$ para representar os números de 0 a $b-1$. Um número natural m na base b é escrito na forma $d_n d_{n-1} \ldots d_1 d_0$, com $d_i \in S$ para todo i representando o número (19).

No sistema decimal usamos $S = \{0,1,2,3,4,5,6,7,8,9\}$. Se $b \leq 10$, utilizamos os símbolos $0,1,\ldots,b-1$. Se $b > 10$, normalmente, usamos os símbolos de 0 a 9 e acrescentamos novos símbolos para $10,\ldots,b-1$.

Da demostração acima tiramos que a representação de m na base b é obtida por

$$\begin{aligned} m &= bq_0 + d_0 \\ q_0 &= bq_1 + d_1 \\ q_1 &= bq_2 + d_2 \\ &\vdots \end{aligned}$$

como $q_0 > q_1 > q_2 > \cdots$ essa sequência termina em algum n (corolário 20), de fato, quando $q_{n-1} < b$ temos $q_n = 0$ e a partir daí os restos valem 0.

Exemplo. 253 *na base binária é obtido por*

$$\begin{aligned} 253 &= 2 \cdot 126 + 1 \\ 126 &= 2 \cdot 63 + 0 \\ 63 &= 2 \cdot 31 + 1 \\ 31 &= 2 \cdot 15 + 1 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

Exemplo 27 (divisibilidade por 5)**.** *Dado* $n \in \mathbb{N}$,

$$\begin{aligned} n &= d_t \cdot 10^t + d_{t-1} \cdot 10^{t-1} + \cdots + d_1 \cdot 10 + d_0 \\ &= 10(d_{t-1} \cdot 10^{t-2} + d_{t-2} \cdot 10^{t-3} + \cdots + d_1 \cdot) + d_0 \end{aligned}$$

assim, se $5|n$*, como* $5|10(d_{t-1} \cdot 10^{t-2} + d_{t-2} \cdot 10^{t-3} + \cdots + d_1 \cdot)$ *(teorema 21) portanto deve dividir* d_0*, logo*

$$d_0 \in \{0, 5\}$$

de modo que um natural é divisível por 5 *se, e só se, termina com o algarismo* 0 *ou o algaismo* 5*.*

Exemplo 28 (divisibilidade por 3)**.** *Vamos denotar, só nesse exemplo, por* $9^{[t]}9$ *o numeral escrito com* t *ocorrências do algarismo* 9*, por exemplo,* $9^{[3]}9 = 999$*.*

Dado $n \in \mathbb{N}$,

$$\begin{aligned} n &= d_t \cdot 10^t + d_{t-1} \cdot 10^{t-1} + \cdots + d_1 \cdot 10 + d_0 \\ &= d_t \cdot (9\overbrace{\ldots}^{[t]}9 + 1) + d_{t-1} \cdot (9\overbrace{\ldots}^{[t-1]}9 + 1) + \cdots + d_1 \cdot (9 + 1) + d_0 \\ &= \left(d_t \cdot 9\overbrace{\ldots}^{[t]}9 + d_{t-1} \cdot 9\overbrace{\ldots}^{[t-1]}9 + \cdots + d_1 \cdot 9\right) + (d_t + d_{t-1} + \cdots + d_0) \\ &= 9 \cdot \left(d_t \cdot 1\overbrace{\ldots}^{[t]}1 + d_{t-1} \cdot 1\overbrace{\ldots}^{[t-1]}1 + \cdots + d_1 \cdot 1\right) + (d_t + d_{t-1} + \cdots + d_0) \end{aligned}$$

assim, se $3|n$, *como* $3|9(d_{t-1} \cdot 1\overbrace{\ldots}^{[t]}1 + \cdots + d_1)$ *(teorema 21) portanto deve dividir* $d_t + d_{t-1} + \cdots + d_0$, *de modo que um natural é divisível por* 3 *se, e só se, a soma de seus algarismos for divisível por* 3.

Exercício 29. *Obtenha um critério de divisibilidade por* 9.

Exercícios

1. Mostre que $8|3^{2n} + 7$ para todo n.
2. Mostre que $3|10^n - 7^n$ para todo n.
3. Mostre que $8|n^2 - 1$ para todo n ímpar.
4. Mostre que $3|2^n - 1$ para todo n par.
5. Mostre que $n^2|(n+1)^n - 1$ para todo n.
6. Sejam $n \in \mathbb{N}$, x, y quaisquer $x \neq -y$. Mostre que $x^{2n} - y^{2n}$ é divisível por $x + y$. Mostre que $x^{2n-1} + y^{2n-1}$ é divisível por $x + y$. Mostre que $x^n - y^n$ é divisível por $x - y$.
7. Seja n um natural. Um, e só um, número dentre n, $n+2$, e $n+4$ é divisível por 3.
8. Mostre que se $3 \nmid a$ então $a^2 \bmod 3 = 1$.
9. Use o exercício anterior para mostrar que se $3|(a^2 + b^2)$ então a e b são divisíveis por 3.
10. Mostre que n^2 dividido por 6 nunca deixa resto 2.
11. Quantos múltiplos de 6 há entre 92 e 196?
12. Mostre que de dois números pares consecutivos um é divisível por 4.
13. Prove que $(121)_b$ em qualquer base $b > 2$ é um quadrado perfeito.
14. Prove que $4|(a_r \cdots a_1 a_0)_5 \Leftrightarrow 4|(a_r + \cdots + a_1 + a_0)$
15. Obtenha um critério de divisibilidade por 4.

2.3 MDC

Para todo $a \in \mathbb{N}$ denotemos por $D(a)$ o conjunto dos divisores de a

$$D(a) = \{m\colon\ m \in \mathbb{N} \text{ e } m|a\}. \tag{20}$$

Para quaisquer a e b temos $1 \in D(a) \cap D(b)$ e se não são ambos nulos temos, para todo $m \in D(a) \cap D(b)$, que $m \leq \max\{a,b\}$, portanto a interseção é não-vazia e limitada superiormente. Pelo exercício 18 está definido o maior elemento $\max D(a) \cap D(b)$ para quaisquer $a, b \in \mathbb{N}$ não ambos nulos. Notemos que se $a = b = 0$ então $D(a) \cap D(b) = \mathbb{N}$.

$\text{mdc}(a,b)$ é o **maior divisor comum** de a e b

$$\text{mdc}(a,b) := \begin{cases} 0, & \text{se } a = b = 0, \\ \max D(a) \cap D(b), & \text{caso contrário.} \end{cases} \tag{21}$$

Claramente, $\text{mdc}(a,b) = \text{mdc}(b,a)$; ressaltamos que $\text{mdc}(0,0) = 0$ é uma convenção. Vejamos alguns casos particulares

1. $a \neq 0 \Rightarrow \text{mdc}(0,a) = a$
2. $\text{mdc}(1,a) = 1$.
3. $b|a$ se, e somente se, $\text{mdc}(a,b) = b$.

Agora, se $b \nmid a$ então temos $a = bq + r$, $0 \neq r < b$. Todo divisor de b e r divide $bq + r$ (teo. 21, item 5) portanto divide a e b; ou seja, $D(b) \cap D(r) \subset D(a) \cap D(b)$. De $r = a - bq$, todo divisor de a e b divide r e b; ou seja, $D(b) \cap D(r) \supset D(a) \cap D(b)$. Logo, $D(b) \cap D(r) = D(a) \cap D(b)$ e, então, $\text{mdc}(a,b) = \text{mdc}(b,r)$.

Repetindo esse processo temos $\text{mdc}(b,r) = \text{mdc}(r, b \bmod r)$ e como o sequência dos restos é decrescente, em algum momento o resto é 0 e voltamos ao caso do item 3 acima.

Teorema 30 (**Algoritmo de Euclides**, livro VII de *Elementos* de Euclides, 300 aC)**.** *Se $a = bq + r$ então* $\text{mdc}(a,b) = \text{mdc}(b,r)$. □

Assim, obtemos $\text{mdc}(a,b)$ com divisões sucessivas:

$$\begin{aligned} a &= bq_1 + r_1,\ r_1 < b \\ b &= r_1 q_2 + r_2,\ r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3,\ r_3 < r_2 \\ r_2 &= r_3 q_4 + r_4,\ r_4 < r_3 \\ r_3 &= r_4 q_5 + r_5,\ r_5 < r_4 \\ &\vdots \end{aligned}$$

a sequência de restos $r_1, r_2, \ldots$ é decrescente, então (corolário 20) para algum n

$$r_{n-2} = r_{n-1}q_n + r_n, \quad r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0$$

$r_n | r_{n-1}$ logo $\mathrm{mdc}(r_n, r_{n-1}) = r_n$ e do teorema acima $\mathrm{mdc}(a,b) = \mathrm{mdc}(b, r_1) = \cdots = \mathrm{mdc}(r_{n-1}, r_n) = r_n$.

Exemplo. $\mathrm{mdc}(41,12) = 1$*:*

$$\begin{aligned} 41 &= 12\cdot 3+5 \\ 12 &= 5\cdot 2+2 \\ 5 &= 2\cdot 2+1 \\ 2 &= 1\cdot 2+0 \end{aligned}$$

Exemplo 31 (números de Fermat)**.** *Para qualquer $n > m$*

$$\mathrm{mdc}\left(2^{2^n}+1, 2^{2^m}+1\right) \tag{22}$$

Da identidade $2^{2^{m+1}} - 1 = (2^{2^m}+1)(2^{2^m}-1)$ *temos*

$$2^{2^n} - 1 = \left(2^{2^{n-1}}+1\right)\left(2^{2^{n-2}}+1\right)\left(2^{2^{n-3}}+1\right)\cdots\left(2^{2^{m+1}}+1\right)\left(2^{2^m}+1\right)\left(2^{2^m}-1\right)$$

portanto

$$\left(2^{2^m}+1\right) \Big| \left(2^{2^n}-1\right) \qquad \textit{(mostre que isso segue do exerc. 6, pág. 30)}$$

portanto um divisor de $2^{2^m}+1$ *divide* $2^{2^n}-1$*, ademais*

$$2^{2^n}+1 = \left(2^{2^n}-1\right)+2$$

portanto um divisor de $2^{2^n}+1$*, que divide* $2^{2^n}-1$*, divide* 2 *(teo. 21, item 3), ou seja, um divisor comum de* $2^{2^n}+1$ *e* $2^{2^m}+1$*, que são ímpares, divide* 2*, logo o* mdc *é* 1.

Quando $\mathrm{mdc}(a,b) = 1$ dizemos que a e b são **coprimos** ou **primos entre si**.

Exercício 32. *Para $a, b, c \in \mathbb{N}$,*

1. $\mathrm{mdc}(ca, cb) = c \cdot \mathrm{mdc}(a,b)$.
2. *Para $a, b \neq 0$, se* $\mathrm{mdc}(a,b) = 1$ *então existem x e y tais que $ax - by = 1$.*
3. *Se $a|bc$ e* $\mathrm{mdc}(a,b) = 1$ *então $a|c$.*
4. *Se $a|c$ e $b|c$, $c \neq 0$, e* $\mathrm{mdc}(a,b) = 1$ *então $ab|c$.*

5. *c é divisível por* 6 *se, e só se, é divisível por* 2 *e por* 3.

6. *Se* $\text{mdc}(a,c) = 1$ *e* $\text{mdc}(b,c) = 1$ *então* $\text{mdc}(ab,c) = 1$.

Solução. Sejam $a, b, c \in \mathbb{N}$.

1. Vamos provar o item 1. Do algoritmo da divisão, para $\text{mdc}(a,b)$ com divisões sucessivas temos:

$$\begin{aligned} ca &= (cb)q_1 + cr_1 \\ cb &= (cr_1)q_2 + cr_2 \\ cr_1 &= (cr_2)q_3 + cr_3 \\ &\vdots \\ cr_{n-2} &= (cr_{n-1})q_n + cr_n \\ cr_{n-1} &= (cr_n)q_{n+1} \end{aligned}$$

   logo $\text{mdc}(ca,cb) = \text{mdc}(cb,cr_1) = \cdots = \text{mdc}(r_{n-1},r_n) = cr_n = c\text{mdc}(a,b)$.□

2. Para provar o item 2, primeiro observamos que se $d = ax - by$ para algum x e algum y, então $d = by' - ax'$ para para algum x' e algum y'. De fato, se $d = ax - by$ então por (16) existem q e p tais que $qa > y$ e $pb > x$. Tomando $m := \max\{q,p\}$ temos $ma > y$ e $mb > x$. Agora, $d = (ma - y)b - (mb - x)a$.

   Agora, consideremos $d = ax_0 - by_0 = by_0' - ax_0'$ o menor natural não-nulo que pode ser escrito da forma $ax - by$. Notemos que $a = a1 - b0$ e que $b = ab - b(a-1)$, portanto d está definido. Se $m = ax - by$, então $d|m$: pelo algoritmo da divisão $r = m - dq$ e $r < d$, i.e,

$$r = ax - by - (by_0' - ax_0')q = a(x + x_0'q) - b(y + y_0'q)$$

   portanto existem x_1, y_1 tais que $r = ax_1 - by_1$ e $r < d$, e como d é o menor não-nulo dessa forma, só resta a possibilidade de $r = 0$. Se $d|m$ então $d|a$ e $d|b$, portanto $d = 1$.

3. Para o item 3, observamos que $an - bm = 1$ pelo item anterior, de modo que $anc - bmc = c$. Como $az = bc$ para algum z, temos $anc - amz = c$, portanto $a|c$. Se $a = 0$ então $b = 1$ e $c = 0$, e se $b = 0$ então $a = 1$, então $a|c$ em ambos os casos.

4. Para o item 4, temos por hipótese (e item 1) que existem x, y, n, m tais que $ax = c$, $by = c$ e $an - bm = 1$. Dessa última, $anc - bmc = c$ e substituindo $anby - bmax = c$, ou seja $ab(ny - mx) = c$, portanto, $ab|c$. Se $a = 0$ então $c = 0$, portanto, $ab|c$. Por hipótese $c \neq 0$, logo $b \neq 0$.

□

2.4 MMC

Analogamente, $M(a) := \{n \cdot a \colon n \neq 0\} \subset \mathbb{N}$ denota o conjunto dos múltiplos de a. Assim $M(a) \cap M(b)$ é não vazio, pois $a \cdot b$ está nessa intersecção, e pelo PBO admite um menor elemento m, dizemos que m é o **mínimo múltiplo comum** de a e b. Denotamos o maior divisor comum de a e b por $\text{mmc}(a,b)$. É claro que $\text{mmc}(a,b) = \text{mmc}(b,a)$.

Proposição 33. *Sejam $a, b \in \mathbb{N}$. O $\text{mmc}(a,b)$ existe e satisfaz*

$$\text{mdc}(a,b) \cdot \text{mmc}(a,b) = a \cdot b \tag{23}$$

Antes de demonstrarmos essa proposição, vejamos uma **notação** bastante útil. Usamos $\lfloor \frac{a}{b} \rfloor$ para o quociente da divisão

$$a = b \left\lfloor \frac{a}{b} \right\rfloor + r,\ r < b$$

No caso $r = 0$ definimos

$$\frac{a}{b} := \left\lfloor \frac{a}{b} \right\rfloor \tag{24}$$

e notemos que

$$b\frac{a}{b} = b \left\lfloor \frac{a}{b} \right\rfloor = a. \tag{25}$$

Demonstração. Sejam $a, b \neq 0$ (os outros casos ficam como exercício),

$$d := \text{mdc}(a,b)$$

e, com a notação introduzida acima

$$m := \frac{ab}{d}$$

de modo que $md = ab$. Vamos mostrar que $m = \text{mmc}(a,b)$

Notemos que $m = a\frac{b}{d} = b\frac{a}{d}$ (verifique), ou seja, $m \in M(a) \cap M(b)$. Ademais

$$\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \tag{26}$$

(verifique).

Agora, seja $c \in M(a) \cap M(b)$. Precisamos mostrar que $m \leq c$ e, para tal, provaremos que $m|c$ (teo. 21, item 6).

Por hipótese existem q e k tais que $c = qa$ e $c = kb$ então $qa = kb$ portanto, por (25), $qd\frac{a}{d} = kd\frac{b}{d}$, e usando a cancelativa, $q\frac{a}{d} = k\frac{b}{d}$, portanto temos que $\frac{a}{d} \Big| k\frac{b}{d}$.

Pelo exercício 32, item 2, $\frac{a}{d} \Big| k\frac{b}{d}$ e $\text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$ implicam $\frac{a}{d}|k$, ou seja, existe t tal que $k = t\frac{a}{d}$ donde $c = t\frac{a}{d}b = tm$, i.e., $m|c$ como queríamos. □

Exercícios

1. Faça os itens 5 e 6 do exercício 32.
2. Prove que para $a, b, c \in \mathbb{N}$ o mdc satisfaz as seguintes propriedades:
   (a) $\text{mdc}(a, b) = \text{mdc}(a, b + a \cdot c)$.
   (b) $\text{mdc}(a, c \cdot a) = a$.
3. Para quaisquer a e b, prove que se exitem n, m tais que $an - bm = 1$ então $\text{mdc}(a, b) = 1$.
4. Para quaisquer a e b, prove que se exitem $x, y \in \mathbb{N}$ que satisfazem $ax + by = \text{mdc}(a, b)$ então $\text{mdc}(x, y) = 1$
5. Determine $\text{mmc}(n, 2n + 1)$ para todo n.
6. Prove que $\text{mmc}(a, b) = ab$ se e só se $\text{mdc}(a, b) = 1$
7. $M(a) \cap M(b) = M(\text{mmc}(a, b))$?
8. Prove que se $a|m$ e $b|m$ então $\text{mmc}(a, b)|m$.
9. Prove a equação (26).

2.5 Soluções de equações diofantinas lineares

Uma *solução* para uma equação da forma

$$aX + bY = c \tag{27}$$

em que $a, b, c \in \mathbb{N}$, a e b não ambos nulos, é um par (x_0, y_0) é um par de números naturais para o qual a igualdade em (27) acima vale quando $(X, Y) = (x_0, y_0)$.

Notemos que para a ou b não-nulo temos $d = \text{mdc}(a, b) \neq 0$ e $d|ax + by$ para quaisquer naturais x e y portanto $ax + by = c$ se, e só se, $d|c$. Então

$$ax + by = c \iff \frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$$

ademais $\text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$, portanto toda equação diofantina linear

$$aX + bY = c$$

é equivalente — tem as mesmas soluções — de uma equação *reduzida*

$$\frac{a}{d}X + \frac{b}{d}Y = \frac{c}{d}$$

na qual os coeficientes são coprimos.

Uma equação $aX + bY = c$ em que $\text{mdc}(a,b) = 1$ tem solução em $\mathbb{N}$ se, e somente se, c pertence ao conjunto

$$S(a,b) = \{xa + yb\colon\ x, y \in \mathbb{N}\}$$

portanto, precisamos estudar os elementos do conjunto $S(a,b)$ ou do conjunto de lacunas de $S(a,b)$:

$$L(a,b) = \mathbb{N} \setminus S(a,b).$$

A equação $aX + bY = c$, onde $\text{mdc}(a,b) = 1$, tem solução em $\mathbb{N}$ se, e somente se, $c \notin L(a,b)$.

Primeiro notemos que $c \in S(a,b)$ se, e só se, existem *únicos* $n, m \in \mathbb{N},\ n < b$, tais que

$$c = na + mb.$$

De fato, se $c \in S(a,b)$ então $c = xa+yb$ e $x = bq+n$ com $n < b$, portanto, $c = (bq+n)a+yb = na+(qa+y)b$. A recíproca é imediata.

Proposição 34. $L(a,b) = \{na - mb \in \mathbb{N}\colon\ m, n \in \mathbb{N},\ n < b\}$.

Demonstração. Pelo exercício 32, item 2 existem naturais x, y tais que $c = (cx)a - (cy)b$ e, dividindo cx por b, temos $c = (bq + n)a - (cy)b$. Agora,

$$c = \begin{cases} na + (qa - cy)b \text{ ou} \\ na - (cy - qa)b \end{cases}$$

portanto se $c \notin S(a,b)$ então $c = na - (cy - qa)b$. □

Corolário 35. *Se $c \geq (b-1)(a-1)$, a equação $aX + bY = c$ admite solução nos naturais.*

Demonstração. Note que o conjunto $L(a,b)$ é finito e o seu maior elemento é $(b-1)a - b$. □

Teorema 36. *Suponha que a equação $aX + bY = c$, com $\text{mdc}(a,b) = 1$, tenha solução e seja $x_0 = m$, $y_0 = n$ a única solução com $m < b$. As soluções (x,y) da equação são dadas pelas fórmulas $x = m + tb$ e $y = n - ta$, para todo $t \in \mathbb{N}$ tal que $n - ta > 0$.*

3 Números primos e Teorema Fundamental da Aritmética

Um natural $p > 1$ é **primo** se os únicos divisores de p são 1 e p; se $p > 1$ não é primo então é dito **composto**; logo, por definição, se n é composto então admite um divisor d tal que $1 < d < n$, logo existe um $1 < q < n$ tal que $n = dq$.

Decorrem da definição os seguintes fatos: Se p e q são primos, então $p|q \Rightarrow p = q$. Também, se $p \nmid a$ então $\text{mdc}(a,p) = 1$.

Exercício 37. *Se $a \neq 0, 1$ e*

$$D'(a) := \{n\colon\ n > 1 \text{ e } n|a\} \tag{28}$$

então o menor elemento de $D'(a)$ é um número primo.

Solução. $D'(a) \neq \emptyset$ pois $a \in D'(a)$. Se $m := \min D'(a)$ é composto então $m = dq$ para algum d, $1 < d < m$. Como $d|m$ e $m|a$ temos, por transitividade, $d|a$.

Como m é menor elemento de $D'(a)$ e $d < m$, temos $m \notin D'(a)$, ou seja, $d \leq 1$, uma contradição. □

Proposição 38 (Proposição 30, livro VII de *Elementos* de Euclides, 300 aC)**.** *Sejam $a, b \neq 0$ naturais. Se p é primo e $p|ab$ então $p|a$ ou $p|b$.*

Demonstração. Sejam a, b, p naturais como enunciado. Se $p \not| a$ então $\text{mdc}(p, a) = 1$ e pelo exercício 32, item 3, $p|b$. Analogamente, $p \not| b \Rightarrow p|a$. □

Corolário. *Se p é primo e $p|a_1 a_2 \cdots a_n$, então $p|a_i$ para algum i. Em particular se $a_1, \ldots, a_n$ são primos então $p = a_i$.*

Demonstração. Segue por indução (verifique). □

Teorema 39 (**Teorema Fundamental da Aritmética (TFA)**)**.** *Todo natural maior que* 1 *ou é primo ou pode ser escrito de maneira única, a menos da ordem dos fatores, como um produto de primos.*

Demonstração. Provemos usando indução em n que o predicado $P(n)$:="*n ou é primo ou é produto de primos*" é verdadeiro para todo $n > 1$.

$P(2)$ é verdadeiro.

Suponha $k > 1$ é um natural e $P(n)$ é verdadeiro para todo $n \in \{2, 3, 4, \ldots, k\}$. Provaremos que $P(k+1)$ é verdadeiro. Pelo exercício 37

$$m := \min D'(k+1)$$

é primo. Se $m = k+1$, então $k+1$ é primo, senão $1 < m < k+1$ é um primo que divide $k+1$, i.e, tal que $k+1 = m \cdot q$. Como $q < k+1$, $P(q)$ é verdadeiro, ou seja, q é primo ou um produto de primos, logo $m \cdot q$ é produto de primos.

Pela 2ª forma do PIF, $P(n)$ é verdadeiro para todo $n > 1$.

Agora, provaremos que a escrita de n como produto de primos é única a menos da ordem dos fatores. Se esse não é o caso, seja n o menor natural que pode ser escrito como diferentes produtos de primos

$$n = p_1 p_2 \cdots p_a = q_1 q_2 \cdots q_b$$

com $p_1 \leq p_2 \leq \cdots \leq p_a$ e $q_1 \leq q_2 \leq \cdots \leq q_b$ primos. Então

$$p_1 | q_1 q_2 \cdots q_b$$

e pelo Corolário acima $p_1 = q_j$ para algum j, ademais $p_1 = q_j \geq q_1$. Analogamente,

$$q_1 | p_1 p_2 \cdots p_b$$

logo para algum i, $q_1 = p_i \geq p_1$. Portanto, $p_1 = q_1$.

Pela minimalidade de n,

$$p_2 \cdots p_a = q_2 \cdots q_b \Rightarrow a = b \text{ e } p_i = q_i$$

uma contradição. □

Assim, para todo $n > 1$ existem $p_1 < p_2 < \cdots < p_k$ primos e $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N} \setminus \{0\}$ *univocamente determinados* tais que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{29}$$

que chamamos de **fatoração canônica de** n em primos. Reforçando, essa descrição de n *é única*. Por exemplo

$$84 = 2^2 \cdot 3 \cdot 7, \quad 120 = 2^3 \cdot 3 \cdot 5 \quad \text{e} \quad 350 = 2 \cdot 5^2 \cdot 7$$

As vezes usamos o expoente 0 em fatores primos quando queremos, por exemplo, escrever dois inteiros diferentes como produto dos mesmos primos. Assim

$$2^3 \cdot 3^2 \cdot 7 \cdot 11 = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 13^0 \cdot 17^0$$
$$2 \cdot 5^2 \cdot 13 \cdot 17 = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13^1 \cdot 17^1$$

Proposição 40. *Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $d > 1$ divide n então $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ com $0 \leq \beta_i \leq \alpha_i$ para todo i.*

Esboço da demonstração. Para cada primo p, se $p^\beta | d$ e $d | n$ então $p^\beta | n$. Como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ temos $p^\beta | p_i^{\alpha_i}$ para algum i, portanto, $p = p_i$ e $0 \leq \beta_i \leq \alpha_i$. □

Exercício 41. *Considere os naturais $a, b > 1$ com as respectivas fatorações $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ (aqui permitimos expoentes nulos). Defina para cada i*

$$\gamma_i := \max\{\alpha_i, \beta_i\}$$

$$\delta_i := \min\{\alpha_i, \beta_i\}$$

e prove que

$$\text{mdc}(a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$$
$$\text{mmc}(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}.$$

Exercício 42. *Quantos divisores tem n, para qualquer $n > 1$?*

Solução.

$$d(n) := (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1) \tag{30}$$

□

Exercício 43. *$d(n)$ é ímpar se, e só se, n é um quadrado perfeito.*

Solução. $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$

$$\begin{aligned} d(n) \text{ ímpar} &\Leftrightarrow \alpha_i + 1 \text{ ímpar } (\forall i) \\ &\Leftrightarrow \alpha_i \text{ par } (\forall i) \\ &\Leftrightarrow n = \left(p_1^{\frac{\alpha_1}{2}}\cdots p_r^{\frac{\alpha_r}{2}}\right)^2 \end{aligned}$$

□

Para $n \neq 0$ e p primo $E_p(n)$ denota o expoente da maior potência de p que divide n.

Proposição 44. *Se m, n são naturais então*

$$m = n \Longleftrightarrow E_p(m) = E_p(n)$$

para todo p primo.

Demonstração. A proposição $m = n \Rightarrow E_p(m) = E_p(n)$ é imediata.

Suponha que $E_p(m) = E_p(n)$ e considere os conjuntos

$$\begin{aligned} \mathscr{P}_m &:= \{p \text{ primo} : E_p(m) > 0\} = \{p \text{ primo} : E_p(n) > 0\} =: \mathscr{P}_n \\ \mathscr{E}_m &:= \{E_p(m) : p \in \mathscr{P}_m\} = \{E_p(n) : p \in \mathscr{P}_n\} =: \mathscr{E}_n. \end{aligned}$$

Se $\mathscr{P}_m = \emptyset = \mathscr{P}_n$ então $m = n = 1$, senão

$$\mathscr{P}_m = \{p_1, \ldots, p_k\} = \mathscr{P}_n$$

e como $E_{p_i}(m) = E_{p_i}(n)$ para todo i, temos $m = n$. □

Assim, vale que para todo primo p

$$E_p\big(\text{mdc}(m,n)\big) = \min\big\{E_p(m), E_p(n)\big\}$$

$$E_p\big(\text{mmc}(m,n)\big) = \max\big\{E_p(m), E_p(n)\big\}.$$

3.1 A distribuição dos números primos

Historicamente, um problema que recebe atenção considerável por parte dos matemáticos é o da distribuição dos números primos no conjunto dos números naturais. A distribuição dos números primos dentro de $\mathbb{N}$ tem muitos problemas desafiadores, como a conjectura dos primos gêmeos, da infinitude de números de Fibonacci (respec., de Mersenne) que são primos. Além desses, existe um primo entre n^2 e $(n+1)^2$? Existem infinitos primos da forma $n^2 - n + 41$? São perguntas difíceis de responder a respeito da distribuição dos primos.

Seja

$$p_1, p_2, p_3, \ldots, p_n, \ldots$$

a sequência dada por todos os números primos em ordem crescente. Primeiro, provaremos que a sequência é ilimitada.

Teorema 45 (Euclides)**.** *Há infinitos números primos.*

Demonstração. Se $p_1, p_2, \ldots, p_r$ são todos os números primos então

$$n = p_1 p_2 \cdots p_r + 1$$

pode ser escrito como o produtos desses primos, mas se $p_i | n$ então $p_i | 1$, um absurdo. □

Exercício 46. *Prove que $p_n \leq 2^{2^{n-1}}$. (Dica: indução e $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$)*

Outra demonstração do teorema de Euclides. Vamos mostrar que para todo natural n existe um primo maior que n. Para tal, tome p um fator primo do número $n! + 1$. Se $p \leq n$ então $p | n!$ por definição de fatorial. Se p divide $n!$ e $n! + 1$ então p divide a diferença desses números, i.e., $p | 1$, portanto $p = 1$, um absurdo que estabelece $p > n$. □

Prova de Krummer. Se $p_1, p_2, \ldots, p_r$ são todos os números primos então o número $n = p_1 p_2 \cdots p_r > 2$ e $n - 1$ tem um divisor primo p_i em comum com n, então $p_i | n - (n-1)$, i.e., $p_i | 1$, uma contradição. □

Sabemos que há primos consecutivos arbitrariamente distantes:

Proposição 47. *Para todo natural $n > 1$, existem n naturais consecutivos e compostos.*

Demonstração. Dado n, tomemos a sequência de n números consecutivos

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n + 1$$

é divisível, respectivamente, por $2, 3, \ldots, n+1$, portanto, nenhum é primo. □

Por outro lado, conhecemos pares (p_n, p_{n+1}) de primos consecutivos que estão o mais próximo possível $p_{n+1} - p_n = 2$. Esse primos são chamados de **primos gêmeos**. Por exemplo, são primos gêmeos

$$(3,5),(5,7),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73),(101,103),(107,109)$$

É atribuído a Euclides a seguinte conjectura

Conjectura dos primos gêmeos. *Há infinitos primos gêmeos.*

Em geral sabemos pouco sobre o comportamento de $p_{n+1} - p_n$. Até recentemente não se sabia se $\liminf(p_{n+1} - p_n)$ é finito, quando em 2013 Zhang mostrou que $\liminf(p_{n+1} - p_n) < 70.000.000$ num trabalho que surpreendeu a comunidade dos especialistas em Teoria dos Números; esse limitante tem sido melhorado e no momento vale $\liminf(p_{n+1} - p_n) < 246$ (de fato, menor que 6 sob certa hipótese que não se sabe ainda se é verdadeira). Se se conseguir reduzir para 2, a conjectura dos primos gêmeos fica provada.

Crivo de Eratóstenes

Os números primos até n podem ser obtidos por um método conhecido como Crivo de Eratóstenes (curador da biblioteca de Alexandria).

Lema 48 (Eratóstenes, 230 ac)**.** *Se $n > 1$ não é divisível por nenhum dos primos p tais que $p^2 \leq n$ então n é primo.*

Demonstração. Se n é composto então tomamos q o menor primo que divide n. Então $n = qm$ com $q \leq m$, logo $q^2 \leq mq = n$ e $q|n$, uma contradição. □

Notação $\lfloor \sqrt{n} \rfloor := \max\{x \in \mathbb{N} \colon x^2 \leq n\}$.

Os números primos até n podem ser obtidos por

1. Liste todos os números de 2 até n
2. Para cada $i \in \{2,3,\ldots,\lfloor \sqrt{n} \rfloor\}$: se i está na lista então apague os múltiplos de i maiores que i.

Por exemplo, para conhecer os primos menores que 60 excluímos das lista $2,\ldots,60$ os múltiplos de 2, 3, 5, 7.

Os naturais que sobram depois desse processo não são divisíveis pelos naturais $x \in \{2,3,\ldots,\lfloor \sqrt{n} \rfloor\}$ para os quais vale que $x^2 \leq n$ por definição de $\lfloor \sqrt{n} \rfloor$.

	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120

Figura 1: Primos até 120 pelo crivo de Eratóstenes.

Densidade de primos — o teorema dos números primos

Denotemos por $\pi(x) : \mathbb{R}^+ \to \mathbb{N}$ a quantidade de números primos que são menores ou iguais a x. Por exemplo

x	0	1	2	3	4	5	6	7
$\pi(x)$	0	0	1	2	2	3	3	4

Claramente $\pi(p_n) = n$ e, de forma geral, $\pi(x) = n$ se $p_n \leq x < p_{n+1}$.

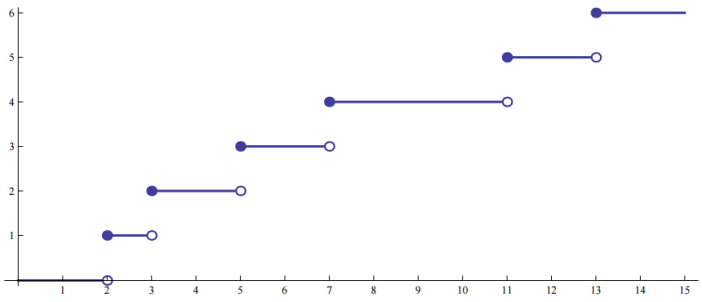


Figura 2: gráfico de $\pi(x)$, $0 \leq x \leq 15$.

A função $\pi(x)$ foi estudada por vários matemáticos notáveis antes que uma aproximação razoável para ela fosse encontrada e devidamente demonstrada.

Comecemos derivando um limitante inferior para $\pi(x)$ a partir do exercício 46. Para todo x, se $2^{2^n} \leq x < 2^{2^{n+1}}$ então $n \leq \log_2(\log_2 x) < n+1$ e $\pi(x) \geq \pi(2^{2^n}) \geq \pi(p_n) = n$, portanto,

$$\pi(x) \geq \log_2(\log_2 x).$$

Um dos primeiros matemáticos a se dedicar ao estudo de $\pi(x)$ foi o matemático suíço Leonhard Euler

que, por volta de 1735, verificou a identidade para todo $k > 1$

$$\sum_{n=1}^{\infty} \frac{1}{n^k} = \left(\sum_{\alpha_1 \geq 0} \frac{1}{2^{k\alpha_1}}\right)\left(\sum_{\alpha_2 \geq 0} \frac{1}{3^{k\alpha_2}}\right)\cdots\left(\sum_{\alpha_r \geq 0} \frac{1}{{p_r}^{k\alpha_2}}\right)\cdots \qquad = \prod_{i=1}^{\infty}\left(\sum_{\alpha_i \geq 0} \frac{1}{p_i^{k\alpha_i}}\right) \Rightarrow$$

$$\sum_{n=1}^{\infty} \frac{1}{n^k} = \prod_{i=1}^{\infty} \frac{1}{1 - \frac{1}{{p_i}^k}}. \tag{31}$$

Para $k = 1$ o lado esquerdo da equação acima diverge.

Prova de Euler para o teorema de Euclides. Fixe $k = 1$ em (31). Se a quantidade de primos é finita então o lado esquerdo de (31) diverge enquanto que o lado direito é finito, uma contradição. □

Euler ainda mostrou que $\sum_p 1/p$ diverge e que, por isso, há infinitos números primos. Mais que isso, como $\sum_n 1/n^2$ converge, então deve haver mais primos que quadrados, o mesmo vale para cubos, etc, logo $\pi(x) > x^{1-\varepsilon}$ para qualquer $\varepsilon > 0$.

Mais uma demonstração do teorema de Euclides, agora usando Cálculo. Para todo $x \in [n, n+1]$ temos

$$\int_1^x \frac{1}{t}\,\mathrm{d}t \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \sum_{m \in R_x} \frac{1}{m}$$

onde $R_x := \{m \in \mathbb{N} : p|m \text{ e } p \text{ primo } \Rightarrow p \leq x\}$. Como todo $m \in R_x$ é escrito de forma única como $\prod_{p \leq x} p^{\alpha_p}$ temos

$$\sum_{m \in R_x} \frac{1}{m} = \prod_{p \leq x}\left(\sum_{k \geq 0} \frac{1}{p^k}\right)$$

com

$$\sum_{k \geq 0} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}$$

portanto

$$\sum_{m \in R_x} \frac{1}{m} = \prod_{p \leq x}\left(\frac{1}{1 - \frac{1}{p}}\right) = \prod_{i=1}^{\pi(x)}\left(\frac{p_i}{p_i - 1}\right)$$

e de $p_i \geq i + 1$ temos $p_i/(p_i - 1) \leq (i+1)/i$ consequentemente

$$\prod_{i=1}^{\pi(x)}\left(\frac{p_i}{p_i - 1}\right) \leq \prod_{i=1}^{\pi(x)}\left(\frac{i+1}{i}\right) = \pi(x) + 1$$

portanto,

$$\ln(x) = \int_1^x \frac{1}{t}\,\mathrm{d}t \leq \pi(x) + 1$$

e como $\ln(x)$ não é limitado, $\pi(x)$ também não é, isto é, $\pi(x) \to \infty$ quando $x \to \infty$. Isso prova que há infinitos números primos. □

Da demonstração acima

$$\pi(x) > \ln(x/e).$$

Legendre e Gauss, independentemente, analisando tabelas de primos chegaram à conclusão de que

$$\pi(x) \approx \frac{x}{\ln(x)}$$

e Chebyshev foi primeiro a dar uma prova definitiva para a ordem de grandeza de $\pi(x)$

$$0{,}92 < \frac{\pi(x)}{\frac{x}{\log(x)}} < 1{,}11$$

além de mostrar que se o limite de $\pi(x)/x\log(x)^{-1}$ existe quando $x \to \infty$, então o limite é 1.

Por volta de 1900, Hadamard e de la Vallée-Poussin, independentemente, provaram o profundo resultado chamado de Teorema dos Números Primos e cujo enunciado simplesmente é

Teorema (Teorema dos Números Primos)**.**

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1. \tag{32}$$

□

x	$\pi(x)$	$\frac{x}{\log x}$	$\pi(x)/(\frac{x}{\log x})$
10	4	4.34	0.92103
10^2	25	21.71	1.15129
10^3	168	144.76	1.16050
10^4	1229	1085.74	1.13195
10^5	9592	8685.89	1.10432
10^6	78498	72382.41	1.08449
10^7	664579	620420.69	1.07117
10^8	5761455	5428681.02	1.06130
10^9	50847534	48254942.43	1.05373

Figura 3: comparação da aproximação dada no teorema.

Esse resultado tem uma justificativa heurística que para $x \geq 2$, a probabilidade de que um natural em $[1, x]$ não seja divisível por p é $(1 - 1/p)$ portanto, assumindo independência (que, de fato, não vale) temos que a probabilidade de p ser primo é $\prod_{p\leq x}(1 - 1/p) \leq 1/\ln(x)$.

Exercício 49. *Deduza do teorema dos números primos que* $p_n \sim n\ln(p_n) \sim n\ln n$ *onde* $a_n \sim b_n$ *significa que* $a_n/b_n \to 1$ *quando* $n \to \infty$.

3.1.1 A Hipótese de Riemann

Em 1859, Bernhard Riemann, foi eleito para a Academia das Ciências de Berlim onde apresentou a monografia *Sobre o número de números primos que não excedem uma grandeza dada.* É aqui que surge a hipótese de Riemann, um dos mais famosos, senão o mais famoso, problema em aberto da Matemática, um um dos Problemas do Milênio do *Clay Mathematics Institute* que oferece um prêmio de 1 milhão pra quem resolvê-lo.

A função **zeta de Riemann** é a função

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

para $s \in \mathbb{C}$ que, quando $\mathrm{Re}(s) > 1$, converge e vale (veja a equação (31))

$$\zeta(s) = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}}.$$

Riemann provou que essa função pode ser estendida para $s \in \mathbb{C} \setminus \{1\}$. A hipótese de Riemann diz respeito aos zeros desta função fora do domínio da convergência

Hipótese de Riemann, 1859. *Se* $\zeta(s) = 0$ *com* $0 \le \mathrm{Re}(s) \le 1$ *então* $\mathrm{Re}(s) = 1/2$.

É possível provar que não há zero no eixo $\mathrm{Re}(s) = 1$, esse resultado é equivalente ao teorema do números primos.

Como uma consequência das muitas consequências da veracidade da hipótese de Riemann na Teoria dos Números citamos a precisão no erro da distribuição

$$\left| \pi(x) - \int_0^x \frac{1}{\ln t}\, \mathrm{d}t \right| \le \frac{1}{8\pi} \sqrt{x} \ln(x) \qquad \forall x \ge 2657$$

de fato, a hipótese de Riemann é equivalente a $\pi(x) = \int_0^x \frac{1}{\ln t}\, \mathrm{d}t + O(\sqrt{x}\ln(x))$.

3.2 Primos em sequências numéricas

De um modo geral, vamos investigar problemas da seguinte forma: dada uma sequência $a_0, a_1, \ldots$ de números naturais, nela ocorrem infinitos primos? A seguir veremos alguns resultados e algumas conjeturas para sequências conhecidas.

Exemplo 50. *Considere a sequência de Fibonacci:* $f_0 = 0$, $f_1 = 1$ *e* $f_n = f_{n-1} + f_{n-2}$ *para* $n > 1$. *Um* ***primo de Fibonacci*** *é um elemento dessa sequência que é primo. Não sabemos responder*

Existem infinitos primos de Fibonacci?

Os primeiros primos de Fibonacci são

$$2, 3, 5, 13, 89, 233, 1597, 28657, 514229, 433494437, 2971215073$$

e o maior primo de Fibonacci conhecido até 2017 é $f_{2904353}$.

Exercício 51. *Prove que se $a|b$ então $f_a|f_b$ e, portanto, para todo $a > 4$ todo primo de Fibonacci tem índice primo.*

Exercício 52. *Prove que* $\text{mdc}(f_a, f_b) = f_{\text{mdc}(a,b)}$.

A partir do exercício anterior, podemos provar (de novo) a infinitude de primos. Suponha que $p_1, p_2, \ldots, p_k$ são todos os primos. Então, cada elemento de $f_{p_1}, f_{p_2}, \ldots, f_{p_k}$ deve ser divisível por um primo diferente porque $\text{mdc}(f_{p_i}, f_{p_j}) = 1$, para $i \neq j$. Pelo Princípio das Gavetas (ou casa dos pombos) cada f_{p_i} é divisível por um único primo p_j, mas $f_{19} = 37 \cdot 113$ não é desta forma, uma contradição.

Números de Fermat

Os *números Fermat* são definidos por $F_n = 2^{2^n} + 1$ para todo $n \geq 0$. Os primeiros números dessa sequência são

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617$$

Em 1640 Fermat mostrou que F_n é primo para $n \in \{0, 1, 2, 3, 4\}$ e até 2017 esses são os únicos primos de Fermat conhecidos. Fermat ainda conjeturou que esses números eram primos até que em 1732 Euler mostrou que F_5 é composto. Atualmente não sabemos responder

1. *F_n é composto para todos $n > 4$?*
2. *Existem infinitos de primos de Fermat?* (Eisenstein 1844)
3. *Existem infinitos números compostos de Fermat?*
4. *Existe um número de Fermat que não é livre de quadrados?*

Exercício 53. *Complete o seguinte argumento para dar uma prova da infinitude de números primos: Os números de Fermat satisfazem a recursão $\prod_{i=0}^{n-1} F_i = F_n - 2$ para todo $n \geq 1$ (prove). Ademais F_n e F_m são coprimos para $n \neq m$ (exemplo 31). Assim, existem infinitos números primos (prove).*

Números de Mersenne

Os maiores primos conhecidos ao longo da história tem sido, quase sempre, números de Mersenne. Isso ocorre devido à forma eficiente como é comprovada a primalidade de números de Mersenne.

Um *número de Mersenne* é um número da forma $M_n = 2^n - 1$, para $n > 1$, se M_n é primo então é chamado *primo de Mersenne*.

Exercício 54. *Prove que se n é composto então M_n é composto.*

Portanto, decorre desse exercício que os primos de Mersenne são os primos M_p para p primo.
Atualmente não sabemos responder

1. *Existem infinitos de primos de Mersenne*?
2. *Existem infinitos primos para os quais M_p é composto*?
3. *Existem infinitos primos para os quais M_p é primo*?

Primos de Mersenne têm uma história longa, os pitagóricos batizaram de *perfeito* todo número n tal que a soma dos divisores positivos vale $2n$, por exemplo 6, 28 e 496 são perfeitos. Euclides notou que *se M_p é primo então $2^{p-1}M_p$ é perfeito*. Não é difícil provar quer todo número perfeito par é da forma $2^{p-1}M_p$ para p primo e M_p primo. A seguinte conjectura é uma das mais antigas da matemática.

Conjetura. *Não existe número perfeito ímpar.*

3.2.1 Primos em progressões aritméticas

Um teorema famoso da Teoria Analítica dos Números, o Teorema de Dirichlet, afirma que

Teorema 55. *A progressão aritmética que começa em a e tem razão d*

$$a, a+d, a+2d, a+3d, \ldots, a+nd, a+(n+1)d, \ldots$$

para quaisquer a, d coprimos, contém infinitos números primos. □

A demonstração deste resultado é bem difícil. Nos limitamos no texto a demonstrar alguns casos particulares do teorema de Dirichlet.

Proposição 56. *Há infinitos primos da forma $4k+3$.*

Demonstração. A prova é um exercício com o seguinte roteiro:

1. Todo primo ímpar é da forma $4k+1$ ou $4k+3$.
2. O produto de dois números da forma $4k+1$ também é dessa forma.
3. Para quaisquer $p_1, \ldots, p_r \in \mathbb{N}\setminus\{0\}$, $N = 4(p_1 \cdots p_r) - 1$ é da forma $4k+3$ e existe um primo p da forma $4k+3$ tal que $p|N$.
4. Suponha que na descrição de N os naturais $p_1, \ldots, p_r$ acima sejam todos os primos da forma $4k+3$. Determine a existência de um primo da forma $4k+3$ que não seja nenhum dos listados acima.

□

Lema 57. *Para todo natural $m \geq 2$, todo divisor ímpar de m^2+1 é da forma $4k+1$.*

Demonstração. Seja p um primo maior que 2 que divide m^2+1. Então $m^2+1 = pt$, logo $m^2 = pt-1$, portanto, como $p-1$ é par

$$(m^2)^{\frac{p-1}{2}} = (pt-1)^{\frac{p-1}{2}} \Rightarrow m^{p-1} = \begin{cases} xp+1, & \text{se } \frac{p-1}{2} \text{ par} \\ yp-1, & \text{se } \frac{p-1}{2} \text{ ímpar} \end{cases}$$

pelo teorema do binômio de Newton. De $m^{p-1} = yp-1$ então $m^{p-1}-1 = yp-2$. Ainda $p \nmid m$ pois, caso contrário, de $p|m^2+1$ teríamos $p|1$. Pelo PTF, $p|m^{p-1}-1$, logo $p|yp-2$, portanto $p|2$, uma contradição. Portanto, $\frac{p-1}{2}$ é par e p é da forma $4k+1$. □

Proposição 58. *Há infinitos primos da forma $4k+1$.*

Demonstração. Suponha, por absurdo, que $p_1, \ldots, p_k$ são todos os primos da forma $4n+1$. Considere o número $a = 4p_1^2 \cdots p_k^2 + 1$. Como $p_i \nmid a$ para todo $i = 1, \ldots, k$, segue que todo divisor primo de a é da forma $4n+3$, o que é um absurdo, em vista do lema 57 acima. □

Proposição 59. *Há infinitos primos da forma $6k+5$.*

Demonstração. Exercício. Dica: suponha finitos e forme $q = 6p_1p_2p_3 \ldots p_r - 1 = 6(p_1p_2p_3 \ldots p_r - 1) + 5$. □

Lema 60. *Não existe uma progressão aritmética formada apenas por números primos.*

Demonstração. Seja $a_n = a+nb$ uma progressão aritmética e3 assuma que a_m é primo. Defina a sequência $b_k = m + ka_m$, $k \geq 1$ e temos

$$a_{b_k} = a + (b_k)b = a + (m+ka_m)b = a + mb + ka_mb = a_m + ka_mb$$

é divisível pelo primo a_m. □

Em 2004, Terence Tao e Ben Green provaram uma conjectura conhecida desde 1770

Teorema 61. *Para todo inteiro $k \geq 1$, os primos contém um progressão aritmética formada por k termos.*

□

3.3 Pequeno Teorema de Fermat (PTF)

Para $0 \leq b \leq a$, é possivel provar que $(b!(a-b)!) \mid b!$ (exercício). Definimos

$$\binom{a}{b} := \frac{a!}{b!(a-b)!} \tag{33}$$

e vale para todo n (outro exercício)

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}. \tag{34}$$

Exercício 62. *Se p é primo então $\binom{p}{i}$ é divisível por p para todo $0 < i < p$.*

Solução. Para $i = 1$ é trivial. Fixe um i, $1 < i < p$. Da equação (33) temos que $i!$ divide $\frac{p!}{(p-i)!} = p(p-1)\cdots(p-i+1)$. Como p não é um fator primo de $i!$ temos $i!|(p-1)\cdots(p-i+1)$, portanto

$$\binom{p}{i} = pq$$

onde $q = \frac{(p-1)\cdots(p-i+1)}{i!}$. □

Teorema 63 (**Pequeno Teorema de Fermat**)**.** *Se p é primo então $p|(a^p - a)$ para todo $a \geq 1$.*

Demonstração. Para $a = 1$ a afirmação certamente vale. Suponha que vale para a e vamos provar que vale para $a+1$.

$$(a+1)^p - (a+1) = \sum_{i=0}^{p} \binom{p}{i} a^i 1^{p-i} - (a+1) = (a^p - a) + \sum_{i=1}^{p-1} \binom{p}{i} a^i 1^{p-i}$$

e como $p|(a^p - a)$ e $p|\binom{p}{i}$ $(0 < i < p)$ temos $p|[(a+1)^p - (a+1)]$. □

Notemos que $p|(a^p - a) \Rightarrow p|a(a^{p-1} - 1)$, portanto, se $p \nmid a$ então $p|(a^{p-1} - 1)$

Corolário 64 (também chamado de **Pequeno Teorema de Fermat**)**.** *Se p é primo e $p \nmid a$, então $p|(a^{p-1} - 1)$.* □

Exemplo. *Se $p \neq 2, 5$ é primo, p divide algum número dentre $1, 11, 111, 1111, 11111, 111111, 1111111, \ldots$. Se $p = 3$ então p divide todo número com quantidade divisível por 3 de algarismos 1. Se $p > 5$ então $\text{mdc}(10, p) = 1$ portanto $p|10^{p-1} - 1 = 9 \cdot 1111\cdots11$ e como $p \nmid 9$ temos $p|1111\cdots11$.*

Exemplo. $10|(n^9 - n)$*. Como n^9 e n têm a mesma paridade, $2|(n^9 - n)$. Vamos verificar que $5|(n^9 - n)$ que, como $\text{mdc}(2,5) = 1$, concluímos que $10|n^9 - n$.*

$$n^9 - n = n(n^4 - 1)(n^4 + 1) = (n^5 - n)(n^4 + 1)$$

O PTF garante que $5|(n^5 - n)$, portanto $10|(n^9 - n)$; em outras palavras n^9 e n têm o mesmo algarismo da unidade em base 10.

De acordo com o teorema de Fermat, dados inteiros n e a, se n é primo e não divide a então $a^{n-1} \bmod n = 1$, portanto, qualquer outro resultado indica que n é composto. Entretanto, o teorema não garante que se $a^{n-1} \bmod n = 1$ então n é primo.

Por exemplo $2340 \bmod 341 = 1$ mas $341 = 11 \cdot 31$ não é primo. Em algumas referências tais números são ditos pseudo-primos de Fermat. Um número inteiro ímpar e composto n é um pseudo-primo para a base a se $a^{n-1} \bmod n = 1$. Assim, 341 é pseudo-primo para a base 2. De fato, é o menor pseudo-primo para a base 2. Podemos descobrir que 341 é composto testando-o contra outras bases e nesse caso $3340 \bmod 341 = 54$ o que atesta que 341 é composto. Entretanto, estender essa estratégia não produz um algoritmo eficiente para decidir primalidade. Não há números que sejam pseudo-primos para toda base $a \in \{2, \ldots, n-2\}$ pois se $\text{mdc}(a,n) > 1$ então $a^{n-1} \bmod n \neq 1$. Isso garante que se incrementamos a base e fazemos o teste de Fermat então o mais longe que iremos é até o menor divisor primo de n, mas isso pode não ser muito mais eficiente do que usar crivo de Eratóstenes.

Seja a um natural coprimo a 3, 11 e 17. Portanto a e $3 \cdot 11 \cdot 17 = 561$ são coprimos. Ainda,

$$(a^{280}, 3) = (a^{56}, 11) = (a^{35}, 17) = 1$$

pelo Pequeno Teorema de Fermat, $3|(a^{280})^2 - 1$, $11|(a^{56})^{10} - 1$ e $17|(a^{35})^{16} - 1$. Segue-se daí que 561 divide $a^{560} - 1$, para todo a comprimo com 561, que não é primo.

Exercícios

1. Para quais valores de m e n o número $9^m 10^n$ tem 27 divisores?
2. Qual é a forma geral de um número que tem só mais um divisor além do 1 e dele mesmo?
3. Prove que se $\text{mdc}(n,m) = 1$ então $d(n \cdot m) = d(n)d(m)$.
4. Verifique as afirmações.
   (a) 287 é primo.
   (b) Todo primo da forma $3k+1$ é da forma $6q+1$.
   (c) Entre n e $n!$ existe um primo.(Dica: considere $n! - 1$)
   (d) Todo primo maior que 6 é da forma $6k+1$ ou $6k+5$.
   (e) O único primo da forma $n^3 - 1$ é 7.
5. Mostre que há infinitos primos da forma $8k+5$.
6. Se a soma de dois naturais não-nulos é primo, esses números são coprimos?

7. Vamos mostrar que há infinitos primos estabelecendo que $\pi(n) \geq \frac{1}{2}\log_2(n)$.

   (a) Dizemos que r é livre de quadrado se não tem um divisor diferente do 1 que é um quadrado perfeito. Equivalentemente, $r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ com $\alpha_i = 0, 1$ para cada i. Prove que a quantidade de naturais menores ou iguais a n livres de quadrado é no máximo $2^{\pi(n)}$.

   (b) Prove que todo $m \leq n$ é da forma $m = s^2 \cdot r$, com r livre de quadrado e $s^2 \leq m$.

   (c) Use os itens anteriores para provar que $n \leq 2^{\pi(n)} \lfloor \sqrt{n} \rfloor$.

   (d) Prove que $\pi(n) \geq \frac{1}{2}\log_2(n)$.

4 Construção dos Inteiros

Intuitivamente, digamos que queremos construir um conjunto de números onde $n - k$ faça sentido quaisquer que sejam os naturais n, k, por exemplo $4 - 11$. Façamos $-7 := 4 - 11$. Mas então há várias representações $-7 := 4 - 11 = 3 - 10 = 5 - 12 = \cdots$. Notemos que se $a - b = n - m$ então $a + m = b + n$ e s e fizermos todas essas representações do -7 equivalentes temos um velho conhecido, a relação de equivalência do exercício 4.

Formalmente, considere a relação $\mathbf{Z} \subset \mathbb{N} \times \mathbb{N}$ definida por

$$(a, b)\mathbf{Z}(n, m) \text{ se, e só se } a + m = b + n$$

$\mathbf{Z}$ é uma relação de equivalência (exercício 4, página 4).

Para cada (a, b), a *classe de equivalência de* (a, b) é o conjunto

$$[(a, b)] := \{(n, m) \in \mathbb{N} \times \mathbb{N} \colon (a, b)\mathbf{Z}(n, m)\}. \tag{35}$$

Por exemplo,

$$[(1,2)] = \{(0,1), (1,2), (2,3), (3,4), \ldots\}$$

$$[(5,2)] = \{(3,0), (4,1), (5,2), (6,3), \ldots\}$$

Notemos que $[(1,2)] = [(2,3)] = [(0,1)] \neq [(5,2)] = [(4,1)]$.

Quando denotamos a classe de equivalência para $\{(0,1), (1,2), (2,3), (3,4), \ldots\}$ por $[(2,3)]$ dizemos que o par $(2,3)$ é o *representante* da classe.

$\mathbb{Z}$ é o conjunto dessas classes de equivalência e seus elementos são chamados números inteiros.

Denotamos

$$0 := [(0,0)] = \{(n,n) : n \in \mathbb{N}\}$$
$$1 := [(1,0)] = \{(n+1,n) : n \in \mathbb{N}\}$$
$$-1 := [(0,1)] = \{(n,n+1) : n \in \mathbb{N}\}$$
$$-a := [(0,a)] = \{(n,n+a) : n \in \mathbb{N}\}$$

Denotamos por $\mathbb{Z}^+ := \{1,2,3,4,\ldots\}$ o conjunto dos números inteiros *positivos*, i.e., inteiros *maiores que* 0. O conjunto $\mathbb{Z} \setminus \mathbb{Z}^+$, dos inteiros *menores ou iguais a* 0 são ditos *não-positivos*. Denotamos os inteiros *negativos* por $\mathbb{Z}^- := \{-1,-2,-3,-4,\ldots\}$ e definimos de modo análogo os inteiros *não-negativos*. Assumimos a identificação

$$\mathbb{Z} \setminus \mathbb{Z}^- = \mathbb{N}$$

Denotemos por p a classe $[(a,b)]$ e por q a classe $[(n,m)]$. Definimos $p+q$ como a classe de equivalência

$$p + q := [(a+n, b+m)] \tag{36}$$

Notemos que $[(1,2)] + [(5,2)] = [(0,1)] + [(3,0)]$. Definimos $p \cdot q$ como a classe de equivalência

$$p \cdot q := [(a \cdot n + b \cdot m, a \cdot m + b \cdot n)] \tag{37}$$

Definimos

$$p - q := p + (-q)$$

e definimos

$$p \leq q \Leftrightarrow q - p \in \mathbb{N} \tag{38}$$

para quaisquer inteiros p e q.

Exercícios

1. Prove que a soma de conjuntos definida acima é compatível com a relação de equivalência, isto é, a soma não depende dos representantes de cada classe de equivalência envolvida.

2. Prove que a multiplicação de conjuntos definida acima é compatível com a relação de equivalência, isto é, não depende dos representantes de cada classe de equivalência envolvida.

3. Para classes de equivalência p, q, r e as operações definidas acima valem

(a) $p + (q + r) = (p + q) + r$

(b) $p + q = q + p$

(c) $p + 0 = p$

(d) $p + (-p) = 0$

(e) $p \cdot (q \cdot r) = (p \cdot q) \cdot r$

(f) $p \cdot q = q \cdot p$

(g) $p \cdot 1 = p$

(h) $p \cdot (q + r) = p \cdot q + p \cdot r$

(i) $p \cdot q = 0 \Rightarrow p = 0$ ou $q = 0$

4. A relação $\leq$ é uma **ordem total**: é uma relação reflexiva, antissimétrica e transitiva. Além, disso quaisquer dois inteiros p e q são **comparáveis**, isto é, vale: $p \leq q$ ou $q \leq p$.

5. Prove que

   (a) $p \leq 0 \Rightarrow -p \geq 0$

   (b) $(-p) \cdot q = -(p \cdot q)$

5 Inteiros e suas propriedades aritméticas e de ordem

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

é o conjunto dos números inteiros que munidos das funções (operações) soma e produto $+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ e da ordem total $\leq$ (definida em (38)) satisfazem as seguintes 11 propriedades abaixo que podem ser provadas a partir da construção dos inteiros. Alternativamente, podemos tomar essas 11 propriedades como princípios (axiomas) que a teoria derivada a partir deles é a mesma que a teoria derivada a partir da construção dos inteiros.

5.1 Com relação a soma

1. Associativa $\forall a, b, c \in \mathbb{Z}$

$$a + (b + c) = (a + b) + c$$

2. Comutativa $\forall a, b \in \mathbb{Z}$

$$a + b = b + a$$

3. Elemento neutro $\forall a \in \mathbb{Z}$,

$$a + 0 = a$$

e 0 é o único inteiro que satisfaz essa sentença.

4. Elemento inverso $\forall a \in \mathbb{Z}$, $\exists! b \in \mathbb{Z}$

$$a + b = 0$$

b é denotado por $-a$.

Exercício 65 (Lei cancelativa). $\forall a, b, c \in \mathbb{Z}$

$$a + b = a + c \iff b = c$$

Exercício 66. $\forall a, b \in \mathbb{Z}$

$$-(a + b) = (-a) + (-b) = -a - b$$

5.2 Com relação ao produto

5. Associativa $\forall a, b, c \in \mathbb{Z}$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

6. Comutativa $\forall a, b \in \mathbb{Z}$

$$a \cdot b = b \cdot a$$

7. Elemento neutro $\forall a \in \mathbb{Z}$

$$a \cdot 1 = a$$

e 1 é o único inteiro que satisfaz essa sentença.

8. Distributiva $\forall a, b, c \in \mathbb{Z}$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

9. Lei cancelativa $\forall a, b, c \in \mathbb{Z}$

$$b = c \Rightarrow a \cdot b = a \cdot c$$

$$a \neq 0 \text{ e } a \cdot b = a \cdot c \Rightarrow b = c$$

Exercício 67. *Para quaisquer* $a, b, c \in \mathbb{Z}$

1. $-(-a) = a$
2. $a \cdot 0 = 0$.

3. $(-a)\cdot b = -(a\cdot b) = a\cdot(-b)$.

4. $c(a-b) = ca - cb$.

Exercício 68 (Anulamento). $\forall\, a, b \in \mathbb{Z}$

$$a\cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Exercício 69. *Prove que a lei cancelativa e a propriedade do anulamento são equivalentes.*

5.3 Com relação à ordem $\leq$

10. Tricotomia $\forall\, a, b \in \mathbb{Z}$ vale só um de

$$a < b \text{ ou } a = b \text{ ou } b < a.$$

Exercício 70 (Compatibilidade de $\leq$ com as operações aritméticas). *Para $a, b, c \in \mathbb{Z}$ valem*

1. $a \leq b \Leftrightarrow a + c \leq b + c$

2. *se $c \in \mathbb{N}$ então $a \leq b \Leftrightarrow a\cdot c \leq b\cdot c$.*

Exercício 71. *Para quaisquer inteiros a, b, c*

1. $a < b$ *e* $b \leq c \Rightarrow a < c$.

2. $a \leq b$ *e* $b < c \Rightarrow a < c$.

3. $a \leq b \Leftrightarrow -a \geq -b$.

4. $a < b \Leftrightarrow -a > -b$.

5. *Regras de sinal*

   (a) $a > 0$ *e* $b > 0 \Rightarrow ab > 0$

   (b) $a < 0$ *e* $b < 0 \Rightarrow ab > 0$

   (c) $a < 0$ *e* $b > 0 \Rightarrow ab < 0$

6. $a \leq b$ *e* $c \leq d \Rightarrow a + c \leq b + d$.

7. $a \leq b$ *e* $c < d \Rightarrow a + c < b + d$.

8. $a^2 \geq 0$.

9. $a < b$ *e* $c > 0 \Rightarrow ac < bc$

10. $a < b$ *e* $c < 0 \Rightarrow ac > bc$

11. $ac \leq bc$ *e* $c < 0 \Rightarrow a \geq b$

5.3.1 Valor absoluto

Definimos, para todo $a \in \mathbb{Z}$, o **valor absoluto** ou **módulo** de a

$$|a| := \begin{cases} a & \text{se } a \geq 0, \\ -a & \text{caso contrário.} \end{cases} \tag{39}$$

Exercício 72. *O valor absoluto satisfaz, para quaisquer inteiros a, b*

1. $|a| \geq 0$, *ademais* $|a| = 0$ *se e só se* $a = 0$.
2. $-|a| \leq a \leq |a|$.
3. $|-a| = |a|$.
4. $|ab| = |a||b|$.
5. $|a| \leq b \Leftrightarrow -b \leq a \leq b$.
6. $||a| - |b|| \leq |a + b| \leq |a| + |b|$.
7. $|a| - |b| \leq |a - b| \leq |a| + |b|$

5.4 Princípio da Boa Ordem para os inteiros

$A \subset \mathbb{Z}$ não-vazio é **limitado inferiormente** se existe $m \in \mathbb{Z}$ (chamado **cota inferior**) tal que

$$\forall\, a \in A,\ m \leq a.$$

Se $m \in A$, então m é **menor elemento** ou **mínimo** de A. Denotamos o mínimo de A por $\min(A)$.

11. Boa ordenação *Todo $A \subset \mathbb{Z}$ não vazio e limitado inferiormente tem um elemento mínimo.*

O mínimo, caso exista, é único: se m e m' são mínimos então $m \leq m'$ e $m' \leq m$, portanto $m = m'$.

É possível deduzir que mínimo existe a partir do PBO nos naturais: se m é uma cota inferior de A então

$$B := \{a - m \colon a \in A\} \subset \mathbb{N}$$

logo, para algum $b \in A$ temos $b - m$ é o menor elemento de B. Mostremos que b é uma cota inferior para A. Se $a \in A$ então $a - m \in B$, logo $b - m \leq a - m$, portanto $b \leq a$.

Proposição 73 (**Propriedade arquimediana**)**.** *Para todos $a, b \in \mathbb{Z}$ com $b \neq 0$, existe $n \in \mathbb{Z}$ tal que $n \cdot b > a$.*

Demonstração. De $|b| \neq 0$ temos $|b| \geq 1$ (exercício 17, pág. 20). Então $(|a| + 1) \cdot |b| \geq |a| + 1$ e $|a| + 1 > |a| \geq a$, ou seja, $(|a| + 1) \cdot |b| > a$. Agora, se $b > 0$ então tomamos $n = |a| + 1$ e se $b < 0$ então tomamos $n = -(|a| + 1)$. □

5.4.1 Princípios de indução matemática

No que segue

$$P(n) \text{ é um predicado sobre os inteiros } n.$$

Princípio da Indução Finita. *Se para um inteiro a valem*

1. $P(a)$ *é verdadeiro, e*
2. *para todo* $k \geq a$, *se* $P(k)$ *é verdadeiro então* $P(k+1)$ *é verdadeiro,*

então $P(n)$ *é verdadeiro para todo inteiro* $n \geq a$.

Esse princípio pode ser demonstrado a partir da boa ordenação, faremos essa prova para o caso abaixo, a qual pode ser facilmente adaptada para o caso acima.

Princípio da Indução Finita, segunda forma. *Se para um inteiro a valem*

1. $P(a)$ *é verdadeiro, e*
2. *para todo* $n > a$, *se* $P(k)$ *verdadeiro para todo* $k \in \{a, a+1, \ldots, n\}$ *então* $P(n+1)$ *é verdadeiro,*

então $P(n)$ *é verdadeiro para todo inteiro* $n \geq a$.

Demonstração. Se S é o conjunto dos inteiros $m \geq a$ tais que $P(m)$ é falso e assumimos que $S \neq \emptyset$ então a é uma cota inferior e temos $m_0 = \min S$.

$m_0 > a$ por 1 e $P(a), \ldots, P(m_0 - 1)$ é verdadeiro pela minimalidade de m_0, logo $P(m_0)$ é verdadeiro, por 2, o que é uma contradição. Assim, S deve ser vazio. □

Exercícios

1. Prove a partir das propriedades acima que para $a, b \in \mathbb{Z}$

   (a) $-(-a) = a$.

   (b) $-(a-b) = b-a$.

   (c) $a - b = 0 \Leftrightarrow a = b$.

   (d) $(-a)\cdot(-b) = a \cdot b$.

   (e) $(-1)\cdot a = -a$

   (f) $ab = 1 \Rightarrow a = b = 1$ ou $a = b = -1$

2. Mostre que todo $S \subset \mathbb{Z}$ limitado superiormente possui (único) máximo. Defina, nesse caso, os termos *limitado superiormente*, *máximo* e *cota superior*.

3. Prove usando indução

   (a) Seja $a \in \mathbb{Z}$ e $P(n)$ um predicado a respeito dos inteiros $n \leq a$. Suponha que (i) $P(a)$ é verdadeiro; (ii) para todo $n \leq a$, se $P(n)$ é verdadeiro então $P(n-1)$ é verdadeiro. Prove que $P(n)$ é verdadeiro para todo $n \leq a$.

   (b) Seja $n \in \mathbb{Z}$, $n > 0$. $n = 1+1+1+\cdots+1$ (n parcelas)

   (c) Seja $n \in \mathbb{Z}$, $n < 0$. $n = (-1)+(-1)+(-1)+\cdots+(-1)$ ($-n$ parcelas)

   (d) $2^{n+1} \geq n+2$ para todo $n \geq -1$.

   (e) para $a \neq 0$, $(-a)^n = a^n$ para todo n par.

   (f) para $a \neq 0$, $(-a)^n = -a^n$ para todo n ímpar.

4. Sejam $a > 0$ e b inteiros. Mostre que existe um inteiro k tal que $b + ka > 0$. (dica: boa-ordem)

6 Divisibilidade em $\mathbb{Z}$

Sejam $a, b \in \mathbb{Z}$.

b **divide** a se existe $c \in \mathbb{Z}$ tal que $bc = a$. Dizemos que b é um *divisor* de a, que c é o *quociente*. Se $b|a$ também dizemos que b é **múltiplo** de a. Por exemplo, o subconjunto dos inteiros múltiplos de 0 é $\{0\}$ e dos múltiplos de 1 é $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. Os múltiplos de 2 são os **inteiros pares**

$$\{0, \pm 2, \pm 4, \pm 6 \ldots\}$$

e o complemento

$$\{\pm 1, \pm 3, \pm 5, \ldots\}$$

são os **inteiros ímpares**. De modo geral, o subconjunto dos múltiplos de a, que é o mesmo dos múltiplos de $-a$ é denotado por

$$a \cdot \mathbb{Z} := \{a \cdot n \colon n \in \mathbb{Z}\} = \{0, \pm a, \pm 2a, \pm 3a, \ldots\} \tag{40}$$

Exercício 74. *Prove para inteiros a, b, c*

1. $1|a$, $a|a$ *e* $a|0$.

2. $0|a$ *se e somente se* $a = 0$

3. *Se* $b|a$ *e* $a \neq 0$ *então* $|b| \leq |a|$. *Consequentemente, a tem uma quantidade limitada de divisores pois* $-|a| \leq b \leq |a|$

4. *(reflexiva)* $a|a$.

5. *(transitiva) Se* $a|b$ *e* $b|c$ *então* $a|c$.

6. *Se* $a|b$ *e* $b|a$ *então* $a = \pm b$.

7. *Se* $a|b$ *e* $c|d$ *então* $ac|bd$.

8. *Se* $a|b$ *e* $a|c$ *então* $a|(mb+nc)$ $\forall\, m,n \in Z$.

9. *se* $a|(b+c)$ *então* $a|b$ *se e só se* $a|c$.

10. $a|b$ *se e só se* $|a| \Big| |b|$.

Algumas soluções. 2. Se $b|a$, então $bc = a$ para algum inteiro c. Usando o exercício 72, item 4 $|b||c| = |a|$. Como $c \neq 0$, $|b||c| = |b| + |b|(|c|-1)$, portanto $|b| \leq |a|$.

3. Se $a = b = 0$ então a afirmação vale. Se $a, b \neq 0$ então $a|b \Rightarrow ac = b$, para algum $c \neq 0$ e $b|a \Rightarrow bd = a$, para algum $d \neq 0$. Assim, $a(cd) = a$, logo $cd = 1$ donde concluímos que $c = d = 1$ ou $c = d = -1$ (exercício 1f, página 57).

8. $a|b \Rightarrow ac = b$ para algum c; pelo exercício 72, item 4 $|a||c| = |b|$, portanto, $|a| \Big| |b|$. Por outro lado, se $|a| \Big| |b|$ então $|a|c = |b|$ para algum c; notemos que $c = |c|$, portanto $|ac| = |b|$. Mas $|b| = \pm b$ e $|ac| = \pm ac = a(\pm c)$, logo $b = a(\pm c)$.

□

Exercício 75. *Prove usando indução em n que para quaisquer* $a, b \in \mathbb{Z}$

1. $a - b$ *divide* $a^n - b^n$.

2. $a + b$ *divide* $a^{2n} - b^{2n}$.

3. $a + b$ *divide* $a^{2n+1} + b^{2n+1}$.

6.1 Teorema da Divisão

Teorema 76 (Teorema da Divisão)**.** *Para todo inteiro* a *e todo inteiro* $b \neq 0$ *existe um único inteiro* q *e existe um único inteiro* r *tal que*

$$a = bq + r \;\; e \;\; 0 \leq r < |b| \tag{41}$$

Demonstração. Provaremos em dois casos, de acordo com o sinal de b.

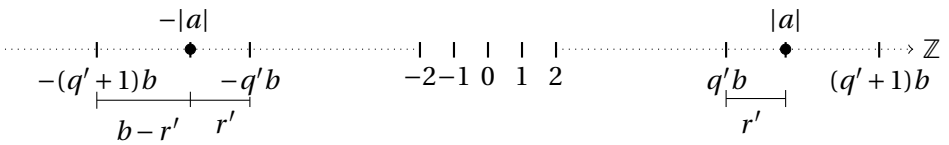
Para $b > 0$: se $a \geq 0$ não há o que demonstrar pois a e b são naturais e já provamos esse caso. Agora, se $a < 0$, tomamos q' e r' tais que $|a| = bq' + r'$. Se $r' = 0$ então $q := -q'$ e $r := 0$ donde

$$a = -|a| = b(-q') + r = bq + r.$$

Senão,

$$q'b \leq |a| < (q'+1)b \Rightarrow -(q'+1)b < -|a| \leq -q'b$$

(veja eq. (16)), tomamos $q := -(q'+1)$ e $r := b - r'$,



de modo que

$$a = -|a| = b(-q)' - r' = b(q+1) + r - b = bq + r.$$

Para $b < 0$: tomamos q' e r' tais que $a = q'|b| + r'$ (como fizemos acima) e tomamos $q := -q'$ e $r := r'$, assim $a = qb + r$ com $0 \leq r < |b|$. □

Por exemplo

$$7 = 3 \cdot 2 + 1 \qquad -7 = 3 \cdot (-3) + 2$$
$$7 = -3 \cdot (-2) + 1 \qquad -7 = -3 \cdot 3 + 2$$

Outra demonstração. Para $b > 0$ definimos

$$R := \{a - nb \colon n \in \mathbb{Z}\}$$

e $R \cap \mathbb{Z}^+ \neq \emptyset$ pois para $n = -|a|b$ temos $a + |a|b^2 \geq a + |a| \geq 0$. Seja r o menor inteiro positivo de $R \cap \mathbb{Z}^+$, $r = a - qb$.

Se $r \geq b$ então $r = b + s$ para algum $s \geq 0$. De $b + s = a - qb$ temos $s = a - (q+1)b \in R$ com $s < r$, uma contradição.

Para $b < 0$ tomamos q' e r' tais que $a = q'|b| + r'$ e fazemos $q = -q'$ e $r = r'$, assim $a = qb + r$ com $0 \leq r < |b|$.

A prova de que r e q são únicos fica como exercício. □

6.2 MDC

Para quaisquer $a, b \in \mathbb{Z}$

$$\text{mdc}(a,b) := \text{mdc}(|a|,|b|)$$

Se $d = \text{mdc}(a,b)$ então (verifique)

1. $d \geq 0$
2. $d|a$ e $d|b$
3. $b|a \Rightarrow d = |b|$
4. $a = bq + r \Rightarrow \text{mdc}(a,b) = \text{mdc}(b,r)$

Os inteiros a e b são **coprimos**, ou *primos relativos*, se $\text{mdc}(a,b) = 1$ o que equivale a dizer que os únicos divisores comuns a eles são o 1 e o -1.

Exercícios

1. Prove que se $a|1$ então $a = 1$ ou $a = -1$.
2. Ache o quociente e o resto das divisões inteiras de
   (a) 390 por 74
   (b) -124 por 18
   (c) 420 por -58
3. Na divisão de -345 por $b > 0$ o resto é 12. Quais são os possíveis divisores e quocientes?
4. Mostre que um dos inteiros a, $a+2$, $a+4$ é divisível por 3.
5. Escreva o $\text{mdc}(154,15)$ como combinação linear de 154 e 15.
6. Seja a e b inteiros. Prove que se existem inteiros x e y tais $ax + by = 1$, então a e b são coprimos.
7. Prove que $\text{mdc}(ca,cb) = |c|\text{mdc}(a,b)$.

6.3 Teorema de Bézout

Observemos o seguinte

mdc$(42,12) = 6$:

$$42 = 12\cdot 3+6$$
$$12 = 6\cdot 2+0$$
$$\boxed{42\cdot 1+12\cdot(-3)=6}$$

mdc$(41,12) = 1$:

$$41 = 12\cdot 3+5$$
$$12 = 5\cdot 2+2$$
$$5 = 2\cdot 2+1$$
$$2 = 1\cdot 2+0$$

$$\begin{aligned}1 &= 5-2\cdot 2\\ &= 5-(12-5\cdot 2)2 = 5\cdot 5-12\cdot 2\\ &= (41-12\cdot 3)\cdot 5-12\cdot 2 = 41\cdot 5-12\cdot 17\end{aligned}$$
$$\boxed{1 = 41\cdot 5+12\cdot(-17)}$$

mdc$(81,57) = 3$:

$$\begin{aligned}81 &= 57\cdot 1+24 \Longrightarrow 24 = 81-57\cdot 1\\ 57 &= 24\cdot 2+9 \Longrightarrow 9 = 57-24\cdot 2\\ 24 &= 9\cdot 2+6 \Longrightarrow 6 = 24-9\cdot 2\\ 9 &= 6\cdot 1+3 \Longrightarrow 3 = 9-6\\ 6 &= 3\cdot 2+0.\end{aligned}$$

$$\begin{aligned}3 &= 9-6 = 9-24+9\cdot 2 = (9)3-24\\ &= (57-24\cdot 2)3-24 = 57\cdot 3-(24)7\\ &= 57\cdot 3-(81-57\cdot 1)7 = 81\cdot(-7)+57\cdot 10\end{aligned}$$
$$\boxed{3 = 81\cdot(-7)+57\cdot 10}$$

Obs.: $1 = 41\cdot 17+12\cdot(-58)$ e $3 = 81\cdot(12)+57\cdot(-17)$, i.e., o modo de escrever não é único.

Definimos

$$a\cdot\mathbb{Z}+b\cdot\mathbb{Z}:=\{a\cdot n+b\cdot m\colon\ n,m\in\mathbb{Z}\} \tag{42}$$

o conjunto de todos os números que são *combinações lineares inteiras* de a e b, ou seja, o conjunto dos inteiros da forma $ax+by$ para algum x e algum y inteiros. Vamos provar que o menor elemento positivo desse conjunto é o mdc de a e b.

Teorema 77 (Teorema de Bézout)**.** *Se $a,b\in\mathbb{Z}$ então existem inteiros x e y tais que*

$$ax+by=\text{mdc}(a,b) \tag{43}$$

Demonstração. O caso $a=b=0$ é trivial. Vamos supor que $a\neq 0$ ou $b\neq 0$, portanto $(a\cdot\mathbb{Z}+b\cdot\mathbb{Z})\cap\mathbb{Z}^+\neq\emptyset$ (justifique com detalhes) e podemos usar o PBO e tomarmos

$$d:=\min[(a\cdot\mathbb{Z}+b\cdot\mathbb{Z})\cap\mathbb{Z}^+]$$

o menor elemento positivo de $a\cdot\mathbb{Z}+b\cdot\mathbb{Z}$. Existem $x_0,y_0\in\mathbb{Z}$ tais que $d=ax_0+by_0$.

Mostraremos que d divide qualquer elemento de $a\cdot\mathbb{Z}+b\cdot\mathbb{Z}$.

Seja $c\in a\cdot\mathbb{Z}+b\cdot\mathbb{Z}$. Existem inteiros x_1 e y_1 tais que $c=ax_1+by_1$. Pelo Teorema da Divisão existem inteiros q e r tais que $c=dq+r$, onde $0\leq r<d$, e

$$r=c-dq=ax_1+by_1-(ax_0+by_0)q=a(x_1-x_0q)+b(y_1-y_0q), \tag{44}$$

ou seja, $r\in a\cdot\mathbb{Z}+b\cdot\mathbb{Z}$. Como $0\leq r<d$ e d é mínimo deduzimos que $r=0$, portando $d|c$.

Em particular, $d|a$ e $d|b$, isto é, $d\in D(a)\cap D(b)$ por definição de mdc temos $d\leq\text{mdc}(a,b)$. Por outro lado, $d=ax_0+by_0$ e como $\text{mdc}(a,b)|ax_0+by_0$ segue que $\text{mdc}(a,b)|d$ (veja exerc. 74, item 8). Do exercício 74 (item 3) $\text{mdc}(a,b)\leq d$, logo, $\text{mdc}(a,b)=d$. □

Corolário 78. *Se a e b são inteiros não ambos nulos e c é um inteiro tal que $c|a$ e $c|b$, então $c|\text{mdc}(a,b)$.*

Demonstração. Basta notar que se $c|a$ e $c|b$ então c divide todo elemento de $a\mathbb{Z}+b\mathbb{Z}$. Em particular, $c|\text{mdc}(a,b)$. □

Com isso temos que se $d=\text{mdc}(a,b)$, então (i) $d\geq 0$, (ii) $d|a$ e $d|b$, e (iii) para todo c, $c|a$ e $c|b\Rightarrow c|d$. Essas três propriedades de fato caracterizam o mdc.

Teorema 79. *Se a e b são inteiros não ambos nulos, então $d=\text{mdc}(a,b)$ se, e somente se,*

1. *$d\geq 0$;*
2. *$d|a$ e $d|b$;*
3. *para todo inteiro c, $c|a$ e $c|b\Rightarrow c|d$.*

Demonstração. Exercício. □

Corolário 80. *Se a, b, c são inteiros tais que $a|bc$ e* $\mathrm{mdc}(a,b) = 1$*, então $a|c$.*

Demonstração. Exercício. □

Exercício 81. *Se $a|c$ e $b|c$, $c \neq 0$, e* $\mathrm{mdc}(a,b) = 1$ *então $ab|c$.*

Exercício 82. *Se a e b são inteiros, pelo menos um não-nulo, e $d = \mathrm{mdc}(a,b)$, então* $\mathrm{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$.

Solução. Existem n, m tais que $an + bm = d$, portanto $\frac{a}{d}n + \frac{b}{d}m = 1$, que é o menor positivo de $\frac{a}{d}\mathbb{Z} + \frac{b}{d}\mathbb{Z} = 1$, portanto $\mathrm{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$. □

6.4 Equações diofantinas lineares

Estudaremos as equações da forma

$$aX + bY = c \tag{45}$$

em que $a, b, c \in \mathbb{Z}$, a e b não ambos nulos; uma *solução* para tal equação é um par de inteiros (x_0, y_0) para o qual a igualdade acima vale quando $X = x_0$ e $Y = y_0$.

Proposição 83. *Dados inteiros a, b e c a equação* (45) *admite solução inteira se e somente se* $\mathrm{mdc}(a,b)|c$.

Demonstração. Denotemos por $d := \mathrm{mdc}(a,b)$ e por (n,m) uma solução de $aX + bY = d$ caso exista.

De $d|(ax + by)$ para quaisquer $x, y \in \mathbb{Z}$, em particular, caso (45) tenha solução, $d|an + bm$ e portanto $d|c$.

Por outro lado, se $d|c$ então existe q tal que $dq = c$. Pelo Teorema de Bézout existem $x, y \in \mathbb{Z}$ tais que $ax + by = d$, portanto (qx, qy) é solução de $aX + bY = c$. □

O resultado acima estabelece a seguinte iguldade de conjuntos

$$a \cdot \mathbb{Z} + b \cdot \mathbb{Z} = \mathrm{mdc}(a,b) \cdot \mathbb{Z}$$

Notemos que se a e b são coprimos então (45) tem solução qualquer que seja o inteiro c. Também vale a recíproca.

Corolário 84. *Dois inteiros a, b são coprimos se, e só se, a equação* (45) *admite solução inteira, qualquer que seja $c \in \mathbb{Z}$.*

Demonstração. Se a e b são coprimos então, pela proposição 83 a equação (45) tem solução qualquer que seja o inteiro c.

Agora, se existem $x, y \in \mathbb{Z}$ que satisfazem a equação para $c = 1$, então todo divisor d de a e b divide $ax + ay = 1$, portanto, $d = \pm 1$, logo $\mathrm{mdc}(a,b) = 1$. □

Notemos que para a ou b não-nulo e $d = \text{mdc}(a,b) \neq 0$

$$ax + by = c \iff \frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$$

para quaiquer $x, y \in \mathbb{Z}$ ($d|c$ como provamos acima, logo $\frac{c}{d}$ tem sentido). Ademais $\text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$, portanto toda equação diofantina linear

$$aX + bY = c$$

é equivalente — tem as mesmas soluções — de uma equação *reduzida*

$$\frac{a}{d}X + \frac{b}{d}Y = \frac{c}{d}$$

na qual os coeficientes são coprimos.

Ainda, se (x_0, y_0) é uma solução de $\frac{a}{d}X + \frac{b}{d}Y = 1$ então $(x_0\frac{c}{d}, y_0\frac{c}{d})$ é uma solução de $\frac{a}{d}X + \frac{b}{d}Y = \frac{c}{d}$.

Por exemplo, para achar uma solução de $81X + 57Y = 27$ basta achar uma solução de $27X + 19Y = 9$ e para achar uma solução dessa equação, primeiro procuramos por uma solução de $27X + 19Y = 1$.

Usando o algoritmo de Euclides para calcular o mdc e substituindo-se os restos, como fizemos anteriormente $\text{mdc}(27,19) = 1$:

$$\begin{aligned}
27 &= 19\cdot 1 + 8 \\
19 &= 8\cdot 2 + 3 \\
8 &= 3\cdot 2 + 2 \\
3 &= 2\cdot 1 + 1 \Leftrightarrow 1 = 3 - 2\cdot 1 \\
&\Leftrightarrow 1 = 3 - (8 - 3\cdot 2)\cdot 1 \\
&\Leftrightarrow 1 = -8 + 3\cdot 3 = -8 + (19 - 8\cdot 2)\cdot 3 \\
&\Leftrightarrow 1 = 8\cdot(-7) + 19\cdot 3 \\
&\Leftrightarrow 1 = (27 - 19\cdot 1)\cdot(-7) + 19\cdot 3 \\
&\Leftrightarrow \boxed{1 = 27\cdot(-7) + 19\cdot 10}
\end{aligned}$$

logo $(-7, 10)$ é solução de $27X + 19Y = 1$, portanto $(-7\cdot 9, 10\cdot 9)$ é solução de $27X + 19Y = 9$ e, consequentemente, de $81X + 57Y = 27$.

Teorema 85. *Se* (x_0, y_0) *é uma solução particular de* (45) *com* $a \neq 0$ *e* $b \neq 0$*, então o conjunto de todas as soluções de* (45) *é*

$$\left\{\left(x_0 + \frac{b}{d}t, y_o - \frac{a}{d}t\right) : t \in \mathbb{Z}\right\} \tag{46}$$

em que $d = \text{mdc}(a,b)$.

Demonstração. É um exercício verificar que $\left(x_0 + \frac{b}{d}t, y_o - \frac{a}{d}t\right)$ é solução de (45).

Agora, suponha que (x, y) seja uma solução de (45), então

$$ax + by = c = ax_0 + by_0$$

portanto

$$a(x - x_0) = b(y_0 - y).$$

Se $a = dr$ e $b = sd$,

$$r(x - x_0) = s(y_0 - y) \tag{47}$$

com $\text{mdc}(r, s) = 1$. Ainda, $s|r(x - x_0)$, portanto, $s|(x - x_0)$, ou seja, existe $t \in \mathbb{Z}$ tal que $x - x_0 = st$, portanto

$$x = x_0 + \frac{b}{d}t. \tag{48}$$

Substituindo $x - x_0 = st$ em (47) $s(y_0 - y) = r(x - x_0) = rst$, logo

$$y = y_0 - \frac{a}{d}t \tag{49}$$

como queríamos. □

Exercício 86. *De quantas maneiras podemos comprar selos de 3 e 5 reais de modo a gastar 50 reais?*

Exercício 87. *Mostre que se* (x_0, y_0) *é solução de* $aX + bY = c$*, então*

1. $(-x_0, y_0)$ *é solução de* $-aX + bY = c$*;*
2. $(x_0, -y_0)$ *é solução de* $aX - bY = c$*;*
3. $(-x_0, -y_0)$ *é solução de* $-aX - bY = c$*.*

Exercício 88. *Sejam* a, b, c, d *inteiros. Defina* $\text{mdc}(a, b, c) := \text{mdc}(\text{mdc}(a, b), c)$*. Estabeleça e prove um critério para existência de solução de*

$$aX + bY + cZ = d.$$

Exercícios

1. Deduza do Teorema de Bézout:
   (a) se $a|c$ então $\text{mdc}(a, b)|\text{mdc}(c, b)$.
   (b) se a e b são coprimos então $\text{mcd}(ac, b) = \text{mdc}(c, b)$.

2. Sejam a e b inteiros positivos e coprimos. Mostre que para todo inteiros $c > ab - a - b$, a equação $aX + bY = c$ admite soluções inteiras não-negativas.

3. Sejam a e b inteiros positivos e coprimos. Mostre que equação $aX - bY = c$ admite infinitas soluções nos naturais.

4. Determine as soluções inteiras de

   (a) $3x + 4y = 20$

   (b) $5x - 2y = 2$

   (c) $18x - 20y = -8$

5. Ache todos inteiros positivos que deixam resto 6 quando divididos por 11 e resto 3 quando divididos por 7.

6. Ache todos os naturais que quando divididos por 18 deixam resto 4 e que quando divididos por 14 deixam resto 6.

7. Um parque cobra ingresso de 1 real de crianças e 3 de adultos. Para que a arrecadação de um dia seja 200 reais qual o menor numero de pessoas, adultos e crianças, que frequentam o parque?

8. Um fazendeiro dispõe de 1.770 reais pra gastar em boi e cavalo. Um cavalo custa 31 reais e boi 21 reais. Qual o maior número de animais que pode comprar?

7 Decomposição de inteiros em fatores primos

Agora, dizemos que $p > 1$ é primo se seus únicos divisores são ± 1 e $\pm p$, caso contrário é composto.

Segue do estudo feito na seção 3 que

Teorema 89. *Todo inteiros $n \neq 0, -1, 1$ pode ser escrito como*

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

para primos $p_1 < p_2 < \cdots < p_k$ e inteiros positivos $\alpha_1, \ldots, \alpha_k$ univocamente determinados. □

8 Congruências

Para inteiros a, b, n, com $n \neq 0$, dizemos que a **é congruente a** b **módulo** n, e escrevemos

$$a \equiv b \pmod{n} \tag{50}$$

se $n|(a-b)$. Como $n|(a-b) \Leftrightarrow -n|(a-b)$ nos restringiremos ao caso $n > 0$. O caso $n = 1$ é trivial pois quaisquer dois inteiros são congruentes. Geralmente, os casos interessantes são para $n > 1$. Para $n = 2$, por exemplo, dois inteiros são congruentes se, e só se, eles diferem por um inteiro par, ou seja, têm mesma paridade.

Por exemplo, $152 \equiv 5 \pmod 7$ ($152 = 21 \cdot 7 + 5$) e $-152 \equiv 2 \pmod 7$ ($152 = (-22) \cdot 7 + 2$). Também, $7 \equiv 15 \pmod 8$, $3 \equiv 21 \pmod 6$.

Dados a e b congruentes, usando o Teorema da Divisão, dividimos ambos por n e temos únicos q_a, r_a, q_b, r_b tais que $a = nq_a + r_a$ e $b = nq_b + r_b$ de modo que $0 \leq r_a, r_b < n$, portanto, $-n < r_a - r_b < n$ e temos

$$a - b = n(q_a - q_b) + (r_a - r_b) \tag{51}$$

com $n|(a-b)$ e $n|n(q_q - q_b)$ logo $n|(r_a - r_b)$ e como o único múltiplo de n que satisfaz $-n < r_a - r_b < n$ é o 0 temos

$$r_a = r_b.$$

Concluindo, se a é congruente a b módulo n então a e b deixam o mesmo resto quando divididos por n. Por outro lado, se a e b deixam o mesmo resto quando divididos por n então $n|(a-b)$ pois $a - b = n(q_a - q_b)$. Usando a notação introduzida na página 26, o que estabelecemos foi

Proposição 90. *$a \equiv b \pmod n \iff a \bmod n = b \bmod n$, para quaisquer inteiros a, b e $n > 0$.* □

Observação 91. *Segue da equivalência dada na proposição acima e do Teorema da Divisão que todo inteiro é congruente a um, e somente um, dentre os números $\{0, 1, 2, \ldots, n-1\}$*

Claramente, $\equiv \pmod n$ é uma relação de equivalência; é reflexiva ($a \equiv a \pmod n$), é simétrica ($a \equiv b \pmod n \Leftrightarrow b \equiv a \pmod n$), e é transitiva ($a \bmod n = b \bmod n$ e $b \bmod n = c \bmod n \Leftrightarrow a \bmod n = c \bmod n$).

Proposição 92. *$\equiv$ é uma relação de equivalência sobre $\mathbb{Z}$.* □

Além de ser relação de equivalência, congruência é compatível com as operações aritméticas dos inteiros.

Proposição 93. *Para quaisquer inteiros a, b, c, d e $n > 0$, se $a \equiv b \pmod n$ e $c \equiv d \pmod n$ então valem*

1. $a + c \equiv b + d \pmod n$
2. $a - c \equiv b - d \pmod n$
3. $a \cdot c \equiv b \cdot d \pmod n$

Note que, em particular, vale quando $c = d$.

Demonstração. Da hipótese temos que $n|(a-b)$ e $n|(c-d)$ e do exercício 74, item 8 temos que $n|x(a-b)+y(c-d)$ para quaisquer $x, y \in \mathbb{Z}$, daí

1. o item 1 segue de $(a-b)+(c-d)=(a+c)-(b+d)$;
2. o item 2 segue de $(a-b)-(c-d)=(a-c)-(b-d)$;
3. o item 3 segue de $c(a-b)+b(c-d)=ac-bd$.

□

Corolário 94. *Para quaisquer inteiros a, b, c e $n>0$*

$$a+c \equiv b+c \pmod{n} \Rightarrow a \equiv b \pmod{n}.$$

Demonstração. Segue do item 2. Observe que $(a+b)+c \equiv a+(b+c) \pmod{n}$. □

Não vale a versão análoga para o produto como mostra o seguinte exemplo: $6 \cdot 9 \equiv 6 \cdot 5 \pmod{8}$, entretanto $9 \not\equiv 5 \pmod{8}$. Uma versão que vale para o produto é dada pelo lema 106 abaixo.

Corolário 95. *Se $a \equiv b \pmod{n}$, então $a^k \equiv b^k \pmod{n}$, para todo $k \in \mathbb{N}$.*

Demonstração. Segue do item 3 por indução em k. □

Exemplo 96. *Qual o resto da divisão de $5^{3^{20}}$ por 13?*

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

os restos se repetem com período 4. Portanto precisamos conhecer $3^{20} \bmod 4$: temos $3 \equiv -1 \pmod{4}$ logo $3^{20} \equiv 1 \pmod{4}$, portanto $5^{3^{20}} \equiv 5 \pmod{13}$.

Exercício 97. *Sejam $a, b \in \mathbb{Z}$ e $n>0$. Prove que se $a \equiv b \pmod{n}$ e $d|n$ então $a \equiv b \pmod{d}$.*

Exercício 98. *Mostre, usando indução, que para m pares de inteiros a_i e b_i, tais que $a_i \equiv b_i \pmod{n}$ ($i \in \{1,2,\ldots,m\}$) valem*

$$\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} b_i \pmod{n} \tag{52}$$

$$\prod_{i=1}^{m} a_i \equiv \prod_{i=1}^{m} b_i \pmod{n} \tag{53}$$

Exercício 99. *Prove que se* $a \equiv b \pmod{n}$ *então* $(a,n) = (b,n)$.

Solução. Se $a \equiv b \pmod{n}$ então $b = a + nq$ e do exercício 2, página 35, $(a,n) = (a+nq,n) = (b,n)$. □

Exemplo 100 (critério de divisibilidade por 9)**.** *Seja* $a_r \ldots a_0$ *a representação decimal de* n. *De* $10 \equiv 1 \pmod{9}$ *temos, pela proposição 93 que* $10^s \equiv 1 \pmod{9}$, $a \cdot 10^s \equiv a \pmod{9}$ $(\forall a)$, *portanto, pelo exercício 98*

$$a_0 + a_1 10 + a_2 10^2 + \cdots + a_r 10^r \equiv a_0 + a_1 + a_2 + \cdots + a_r \pmod{9}.$$

Exemplo 101 (critério de divisibilidade por 11)**.** *Seja* $a_r \ldots a_0$ *a representação decimal de* n. *De* $10 \equiv -1 \pmod{11}$ *temos que* $a \cdot 10^s \equiv a \cdot (-1)^s \pmod{11}$ *portanto*

$$a_0 + a_1 10 + a_2 10^2 - \cdots + a_r 10^r \equiv a_0 - a_1 + a_2 - \cdots + (-1)^r a_r \pmod{11}.$$

Exemplo (ISBN – *International Standard Book Number*)**.** *Um dos livros texto tem ISBN 8-585-81825-5.*

O ISBN tem dez dígitos. O último é um dígito de controle. Os primeiros nove dígitos codificam informações como a língua e a editora do livro. Um código ISBN válido $d_0 - d_1 d_2 d_3 - d_4 d_5 d_6 d_7 d_8 - d_9$ *satisfaz*

$$10d_0 + 9d_1 + 8d_2 + 7d_3 + 6d_4 + 5d_5 + 4d_6 + 3d_7 + 2d_8 + 1d_9 \equiv 0 \pmod{11}$$

quando d_9 *vale* 10 *é usado a letra* X.

Exercício 102. *Qual os dois últimos algarismos de* 3^{200}.

Solução. $3^{200} = 9^{100} = (10-1)^{100} = \sum_{k=0}^{100} \binom{100}{k} 100^{100-k}(-1)^k \equiv -\binom{100}{99}10 + \binom{100}{100} \pmod{100} \equiv 1 \pmod{100}$. Portanto, 01. □

Usando a definição de congruência podemos reescrever o Pequeno Teorema de Fermat do seguinte modo.

Teorema 103 (**Pequeno Teorema de Fermat revisitado**)**.** *Se* p *é primo e* $a \in \mathbb{Z}$ *então* $a^p \equiv a \pmod{p}$. *Ademais, se* $p \nmid a$, *então* $a^{p-1} \equiv 1 \pmod{p}$. □

Exemplo. *Se* p *é primo e* $a, b \in \mathbb{Z}$, *então* $a \equiv a^p \pmod{p}$ *e* $b \equiv b^p \pmod{p}$, *portanto* $a + b \equiv a^p + b^p \pmod{p}$. *Ainda* $a + b \equiv (a+b)^p \pmod{p}$. *Logo*

$$a^p + b^p \equiv (a+b)^p \pmod{p}.$$

Também $a^p \equiv (a - b + b)^p \equiv (a-b)^p + b^p \pmod{p}$ *de modo que*

$$a^p - b^p \equiv (a-b)^p \pmod{p}.$$

Ainda, se $a^p \equiv b^p \pmod{p}$ *então* $p|a^p - b^p$, *portanto, pela equação acima,* $p|(a-b)^p$, *logo* $p|a-b$, *ou seja,* $a \equiv b \pmod{p}$ *e, portanto,* $a^k \equiv b^k \pmod{p}$ *para todo* $k \in \mathbb{N}$. *Disso temos que* $b^k a^{p-1-k} \equiv a^{p-1} \pmod{p}$ *logo* $a^{p-1} + ba^{p-2} + \cdots + b^{p-2}a + b^{p-1} \equiv pa^{p-1} \equiv 0 \pmod{p}$. *Como*

$$a^p - b^p = (a-b)(a^{p-1} + ba^{p-2} + \cdots + b^{p-2}a + b^{p-1})$$

e $p|a-b$ *e* $p|)(a^{p-1} + ba^{p-2} + \cdots + b^{p-2}a + b^{p-1})$ *concluímos que*

$$a^p \equiv b^p \pmod{p} \Rightarrow a^p \equiv b^p \pmod{p^2}.$$

Exemplo 104. *Qual o resto da divisão de* 237^{28} *por* 13*?*

Notemos que $237^{12} \equiv 1 \pmod{13}$ *pelo PTF, logo* $237^{24} \equiv 1 \pmod{13}$. *Ainda* $237 \equiv 3 \pmod{13}$, *logo* $237^4 \equiv 3^4 \pmod{13}$, *portanto* $237^{28} \equiv 3^4 \pmod{13}$. *Agora* $3^4 \equiv 81 \equiv 3 \pmod{13}$, *portanto o resto é* 3.

Exemplo 105. *Mostre que* $31|20^{15} - 1$.

Como $31 = 20 + 11$, *temos* $20 + 11 \equiv 0 \pmod{31}$, *ou seja,* $20 \equiv -11 \pmod{31}$ *portanto* $20^2 \equiv 121 \equiv -3 \pmod{31}$. *Multiplicando as congruências* $20^3 \equiv 33 \equiv 2 \pmod{31}$ *logo* $20^{15} \equiv 2^5 \pmod{31}$. *Mas* $2^5 = 32$ *de modo que* $20^{15} \equiv 1 \pmod{31}$.

Vejamos mais propriedades multiplicativas das congruências.

Lema 106. *Se* $ca \equiv cb \pmod{n}$ *e* $\text{mdc}(c,n) = d > 0$ *então*

$$a \equiv b \pmod{\frac{n}{d}}.$$

Demonstração. Se $ca \equiv cb \pmod{n}$ então existe q tal que $nq = ca - cb = c(a-b)$. Como $d > 0$ divide n e divide c temos $\frac{n}{d}q = \frac{c}{d}(a-b)$, portanto $\frac{n}{d}|\frac{c}{d}(a-b)$ mas $\text{mdc}(\frac{n}{d}, \frac{c}{d}) = 1$, portanto $\frac{n}{d}|(a-b)$. □

Corolário 107. *Se* $\text{mdc}(c,n) = 1$ *então*

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

Corolário 108. *Se* $ca \equiv cb \pmod{p}$ *e* p *primo que não divide* c *então*

$$a \equiv b \pmod{p}.$$

Por exemplo, $10 \equiv -1 \pmod{11}$, portanto $10^{200} \equiv -1^{200} \pmod{11}$, e como $1 \equiv -1^{200} \pmod{11}$ temos $1 \equiv 10^{200} \pmod{11}$, portanto, $11|10^{200} - 1$.

Exemplo. *Quais são os inteiros* x *tais que* $7(x^2 - 1) \equiv 21 \pmod{8}$*?*

Escrevendo $21 = 7 \cdot 3$ *temos que* $7(x^2 - 1) \equiv 21 \pmod{8}$ *se, e so se,* $7(x^2 - 1) \equiv 7 \cdot 3 \pmod{8}$. *Como* $(7,8) = 1$, *pelo Corolário 107 obtemos* $x^2 - 1 \equiv 3 \pmod{8}$ *que equivale a* $x^2 \equiv 4 \pmod{8}$. *Analisando os*

restos da divisão por 8*:*

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

portanto $x = 8k+2$ *ou* $8k+6$ *para* $k \in \mathbb{Z}$.

Exercício 109. *Sejam* $m_1, m_2, \ldots, m_k$ *inteiros positivos e defina para todo* $k > 2$, $\text{mmc}(m_1, m_2, \ldots, m_k) := \text{mmc}(\text{mmc}(m_1, m_2, \ldots, m_{k-1}), m_k)$. *Prove que se* $a \equiv b \pmod{m_i}$ *para todo* i*, então*

$$a \equiv b \pmod{\text{mmc}(m_1, m_2, \ldots, m_k)}. \tag{54}$$

Prove a recíproca.

Solução. Se $a \equiv b \pmod{m_i}$, $i = 1, \ldots, k$, então $m_i | b-a$, para todo i. Sendo $b-a$ múltiplo de cada m_i, segue-se que $\text{mmc}(m_1, \ldots, m_k) | b-a$, o que prova que $a \equiv b \pmod{\text{mmc}(m_1, \ldots, m_k)}$. A recíproca decorre do exercício 97. □

Exemplo 110. *Qual o menor múltiplo positivo de* 7 *que deixa resto* 1 *quando dividido por* 2*,* 3*,* 4*,* 5 *e* 6*? Queremos achar a menor solução positiva do seguinte sistema de congruências:*

$$\begin{cases} 7X \equiv 1 \pmod 2 \\ 7X \equiv 1 \pmod 3 \\ 7X \equiv 1 \pmod 4 \\ 7X \equiv 1 \pmod 5 \\ 7X \equiv 1 \pmod 6. \end{cases}$$

Pelo exercício anterior, a é solução simultânea das congruências se, e só se, é solução da congruência $7a \equiv 1 \pmod{\text{mmc}(2,3,4,5,6)}$. *Portanto, devemos achar a menor solução positiva da congruência* $7X \equiv 1 \pmod{60}$.

Por outro lado, $7x \equiv 1 \pmod{60}$ *para* $x \in \mathbb{Z}$ *se, e só se, existe inteiro* y *tal que* $7x - 1 = 60y$*, ou seja,* $7x - 60y = 1$*. Pelo algoritmo euclidiano estendido,* $x_0 = -17$ *e* $y_0 = -2$ *é uma solução particular da equação diofantina* $7X - 60Y = 1$ *e a sua solução geral é* $x = -17 + 60t$ *e* $y = -2 - 7t$*, para todo* $t \in \mathbb{Z}$*. Portanto, o menor valor positivo de* x *para o qual exista* y *tais que* (x, y) *seja uma solução da equação diofantina* $7X - 60Y = 1$ *é* $x = -17 + 1 \cdot 60 = 43$.

8.1 Sistema completo de restos

$S \subset \mathbb{Z}$ é um **sistema completo de restos módulo** n se para todo $a \in \mathbb{Z}$ existe um, e só um, $b \in S$ tal que $a \equiv b \pmod{n}$. Por exemplo, alguns sistemas completos de resíduos módulo 5 são os conjuntos:

$$\{-2,-1,0,1,2\},$$

$$\{0,1,2,3,4\},$$

$$\{1,2,3,4,5\},$$

$$\{12,24,35,-4,18\}.$$

Conforme vimos, observação 91, $\{0,1,\ldots,n-1\}$ é um sistema completo de restos módulo n.

Para qualquer sistema completo de restos módulo n deve haver uma bijeção com $\{0,1,\ldots,n-1\}$ (por quê?) logo todo sistema completo de restos módulo n tem que ter cardinalidade n.

Observação 111. $\equiv$ *é uma relação de equivalência; uma classe de equivalência é dada por todos os inteiros que deixam o mesmo resto quando divididos por* n*. Um sistema completo de restos é um conjunto formado por um representante de cada classe de equivalência.*

Por exemplo, definimos para $r \in \mathbb{Z}$

$$[r]_n := \{a \in \mathbb{Z} \colon a \equiv r \pmod{n}\}$$

e temos as classes que equivalência módulo 5 dadas por $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$. Ademais, no exemplo acima identificamos que $[0]_5 = [5]_5 = [35]_5$, e $[-2]_5 = [3]_5 = [18]_5$, e $[-1]_5 = [4]_5 = [24]_5$, e $[2]_5 = [12]_5$ e $[-4]_5 = [1]_5$.

Exemplo 112. *A equação* $X^3 - 117Y^3 + 1 = 5$ *não tem solução inteira*[6].

Se (x,y) *é uma solução de inteiros então deve valer que* $x^3 - 117y^3 + 1 \equiv 5 \pmod{9}$. *Como* 117 *é múltiplo de* 9*, equivale a* $x^3 + 1 \equiv 5 \pmod{9}$ *a qual não tem solução pois, considerando o sistema completo de restos* $S = \{0,1,2,3,4,5,6,7,8\}$*,* $x \in \mathbb{Z}$ *é congruente a um (e só um) elemento* $r \in S$*, portanto,* $x^3 \equiv r^3 \pmod{9}$ $(r \in S)$ *e os cubos módulo* 9 *são* $\{0,1,8\}$

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

porém nenhum inteiro dentre $0,1,8$ *satisfaz* $X^3 + 1 \equiv 5 \pmod{9}$.

Exercício 113. *A congruência* $X^2 + 1 \equiv 0 \pmod{8}$ *não tem solução.*

[6] uma história curiosa a respeito dessa equação pode ser lida na página 81 de COUTINHO, C.; Números inteiros e criptografia RSA. IMPA-SBM, 2009.[512.7 COUn Estante:4H]

Solução. Consideremos o seguinte sistema completo de restos módulo 8 (verifique): $\{0,\pm1,\pm2,\pm3,4\}$. Se $x\in\mathbb{Z}$ então existe um único $r\in\{0,\pm1,\pm2,\pm3,4\}$ tal que $x\equiv r \pmod 8$, assim $x^2\equiv r^2 \pmod 8$ e

r	4	±3	±2	±1	0
$r^2 \bmod 8$	0	1	4	1	0

portanto x^2+1 é congruente a um dentre $1,2,5$. □

Exercício 114. *Sejam $i,n,m\in\mathbb{Z}$, com $n,m>1$ e $(n,m)=1$. Se $a_1,a_2,\ldots,a_n$ é um sistema completo de restos módulo n, então $i+ma_1, i+ma_2,\cdots,i+ma_n$ também é um sistema completo de restos módulo n. Em particular, se $(a_1,a_2,\ldots,a_n)=(0,1,\ldots,n-1)$ então $i,i+m,\cdots,i+m(n-1)$ também é um sistema completo de resíduos módulo n.*

Exercícios

1. Sejam a,b,r,s inteiros, $s\neq0$. Prove que $a\equiv b \pmod r$ se, e somente se, $as\equiv bs \pmod{rs}$.
2. Prove que se a é um cubo então a^2 é congruente a 0, ou 1, ou 9, ou 28 módulo 36.
3. Determinar todos os inteiros positivos m tais que as soluções de $X^2\equiv0\pmod m$ também sejam soluções de $X\equiv0 \pmod m$.
4. Determinar os restos das divisões
   (a) 2^{50} por 7;
   (b) 41^{65} por 7.
5. Verifique
   (a) $89|(2^{44}-1)$;
   (b) $97|(2^{11}-1)$.
6. Qual os dois últimos algarismos de $7^{7^{100}}$. (dica: $7^k \bmod 100$ é periódico)

9 O Teorema de Euler

9.1 A função φ de Euler

A função φ de Euler associa a cada inteiro positivo n a quantidade de inteiros positivos menores que n que são coprimos com n

$$\varphi(n) := \Big|\{a\in\mathbb{N}\colon \operatorname{mdc}(a,n)=1 \text{ e } 1\le a\le n\}\Big| \tag{55}$$

por exemplo

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

Decorre da definição que se p é primo então

$$\varphi(p) = p - 1 \text{ para todo primo } p.$$

Para potências de primo temos que dentre $1, 2, \ldots, p^k$ não são coprimos com p^k aquele que têm p como fator primo, a saber $p, 2p, 3p, \ldots, p^{k-1}p$, portanto $p^k - p^{k-1} = \varphi(p^k)$ são os coprimos, isto é

$$\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right) \text{ para todo primo } p.$$

Para determinarmos o valor da função de Euler nos naturais que não são potência de primo o seguinte é fundamental: a função φ é multiplicativa.

Teorema 115. *Se $n, m \in \mathbb{Z}^+$ são coprimos então $\varphi(nm) = \varphi(n)\varphi(m)$.*

Demonstração. O caso $m = 1$ ou $n = 1$ é imediato. Sejam $n, m > 1$ inteiros. Para todo inteiro a

$$\text{mdc}(a, nm) = 1 \Leftrightarrow \text{mdc}(a, n) = 1 \text{ e } \text{mdc}(a, m) = 1 \tag{56}$$

pois se $\text{mdc}(a, nm) = 1$ então existem $x, y \in \mathbb{Z}$ tais que $ax + nmy = 1$ donde temos que $aX + nY = 1$ tem solução e $aX + mY = 1$ tem solução, portanto, $\text{mdc}(a, n) = \text{mdc}(a, m) = 1$ pelo corolário 84. A recíproca segue do exercício 32, item 6. Desse modo, $\varphi(nm)$ é a quantidade de naturais entre 1 e nm que são coprimos com n e com m concomitantemente. Em há

$$\begin{array}{ccccccc}
1 & 2 & \ldots & i & \ldots & m \\
m+1 & m+2 & \ldots & m+i & \ldots & 2m \\
2m+1 & 2m+2 & \ldots & 2m+i & \ldots & 3m \\
\vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+i & \ldots & nm
\end{array}$$

$\varphi(m)\varphi(n)$ coprimos com n e m pois: se um divisor de m divide i então divide todos os números na coluna i. Portanto, os coprimos com m e com n aparecem nas $\varphi(m)$ colunas dos coprimos com m. A coluna i é um sistema completo de restos módulo n, pelo exercício 114, portanto há, nela, $\varphi(n)$ coprimos com n. □

Exercício 116. *Use indução (em k) para mostrar que se* $\text{mdc}(n_i, n_j) = 1$ *para todo $i \neq j$ então $\varphi(n_1 n_2 \cdots n_k) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_k)$.*

Corolário 117. *Se $n = p_1^{m_1} \cdots p_k^{m_k}$ é a fatoração canônica de n então*

$$\varphi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right). \tag{57}$$

Demonstração. Se $n = p_1^{m_1} \cdots p_k^{m_k}$ é a fatoração canônica de n então, usando indução em k,

$$\varphi\left(\prod_{i=1}^{k} p_i^{m_i}\right) = \prod_{i=1}^{k} \varphi(p_i^{m_i})$$

pois $p_i^{m_i}$ e $p_j^{m_j}$ são coprimos para quaisquer $i \neq j$. Assim

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

□

Exercício 118. *Mostre que $\varphi(n) = n - 1$ se e só se n primo.*

9.2 Sistema completo de invertíveis (sci) ou sistema reduzido de restos

Do conjunto $R := \{0, 1, \ldots, n-1\}$ dos restos módulo n, consideremos apenas os que são coprimos com n, isto é, o subconjunto $S := \{r_1, r_2, \ldots, r_{\varphi(n)}\} \subset R$ de todos os restos $r_i \in R$ tais que $\text{mdc}(r_i, n) = 1$. Como R é um sistema completo de restos (scr) módulo n, todo inteiro b é côngruo a um, e só um, $r \in R$; agora, se b é coprimo com n então $r \in S$: do Teorema de Euclides temos $\text{mdc}(n, b \bmod n) = \text{mdc}(b, n) = 1$ e $r = b \bmod n$. Ou seja, *todo inteiro coprimo com n é congruente a um e só um elemento de S.*

Dizemos que um inteiro a tem inverso multiplicativo módulo n se a equação $aX \equiv 1 \pmod{n}$ admite solução $x_0 \in \mathbb{Z}$. Dizemos que a solução é única módulo n se $x_0 \in \{0, 1, \ldots, n-1\}$ e para qualquer outra solução x vale que $x \equiv x_0 \pmod{n}$.

Proposição 119 (**Inverso multiplicativo mod n**)**.** *Sejam $a, n > 1$ inteiros. A equação $aX \equiv 1 \pmod{n}$ tem solução se e somente se* $\text{mdc}(a, n) = 1$. *Ademais, se há solução então ela é única modulo n.*

Demonstração. Dados a, n temos da proposição 83 (pág. 64) que

$$aX + nY = 1$$

admite solução inteira se, e somente se, $\text{mdc}(a, n) = 1$.

Se $\text{mdc}(a, n) = 1$ então existem x_0 e y_0 tais que $ny_0 = ax_0 - 1$, ou seja, $n | ax_0 - 1$, portanto, $ax_0 \equiv 1 \pmod{n}$. Por outro lado, se $ax_0 \equiv 1 \pmod{n}$ então $n | ax_0 - 1$ de modo que existe y_0 tal que $ax_0 + ny_0 = 1$.

Ainda, se $ax \equiv 1 \pmod{n}$ e $ax_0 \equiv 1 \pmod{n}$ então $ax \equiv ax_0 \pmod{n}$ portanto, do corolário 107, $x \equiv x_0 \pmod{n}$. □

A única solução módulo n garantida no último resultado é chamado de *inverso multiplicativo de a módulo n*.

Para $n \geq 1$, um conjunto com $\varphi(n)$ inteiros incongruentes entre si módulo n e coprimos com n é chamado de *sistema completo de invertíveis módulo n*. Equivalentemente, um conjunto $S \subset \mathbb{Z}$ tal que

$\text{mdc}(a,n) = 1$ para todo $a \in S$ e tal que para todo $z \in \mathbb{Z}$ com $\text{mdc}(z,n) = 1$ existe um único $a \in A$ tal que $a \equiv z \pmod{n}$ é um *sistema completo de invertíveis módulo n*.

Por exemplo $\{1,3,5,7\}$, $\{\pm 1, \pm 3\}$ e $\{\pm 5, \pm 7\}$ são sci módulo 8.

Exercício 120. *Seja S um scr módulo n qualquer. Mostre que os elementos de S coprimos como n formam um sci módulo n.*

Em vista disso, um sci também é chamado de *sistema reduzido de restos módulo n*.

Proposição 121. *Se S é um sci módulo n então para todo a coprimo com n o conjunto $a \cdot S$ é um sci módulo n.*

Demonstração. Tome $S = \{x_1, x_2, \ldots, x_{\varphi(n)}\}$ um sistema completo de invertíveis módulo n e forme o conjunto $a \cdot S = \{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}$ para a coprimo com n. Como a é invertível módulo n, então

$$ax_i \equiv ax_j \pmod{n} \Rightarrow x_i \equiv x_j \pmod{n} \Rightarrow i = j,$$

ademais $\text{mdc}(ax_i, n) = 1$ para todo i, ou seja, os $\varphi(n)$ elementos de $a \cdot S$ são incongruentes entre si e invertíveis módulo n. □

9.3 O Teorema de Euler

Teorema 122 (Teorema de Euler)**.** *Sejam $a, n \in \mathbb{Z}$, $n > 0$ e $\text{mdc}(a,n) = 1$. Então*

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{58}$$

Demonstração. Tome $A = \{x_1, x_2, \ldots, x_{\varphi(n)}\}$ sci e consideremos $a \cdot A$. Como, para cada i vale $\text{mdc}(ax_i, n) = 1$, devemos ter $ax_i \equiv x_j \pmod{n}$ para algum j portanto,

$$x_1 x_2 \cdots x_{\varphi(n)} a^{\varphi(n)} \equiv x_1 x_2 \cdots x_{\varphi(n)} \pmod{n}$$

e como cada x_i é invertível módulo n segue (58). □

Exemplo. *O resto da divisão de 3^{100} por 34 é 13. Dos resultados acima $\varphi(34) = 16$ e $3^{16} \equiv 1 \pmod{34}$. Assim $3^{100} = 3^{16 \cdot 4 + 4} \equiv 3^4 \equiv 13 \pmod{34}$.*

Corolário 123 (Pequeno Teorema de Fermat)**.** *Seja $a \in \mathbb{Z}$ e p um primo que não divide a. Então*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{59}$$

Demonstração. Veja o exercício 118. □

Exemplo. $30|(n^{13}-n)$ *para todo* n.

$2|(n^{13}-n)$ *para todo n pois*

$$n^{13}-n = n(n^{12}-1) \quad e \quad n^{12}-1 = (n-1)(n^{11}+n^{10}+\cdots+n+1)$$

e $2|n$ *ou* $2|n-1$.

$3|(n^{13}-n)$ *para todo n pois*

$$n^{13}-n = n(n^{12}-1) \quad e \quad n^{12}-1 = (n^2-1)(n^{10}+n^8+\cdots+n^2+1)$$

e $3|n$ *ou, pelo PTF,* $n^2 \equiv 1 \pmod 3$ *isto é* $3|n^2-1$.

$5|(n^{13}-n)$ *para todo n pois*

$$n^{13}-n = n(n^{12}-1) \quad e \quad n^{12}-1 = (n^4-1)(n^8+n^4+1)$$

e $5|n$ *ou, pelo PTF,* $n^4 \equiv 1 \pmod 5$ *isto é* $5|n^4-1$.

A recíproca do teorema de Fermat não é verdadeira, mas vale o seguinte resultado.

Teorema 124 (Teorema de Lucas)**.** *Sejam* $a, n > 1$ *inteiros tais que* $\mathrm{mdc}(a,n) = 1$, $a^{n-1} \equiv 1 \pmod n$ *e* $a^k \not\equiv 1 \pmod n$ *para todo* $k \in \{1,2,\ldots,n-2\}$ *então n é primo.*

Demonstração. Do Teorema de Euler temos $a^{\varphi(n)} \equiv 1 \pmod n$, portanto, por hipótese, $\varphi(n) \geq n-1$, donte temos $\varphi(n) = n-1$. O teorema segue do exercício 118. □

9.3.1 Ordem e raizes primitivas

Proposição 125. *Seja* $a > 1$ *um inteiro. Existe um inteiro positivo h tal que* $a^h \equiv 1 \pmod n$ *se, e só se,* $\mathrm{mdc}(a,n) = 1$.

Demonstração. Se $\mathrm{mdc}(a,n) = 1$, basta tomar $h = \varphi(n)$. Por outro lado, se $\mathrm{mdc}(a,n) \neq 1$, então $aX \equiv 1 \pmod n$ não tem solução (proposição 119), portanto não existe $h > 1$ tal que $a^h \equiv 1 \pmod n$. □

Definimos

$$\mathrm{ord}_n(a) := \min\{h \in \mathbb{Z}^+ : a^h \equiv 1 \pmod n\}. \tag{60}$$

Lema 126. *Sejam* $a, n > 1$ *inteiros coprimos.*

$$a^m \equiv 1 \pmod n \iff \mathrm{ord}_n(a)|m.$$

Demonstração. Se $m = \text{ord}_n(a) \cdot q$ então

$$a^m = (a^{\text{ord}_n(a)})^q \equiv 1 \; q = 1 \pmod{n}.$$

Por outro lado, suponha $a^m \equiv 1 \pmod{n}$ e tome q e $r < \text{ord}_n(a)$ dados pelo Teorema da Divisão com $m = \text{ord}_n(a) \cdot q + r$

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

o que é contradição pois $r < \text{ord}_n(a)$. □

Corolário 127. *Se $a, n > 1$ são inteiros coprimos então* $\text{ord}_n(a) | \varphi(n)$.

Dizemos que a é uma **raiz primitiva** módulo n se $\text{ord}_n(a) = \varphi(n)$. Pr exemplo, 2 é raiz primitiva módulo 5

Proposição 128. *Todo divisor do número de Fermat $F_n = 2^{2^n} + 1$ é da forma $2^{n+1}k + 1$.*

Demonstração. Note que $(2^{n+1}k + 1)(2^{n+1}k' + 1) = 2^{n+1}k'' + 1$ de modo que é suficiente provar a proposição para os divisores primos de F_n.

Seja p um divisor primo de $2^{2^n} + 1$. Então $2^{2^n} \equiv -1 \pmod{p}$ de modo que $\text{ord}_p(2) \not| 2^n$.

Entretanto $\left(2^{2^n}\right)^2 \equiv 1 \pmod{p}$ de modo que $\text{ord}_p(2) | 2^{n+1}$.

De $\text{ord}_p(2) \not| 2^n$ e $\text{ord}_p(2) | 2^{n+1}$ temos $\text{ord}_p(2) = 2^{n+1}$.

Pelo PTF, $2^{p-1} \equiv 1 \pmod{p}$ logo $\text{ord}_p(2) | p - 1$, ou seja, existe k tal que $p = 2^{n+1}k + 1$. □

9.3.2 Solução de congruência linear

Se $\text{mdc}(a, n) = 1$ então

$$aX \equiv b \pmod{n} \tag{61}$$

tem solução $x = a^{\varphi(n)-1}b$ e qualquer outra solução x_0 é congrua a x módulo n, i.e., a solução

$$x \equiv a^{\varphi(n)-1}b \pmod{n} \tag{62}$$

é única módulo n de modo que todas as soluções da congruência linear são

$$x = a^{\varphi(n)-1}b + tn, \qquad \forall\, t \in \mathbb{Z}. \tag{63}$$

Agora, se $\text{mdc}(a, n) = d > 1$ e a equação (61) tem solução, então a congruência (61) tem as mesmas soluções de

$$\frac{a}{d}X \equiv \frac{b}{d} \pmod{\frac{n}{d}} \tag{64}$$

de modo que, agora $\text{mdc}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ e a única solução de (64) é

$$x = \left(\frac{a}{d}\right)^{\varphi(\frac{n}{d})-1} \frac{b}{d} \tag{65}$$

e as d soluções módulo n de (61)são

$$x \equiv \left(\frac{a}{d}\right)^{\varphi(\frac{n}{d})-1} \frac{b}{d} + \frac{n}{d}t \pmod{n}, \qquad \forall\, t \in \{0,1,\ldots,d-1\}. \tag{66}$$

Exercícios

1. Se $n = kd$ então $|\{m\colon 1 \le m \le n \text{ e } \mathrm{mdc}(m,n) = d\}| = \varphi(k)$.
2. Mostre que se p é primo ímpar então $\{\pm 1, \pm 2, \ldots, \pm(p-1)/2\}$ é um sci módulo n.
3. Mostre que se $\mathrm{mdc}(a,n) = 1$ então

$$i \equiv j \pmod{\varphi(n)} \Rightarrow a^i \equiv a^j \pmod{n}.$$

4. Mostre que 7 e 13 dividem $n^{13} - n$ para todo n.
5. Mostre que $2730 | n^{13} - n$.
6. Seja p primo.
   (a) Prove que p divide $\binom{p}{i}$ para todo $i \in \{1,2,\ldots,p-1\}$.
   (b) Prove que para inteiros x e y vale $(x+y)^p \equiv x^p + y^p \pmod{p}$.
   (c) Prove, usando indução, que $n^p \equiv n \pmod{p}$ para todo natural $n \ge 1$.
   (d) Deduza (59) a partir dos resultados obtidos acima.
7. Use o Pequeno Teorema de Fermat para provar que
   (a) $13 | (2^{70} + 3^{70})$.
   (b) $9 | (n^3 + (n+1)^3 + (n+2)^3)$.
   (c) $X^{13} + 12X + 13Y^6 = 1$ não admite solução inteira.

RSA

Relembrando o protocolo de criptografia RSA:

1. Escolha dois números primos p e q e compute $n := p \cdot q$;
2. Compute $\varphi(n) = (p-1)\cdot(q-1)$;
3. Escolha $e \in \{2,3,\ldots\varphi(n)-1\}$ com $\mathrm{mdc}(e,\varphi(n)) = 1$; disponibilize o par (e,n), é a sua **chave pública**.
4. Compute d tal que $d \cdot e \equiv 1 \pmod{\varphi(n)}$ e mantenha-o em segredo, a **chave privada** é o par (d,n).

Consideremos que uma mensagem é um natural $m \in \mathbb{Z}$ (por exemplo, m é o número representado em base 2 que o computador usa para gravar o arquivo com a mensagem no HD) tal que $m < n$ (isso não é uma restrição que põe tudo a perder, como foi explicado em sala, basta considerar o binário em blocos).

Para eu mandar-lhe a mensagem m criptografada busco pela sua chave pública e calculo $c := m^e \bmod n$ e o envio. Você, que é o único portador da chave privada, calcula a $c^d \bmod n$ e tem de volta a mensagem m.

$$c^d \bmod n = (m^e \bmod n)^d \bmod n$$

Notemos que, quaisquer inteiros a e $k \geq 0$, vale $a^k \equiv (a \bmod n)^k \pmod{n}$. Assim, $c^d \equiv (m^e)^d \pmod{n}$ e de $ed = 1 + r\varphi(n)$ para algum $r \in \mathbb{Z}$

$$m^{ed} = m^{1+r\varphi(n)} = m\left(m^{p-1}\right)^{(q-1)r}$$

Se $p \nmid m$ então

$$m\left(m^{p-1}\right)^{(q-1)r} \equiv m \pmod{p} \tag{67}$$

pois $m^{p-1} \equiv 1 \pmod{p}$ pelo Pequeno Teorema de Fermat. Também, $m^{ed} \equiv m \pmod{p}$ se $p|P$, ou seja,

$$m^{ed} \equiv m \pmod{p}. \tag{68}$$

Analogamente, vale

$$m^{ed} \equiv m \pmod{q}. \tag{69}$$

De (68) e (69) temos que $pq|m^{ed} - m$, ou seja, $m^{ed} \equiv m \pmod{n}$. Como $m < n$, temos $m^{ed} \bmod n = m$.

10 Congruências lineares e sistemas de congruências

Dados inteiros a, b não nulos e $n > 0$ vamos estudar as soluções da **congruência linear em uma variável** com incógnita X

$$aX \equiv b \pmod{n}. \tag{70}$$

Uma *solução* dessa congruência linear é um inteiro x tal que $ax \equiv b \pmod{n}$ e uma *solução módulo n* é um inteiro x tal que $x \in \{0, 1, \ldots, n-1\}$ (ou qualquer outro s.c.r. previamente escolhido) e $ax \equiv b \pmod{n}$.

Por definição, existe um inteiro x tal que $ax \equiv b \pmod{n}$ se, e somente se, $ax - b$ é um múltiplo de n, ou seja, existe $y \in \mathbb{Z}$ tal que $ax - b = ny$ que reescrevemos como

$$ax + ny = b \tag{71}$$

Pelo Teorema de Bézout a existência de inteiros x e y que satisfazem a equação acima é equivalente a $\text{mdc}(a,n)|b$, além disso, se x_0 é uma solução particular então todas as soluções x da equação (71) são (teorema 85)

$$x_t := x_0 + \frac{n}{\text{mdc}(a,n)}t, \qquad \forall\, t \in \mathbb{Z} \tag{72}$$

portanto uma congruência linear que tem solução, tem infinitas soluções. Vejamos quando duas dessas infinitas soluções são congruentes módulo n. Façamos $d := \text{mdc}(a,n)$ $(d > 0)$

$$\begin{aligned} x_t \equiv x_s \pmod{n} &\Leftrightarrow x_0 + \frac{n}{d}t \equiv x_0 + \frac{n}{d}s \pmod{n} \\ &\Leftrightarrow \frac{n}{d}t \equiv \frac{n}{d}s \pmod{n} \end{aligned}$$

e como $\text{mdc}(\frac{n}{d}, n) = \frac{n}{d}$ temos, pelo lema 106 que

$$x_t \equiv x_s \pmod{n} \Leftrightarrow t \equiv s \pmod{d}$$

portanto, quando há solução, há exatamente $d = \text{mdc}(a,n)$ soluções incongruentes x_t com $t \in \{0,1,\ldots,d-1\}$ (ou em qualquer sistema completo de restos mod d).

Ademais, se $x \in \mathbb{Z}$ é solução então $ax \equiv ax_0 \pmod{n}$ de modo que $x_0 \equiv x \pmod{\frac{n}{d}}$, ou seja $x_o - x = k\frac{n}{d}$. Pelo algoritmo da divisão podemos escrever $x - x_0 = (dq + r)\frac{n}{d}$, logo, $x - x_0 = nd + r\frac{n}{d}$ donde concluímos que

$$x \equiv x_0 + r\frac{n}{d} \pmod{n}$$

para algum $r \in \{0,1,\ldots,d-1\}$

Teorema 129. *Uma congruência linear em uma variável* $aX \equiv b \pmod{n}$ *admite solução inteira se e somente se* $\text{mdc}(a,n)|b$. *No caso de haver solução, se* $x_0 \in \{0,1,\ldots,n-1\}$ *é solução então*

$$\left\{x_0 + \frac{n}{\text{mdc}(a,n)}t\colon\ t \in \mathbb{Z}\right\}$$

são todas as soluções e

$$\left\{x_0 + \frac{n}{\text{mdc}(a,n)}t\colon\ t \in \{0,1,\ldots,\text{mdc}(a,n)-1\}\right\}$$

são todas as soluções módulo n da congruência. □

Por exemplo, $3X \equiv 6 \pmod{15}$ é satisfeita por todo inteiro x da forma $2+5t$ $(t \in \mathbb{Z})$ e $2,7,12$ são três soluções incongruentes módulo 15.

Corolário 130. *Se* $\text{mdc}(a,n) = 1$ *então* $aX \equiv b \pmod{n}$ *tem única solução módulo n.*

Por exemplo, $3X \equiv 1 \pmod{5}$ tem solução e como 3 e 5 são coprimos a solução módulo 5 é única. Uma solução para a equação é $x = 2$, portanto, toda solução inteira x é da forma $x = 2+5t$, portanto se x é solução então

$$x \equiv 2 \pmod{5}.$$

Notemos que toda solução de $3X \equiv 1 \pmod 5$ também é solução de $X \equiv 2 \pmod 5$, ademais 2 é o inverso multiplicativo de 3 módulo 5.

A equação $2X \equiv 3 \pmod 9$ também tem única solução módulo 9, que é 6, donde temos que $6+9t$ são todas as soluções, ou seja, se x é solução então $x \equiv 6 \pmod 9$; de novo, notemos que toda solução de $2X \equiv 3 \pmod 5$ também é solução de $X \equiv 6 \pmod 9$. Esse fato não é um particularidade desses exemplos.

Proposição 131. *Sejam $a, n \in \mathbb{Z}$ inteiros quaisquer, não nulos e $d := \mathrm{mdc}(a,n)$; $b \in d \cdot \mathbb{Z}$. As equações*

$$aX \equiv b \pmod n \quad e \quad \frac{a}{d}X \equiv \frac{b}{d} \pmod{\frac{n}{d}} \tag{73}$$

têm as mesmas soluções.

Demonstração. Para quaisquer $x, y \in \mathbb{Z}$

$$ax + ny = b \Leftrightarrow \frac{a}{d}x + \frac{n}{d}y = \frac{b}{d}.$$

□

Como $\mathrm{mdc}(\frac{a}{d}, \frac{n}{d}) = 1$, usamos a proposição 119 para termos o inverso a' de $\frac{a}{d}$ módulo $\frac{n}{d}$ logo

$$\frac{a}{d}X \equiv \frac{b}{d} \pmod{\frac{n}{d}} \Leftrightarrow X \equiv a'\frac{b}{d} \pmod{\frac{n}{d}}$$

portanto

Proposição 132.

$$aX \equiv b \pmod n \quad e \quad X \equiv a'\frac{b}{d} \pmod{\frac{n}{d}} \tag{74}$$

têm as mesmas soluções. □

Ademais, todas as soluções inteiras de $X \equiv a'\frac{b}{d} \pmod{\frac{n}{d}}$ são dadas por

$$a'\frac{b}{d} + \frac{n}{d}t, \quad \forall t \in \mathbb{Z}$$

e todo inteiro dessa forma é congruente a algum de

$$a'\frac{b}{d} + \frac{n}{d}t, \quad \forall t \in \{0, 1, 2, \ldots, d-1\}.$$

Em vista desse último resultado vamos, na próxima seção, considerar apenas equações da forma $X \equiv c \pmod n$ pois sempre que uma equação da forma $aX \equiv b \pmod n$ tem solução ela é equivalente a uma equação da primeira forma.

10.1 Teorema chinês do resto

Consideremos o seguinte sistema de congruências lineares

$$\begin{cases} X \equiv 2 \pmod 5 \\ X \equiv 6 \pmod 9 \\ X \equiv 5 \pmod{11} \end{cases}$$

se a primeira congruência é satisfeita por $x \in \mathbb{Z}$ então $x = 2+5t$, para algum t, que para satisfazer a segunda congruência deve valer $2+5t \equiv 6 \pmod 9$, que equivale a $5t \equiv 4 \pmod 9$ que, como 5 tem inverso 2 módulo 9, equivale a $t \equiv 8 \pmod 9$ donde $t = 8+9s$, logo

$$x = 2+5t = 2+5(8+9s) = 42+45s.$$

Observemos que para cada $s \in \mathbb{Z}$ o valor de x associado satisfaz as duas primeiras congruências lineares do sistema. Agora, para x satisfazer a última congruência linear $42+45s \equiv 5 \pmod{11}$ que equivale a $45s \equiv -37 \pmod{11}$ ou ainda $45s \equiv 7 \pmod{11}$. Como 45 é invertível módulo 11, e seu inverso é 1, a última congruência equivale a $s \equiv 7 \pmod{11}$, ou seja, $s = 7+11u$, portanto

$$x = 42+45r = 42+45(7+11u) = 357+495u$$

ou seja, para cada $u \in \mathbb{Z}$ o inteiro x associado satisfaz o sistema de congruências lineares acima. De fato, essas são todas as soluções inteiras, e a única solução módulo $495 = 5 \cdot 9 \cdot 11$ é 357

$$x \equiv 357 \pmod{5 \cdot 9 \cdot 11}.$$

No caso geral, consideremos o sistema de congruências lineares

$$\begin{cases} X \equiv a \pmod n \\ X \equiv b \pmod m \end{cases} \tag{75}$$

a primeira congruência linear tem soluções inteiras $a+nt$, para $t \in \mathbb{Z}$. Dos inteiros que satisfazem a primeira congruência, substituindo em X na segunda congruência linear, temos os inteiros que satisfazem as duas congruências concomitantemente, que são dados pelos inteiros t tais que $a+nt \equiv b \pmod m$, ou seja, as soluções de

$$nX \equiv b-a \pmod m \tag{76}$$

caso existam. Portanto,

$$(75) \textit{ tem solução se e só se } \mathrm{mdc}(m,n) | b-a. \tag{77}$$

ou ainda (75) tem solução se e só se

$$b \equiv a \pmod{\text{mdc}(m,n)}. \tag{78}$$

Garantimos essa condição exigindo que $\text{mdc}(m,n) = 1$

Observação 133. *A hipótese* $\text{mdc}(m,n) = 1$ *é suficiente mas não é necessária para que* $\text{mdc}(m,n)|b-a$.

Ademais, se $\text{mdc}(m,n) = 1$ então n tem inverso n' módulo m, portanto, t é solução de (76) se, e só se,

$$t \equiv n'(b-a) \pmod{m}$$

ou seja $t = n'(b-a)+ms$, para todo $s \in \mathbb{Z}$, portanto, se x é uma solução inteira do sistema de congruências então, para algum s,

$$x_s = a + nt = a + n(n'(b-a) + ms) = (1-nn')a + nn'b + nms$$

e, ainda, $1 - nn' = mm'$ para algum $m' \in \mathbb{Z}$ (segue do teorema de Bézout, m' é o inverso de m módulo n), o que resulta em

$$x_s = mm'a + nn'b + nms, \tag{79}$$

e o valor de x_s é uma solução inteira para ambas congruências para cada $s \in \mathbb{Z}$.

De fato, todas as soluções são da forma (79). Se $x, y \in \mathbb{Z}$ satisfazem ambas as equações acima, então por transitividade vale que $x \equiv y \pmod{n}$ e $x \equiv y \pmod{m}$, donde $n|(x-y)$ e $m|(x-y)$ e como $\text{mdc}(m,n) = 1$ temos (exercício 81) $mn|(x-y)$, isto é, $x \equiv y \pmod{mn}$.

Portanto, a *única* solução módulo mn é

$$x \equiv mm'a + nn'b \pmod{mn}. \tag{80}$$

Observamos que esse caso é suficiente para resolver um sistema com qualquer número de congruências lineares, como os módulos coprimos dois-a-dois, resolvendo-as duas-a-duas. No entanto, podemos generalizar a demonstração acima, o que fazemos abaixo.

O seguinte resultado é o famoso Teorema Chinês do Resto. A forma original do teorema apareceu no livro *Sun Tzu Suan Ching* (manual de aritmética de Sun Tzu) do terceiro-século e generalizado e republicado em 1247 por Qin Jiushao.

Teorema 134 (Teorema Chinês do Resto)**.** *Sejam* $n_1, n_2, \ldots, n_k$ *inteiros maiores que 1 e tais que* $\text{mdc}(n_i, n_j) = 1$ *para todos* $i \neq j$*, e sejam* $a_1, \ldots, a_k$ *inteiros arbitrários. Então o sistema de congruências lineares*

$$X \equiv a_i \pmod{n_i}, \quad \forall i \in \{1,2,\ldots,k\}. \tag{81}$$

tem uma única solução módulo $n = n_1 n_2 \cdots n_k$ dada por

$$m_1' m_1 a_1 + m_2' m_2 a_2 + \cdots + m_k' m_k a_k \tag{82}$$

em que $m_i = \frac{n_1 n_2 \cdots n_k}{n_i}$ e m_i' é o inverso multiplicativo de m_i módulo n_i, para todo $i \in \{1, 2, \ldots, k\}$. A solução é única módulo $n_1 \cdot n_2 \cdots n_k$.

Demonstração. Notemos que $\text{mdc}(m_i, n_i) = 1$, logo m_i' existe para todo i. Tomamos $x_0 := \sum_{i=1}^{k} m_i' m_i a_i$ e vamos mostrar que é solução.

Para cada i temos

$$m_j \equiv 0 \pmod{n_i} \quad (\forall\, j \neq i)$$

logo

$$x_0 \equiv m_i' m_i a_i \pmod{n_i} \quad (\forall\, i \in \{1, \ldots, k\}).$$

e $m_i m_i' \equiv 1 \pmod{n_i}$ logo $m_i' m_i a_i \equiv a_i \pmod{n_i}$, portanto

$$x_0 \equiv a_i \pmod{n_i}$$

para todo i, ou seja, x_0 é solução de cada congruência linear.

Agora vamos mostrar que a solução é única módulo n. Assuma que para $x \in \mathbb{Z}$ vale $x \equiv a_i \pmod{n_i}$ para todo i. Por transitividade $x \equiv x_0 \pmod{n_i}$ para todo i, portanto para todo i, $n_i | (x - x_0)$ e pela coprimalidade dos n_i's temos $\prod_{i=1}^{k} n_i | (x - x_0)$. □

Exemplo 135. *Considere o sistema*

$$\begin{cases} X \equiv 2 \pmod{2} \\ X \equiv -1 \pmod{3} \\ X \equiv 4 \pmod{7}. \end{cases}$$

Seguindo a notação da demonstração, $n = 42$, $m_1 = 21$, $m_2 = 15$ e $m_3 = 6$.

i	m_i'	m_i
1	1	21
2	−1	14
3	−1	6

e $x_0 = 2 \cdot 1 \cdot 21 + (-1)(-1)14 + 4(-1)6 = 32$. Ainda, toda solução inteira é da forma $32 + 42t$, para todo $t \in \mathbb{Z}$.

Exercício 136. *Mostre que as soluções do exemplo 135 são soluções do sistema*

$$\begin{cases} 6X \equiv 4 \pmod{4} \\ 2X \equiv 1 \pmod{3} \\ 4X \equiv 2 \pmod{7}. \end{cases}$$

Variantes do TCR

Exercício 137. *Vimos em* (78) *acima que*

$$\begin{cases} X \equiv a \pmod{n} \\ X \equiv b \pmod{m} \end{cases}$$

tem solução apenas quando $a \equiv b \pmod{\text{mdc}(n,m)}$. *Prove que nesse caso a solução é unica módulo* $\text{mmc}(n,m)$.

Exercício 138. *Verifique a seguinte versão do Teorema Chinês do Resto: Sejam* $n_1, n_2, \ldots, n_k$ *inteiros maiores que 1 e sejam* $a_1, \ldots, a_k$ *inteiros arbitrários. Então o sistema*

$$X \equiv a_i \pmod{n_i}, \quad \forall i \in \{1,2,\ldots,k\}. \tag{83}$$

tem solução se e somente se $\text{mdc}(n_i, n_j) | a_i - a_j$ *para todo* $i \neq j$. *Caso exista, a solução é única módulo* $\text{mmc}(n_1, n_2, \ldots, n_k)$. *(Dica: indução e o exercício 109.)*

Exercício 139. *Sejam* $n_1, n_2, \ldots, n_k$ *inteiros maiores que 1, e sejam* $a_1, \ldots, a_k$ *e* $b_1, \ldots, b_k$ *inteiros arbitrários tais que* $\text{mdc}(a_i, n_i) | b_i$ *para todo* i. *Prove que o sistema*

$$a_i X \equiv b_i \pmod{n_i}, \quad \forall i \in \{1,2,\ldots,k\}. \tag{84}$$

tem solução.

Compartilhar segredos usando o TCR

O problema é: dados inteiros $n > k \geq 1$ determinar uma estratégia para que n pessoas partilhem uma senha $s \in \mathbb{Z}$ sem conhece-la de modo que

1. qualquer subconjunto de k pessoas permite calcular s facilmente,
2. para menos que k pessoas quaisquer é muito difícil computar s.

A ideia é tomar uma lista $L = \{m_1 < m_2 < \cdots < m_n\}$ números inteiros tais que $\text{mdc}(m_i, m_j) = 1$ para todo $i \neq j$ e escolher s

$$N < s < M \tag{85}$$

onde $N = m_1 m_2 \cdots m_k$ (produto dos k menores) e $M = m_{n-k+2} m_{n-k+3} \cdots m_n$ (produto dos $k-1$ maiores).

Note que o produto de quaisquer k números de L é maior que N, o produto de menos que k é menor que M e $s > m$ para todo $m \in L$. Cada pessoa recebe um par (m, s_m) com $m \in L$ e $s_m = s \bmod m$. Note que $s > s_m$.

Em um grupo de t pessoas temos o sistema

$$X \equiv s_i \pmod{m_i} \quad \forall i \in \{1,2,\ldots,t\} \tag{86}$$

cuja solução $x_0 \equiv s \pmod{m_1 m_2 \cdots m_t}$. Agora,

$t \geq k$: nesse caso $m_1 m_2 \cdots m_t \geq N > s$ e, pelo teorema chinês do resto, existe uma única solução x_0 módulo $m_1 m_2 \cdots m_t$, como s é solução $x_0 = s$.

$t < k$: nesse caso $m_1 m_2 \cdots m_t < M < s$ e $x_0 \neq s$, mas como s é solução devemos ter $s = x_0 + y(m_1 m_2 \cdots m_t)$, com

$$M < x_0 + y(m_1 \cdots m_t) < N, \tag{87}$$

e podemos escolher os módulos de modo que esse intervalo seja muito grande, o que torna a busca por y inviável.

Como exercício, verifique o protocolo acima de partilha de senha para o caso $k = 2$ com $L = \{11, 13, 17, 19, 23\}$.

A função de Euler é multiplicativa — demonstração usando o TCR

Vamos dar uma demonstração alternativa para *Se $n, m \in \mathbb{Z}^+$ são coprimos então $\varphi(nm) = \varphi(n)\varphi(m)$* usando o teorema chinês do resto.

Demonstração. O caso $m = 1$ ou $n = 1$ é imediato. Sejam $n, m > 1$ inteiros. Definimos os conjuntos

$$A := \{a \in \mathbb{N} \colon \text{mdc}(a, nm) = 1 \text{ e } 1 \leq a \leq nm\}$$
$$B := \{b \in \mathbb{N} \colon \text{mdc}(b, n) = 1 \text{ e } 1 \leq b \leq n\}$$
$$C := \{c \in \mathbb{N} \colon \text{mdc}(c, m) = 1 \text{ e } 1 \leq c \leq m\}$$

portanto o enunciado do teorema afirma que $|A| = |B| \cdot |C|$. Vamos mostrar uma bijeção entre A e $B \times C$. Primeiro, mostraremos que a função

$$\begin{aligned} f \colon A &\to B \times C \\ a &\mapsto (a \bmod n, a \bmod m) \end{aligned}$$

está bem definida. Tomemos $a \in A$. Observemos que $n, m \nmid a$ pois se a é múltiplo de $n > 1$ ou múltiplo de $m > 1$ então $\text{mdc}(a, nm) > 1$, o que contraria $a \in A$. Portanto $(a \bmod n, a \bmod m) \neq (0,0)$. Ainda

$$\text{mdc}(a, nm) = 1 \Rightarrow \text{mdc}(a, n) = 1 \text{ e } \text{mdc}(a, m) = 1 \tag{88}$$

pois existem $x, y \in \mathbb{Z}$ tais que $ax + nmy = 1$ donde temos que $aX + nY = 1$ tem solução e $aX + mY = 1$ tem solução, portanto, $\text{mdc}(a, n) = \text{mdc}(a, m) = 1$ pelo corolário 84. Finalmente, do algoritmo de Euclides

$$\text{mdc}(a \bmod n, n) = \text{mdc}(a, n) = 1 \text{ e}$$
$$\text{mdc}(a \bmod m, m) = \text{mdc}(a, m) = 1$$

de modo que para cada a há único $f(a) \in B \times C$.

Para provar o teorema, vamos mostrar que a função f é uma bijeção. Sejam a_1 e a_2 são elementos de A. Se $f(a_1) = f(a_2)$ então $a_1 \bmod n = a_2 \bmod n$ e $a_1 \bmod m = a_2 \bmod m$ portanto

$$a_1 \equiv a_2 \pmod{n}$$
$$a_1 \equiv a_2 \pmod{m}$$

logo $a_1 \equiv a_2 \pmod{nm}$ (pelo exercício 81 é proposição 33), e como $1 \leq a_1, a_2 \leq nm$ temos $a_1 = a_2$. Portanto a função é injetiva.

Resta provar que a função é sobrejetiva. Seja (b, c) um elemento qualquer de $B \times C$, isto é, $1 \leq b \leq n$, $1 \leq c \leq m$, $\text{mdc}(b, n) = 1$ e $\text{mdc}(c, m) = 1$. Como $\text{mdc}(n, m) = 1$ o Teorema Chinês do Resto garante que há uma única solução a módulo nm para o sistema de congruências

$$\begin{cases} X \equiv b \pmod{n} \\ X \equiv c \pmod{m} \end{cases}$$

portanto $(a \bmod n, a \bmod m) = (b, c)$, ademais, $\text{mdc}(a, nm) = 1$ pela recíproca de (88) (veja exercício 32, item 6). □

Exercícios

1. Num teatro duas tropas se enfrentam numa cena de batalha. Uma tropa tem 100 mosquetes e depois de atirar tantos tiros quanto possíveis lhes sobraram 13 cartuchos. A outra tropa tem 67 mosquetes e ao fim lhes restam 32 cartuchos. Supondo que a cada salva de tiros cada soldado atirou apenas uma vez determine o número mínimo de cartuchos de cada tropa no início da apresentação.

2. Resolva $X^2 + 42X + 21 \equiv 0 \pmod{105}$. (Dica: fatore 105 e resolva a equação para módulo cada fator e use o teorema chinês do resto)

3. A teoria do Biorritmo diz que os estados físico, mental e emocional de uma pessoa oscilam periodicamente, a partir do dia do nascimento, em ciclos de 23, 29 e 33 dias, respectivamente. Dado

que os dias mais positivos dos ciclos físico, mental e emocional são, respectivamente, o 6º, o 7º e o 8º dias de cada ciclo, quantas vezes os três ciclos estão simultaneamente no ponto máximo nos primeiros 10 anos de vida?

4. Verifique que

$$\begin{cases} X \equiv -1 \pmod 4 \\ X \equiv 2 \pmod 6 \end{cases}$$

não tem solução.

5. Verifique que $x \equiv 3 \pmod{12}$ é solução de

$$\begin{cases} X \equiv -1 \pmod 4 \\ X \equiv 3 \pmod 6 \end{cases}$$

(note os módulos não-coprimos).

6. Mostre que $x \equiv 3 \pmod{24}$ é solução de

$$\begin{cases} X \equiv 3 \pmod{12} \\ X \equiv 19 \pmod 8 \end{cases}$$

7. Mostre que

$$\begin{cases} X \equiv a \pmod n \\ X \equiv b \pmod m \end{cases}$$

tem no máximo uma solução módulo $\text{mmc}(n,m)$ (não estamos assumindo coprimalidade).

8. Sejam $p \neq q$ primos, $n = pq$. Digamos que conhecemos uma solução para $X^2 \equiv a \pmod p$ e $X^2 \equiv a \pmod q$. Mostre como usar o teorema chinês do resto para achar solução de $X^2 \equiv a \pmod n$.

9. 3 satélites passarão sobre SA esta noite. O primeiro a 1h da manha, o segundo as 4h e o terceiro as 8h. O primeiro leva 13hs para completar uma volta, o segundo 15h e o terceiro 19h. Quantas horas decorrerão, a partir da meia-noite até que os 3 passam ao mesmo tempo sobre SA.

10. Determine um número que dividido por 3,5,7 de restos 2,3,2

11 Restos quadráticos

Sejam p primo e a, b, c inteiros com a não divisível por p. Notemos que para qualquer inteiro x

$$\begin{aligned} ax^2+bx+c &\equiv 0 \pmod{p} \quad \Leftrightarrow \quad \text{(completando quadrados)} \\ (2ax+b)^2 &\equiv b^2-4ac \pmod{p} \end{aligned}$$

assim, estamos interessados nas soluções módulo p de $X^2 \equiv d \pmod{p}$ (se assumimos que $p>2$ então a e 2 são invertíveis mod p e resolvemos paa x) ou, mais precisamente, determinar quando existe solução.

O caso $d=0$ é trivial, assim como não é difícil mostrar que módulo 2 sempre há solução (justifique), de modo que reformulamos a discussão como segue.

Sejam p um primo ímpar e a um inteiro não divisível por p; dizemos que a é um **resíduo (ou resto) quadrático módulo** p se

$$X^2 \equiv a \pmod{p} \tag{89}$$

tem solução em $\{1,\ldots,p-1\}$.

Por exemplo, 2 não é um resto quadrático módulo 3; módulo 5 temos $0^2 \equiv 0$, $1^2 \equiv 1 \equiv 4^2$, $2^2 \equiv 4 \equiv 3^2$, ou seja, 2 e 3 não são resíduos quadráticos módulo 5.

Notemos que se x é uma solução de (89), então $-x$ também é solução; se y é outra solução então $y^2 \equiv a \equiv x^2 \pmod{p}$, logo $y^2-x^2 \equiv 0 \pmod{p}$ e

$$\begin{aligned} y^2-x^2 \equiv 0 \pmod{p} \quad &\Leftrightarrow \quad (y-x)(y+x) \equiv 0 \pmod{p} \\ &\Leftrightarrow \quad (y-x) \equiv 0 \pmod{p} \text{ ou } (y+x) \equiv 0 \pmod{p} \\ &\Leftrightarrow \quad y \equiv x \pmod{p} \text{ ou } y \equiv -x \pmod{p} \end{aligned}$$

agora ou $x \equiv -x \pmod{p}$ caso em que há uma única solução módulo p de (89), ou $x \not\equiv -x \pmod{p}$ caso em que há exatamente duas soluções módulo p de (89).

Porém, $x \equiv -x \pmod{p} \Leftrightarrow 2x \equiv 0 \pmod{p} \Leftrightarrow p|x$ ou $p|2$. Como $p \not| a$, também $p \not| x^2$, portanto $p \not| x$, e como p é ímpar segue que $x \not\equiv -x \pmod{p}$. Provamos

Proposição 140. *Sejam $p>2$ primo e a inteiro não-múltiplo de p. Se $X^2 \equiv a \pmod{p}$ tem solução então tem duas soluções módulo p.* □

Exercício 141. *Mostre que $(p-1)/2$ inteiros de $\{1,2,\ldots,p-1\}$ são restos quadráticos módulo $p>2$.*

Solução. $\{0,\pm 1,\pm 2,\ldots,\pm(p-1)/2\}$ é um scr, portanto, x^2 é congruente a algum de $\{0^2,1^2,2^2,\ldots,((p-1)/2)^2\}$, para todo inteiro x. Ainda quaisquer dois desses quadrados são incongruentes mod p. Excluindo o 0 dá a resposta. □

Apesar desse exercício, na prática pode ser difícil decidir se um número é ou não é um resíduo quadrático.

Seja x uma solução da congruência de grau 2. Considerando o caso que $x^2 \equiv a \pmod{p}$ com $x \in \{1,\ldots,p-1\}$, notemos que

$$(p-1)! = 1\cdot 2\cdots x\cdots(p-x)\cdots(p-2)\cdot(p-1)$$

Para cada fator $a_0 \in \{1,2,\ldots,p-2,p-1\}$ do fatorial acima a equação $a_0 X \equiv a \pmod{p}$ admite uma solução x_0 módulo p, $1 \leq x_0 \leq p-1$. Ademais, se $a_0 \neq x, p-x$ então $x_0 \neq a_0$. Em outras palavras, exceto por x e $p-x$, os fatores do produto podem ser agrupados aos pares $\{a_0, x_0\}$ de modo que $a_0 x_0 \equiv a \pmod{p}$, i.e.

$$1\cdot 2\cdots(x-1)(x+1)\cdots(p-x-1)(p-x+1)\cdots(p-2)\cdot(p-1) \equiv a^{\frac{p-3}{2}} \pmod{p}$$

portanto

$$(p-1)! \equiv a^{\frac{p-3}{2}} x(p-x) \pmod{p} \tag{90}$$

e como $x(p-x) \equiv x(-x) \equiv -x^2 \equiv -a \pmod{p}$, temos

$$(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p} \tag{91}$$

Agora, no caso que $X^2 \equiv a \pmod{p}$ não tem solução, para cada resto r do conjunto $R := \{1,2,\ldots,p-1\}$, existe um único resto $r' \in R$ tal que $r' \neq r$ e $rr' \equiv a \pmod{p}$ portanto

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{92}$$

Com isso temos o seguinte resultado,

Proposição 142. *Sejam $a \in \mathbb{Z}$ e $p > 2$ primo. Se* $\mathrm{mdc}(p,a) = 1$ *então*

1. *se a é um resto quadrático módulo p então* $(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p}$*;*
2. *se a não é um resto quadrático módulo p então* $(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$. □

11.1 O Teorema de Wilson

O seguinte resultado foi enunciado por Ibn al-Haytham[7] e por e John Wilson[8]. Edward Waring[9] anunciou o teorema em 1770, embora nem ele nem seu aluno Wilson deram uma prova. Lagrange deu a primeira prova em 1771.

[7] nasceu no ano 965 em Basra (Iraque) e morreu em 1040 na cidade do Cairo. Físico e matemático árabe. Pioneiro da Óptica, depois de Ptolomeu. Um dos primeiros a explicar o fenômeno dos corpos celestes no horizonte.

[8] matemático inglês do fim do século 18

[9] orientador de Wilson, *Lucasian Professor of Mathematics* na Universidade de Cambridge que é uma das mais prestigiadas cátedras no mundo, já foi ocupada por Isaac Newton, Paul Dirac e Stephen Hawking entre outros.

Teorema 143 (**Teorema de Wilson**)**.** *p é primo se, e somente se,* $(p-1)! \equiv -1 \pmod{p}$.

Demonstração. Seja p um primo. O caso $p = 2$ é imediato, portanto supomos $p > 2$. 1 é um resíduo quadrático módulo p, portanto, $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Seja p composto. Se $p = 4$ então $(p-1)! \equiv 6 \not\equiv -1 \pmod{4}$. Se $p > 4$ então $p = ab$ com $1 < a, b < p$. Se $a \neq b$ então a e b ocorrem em $(p-1)!$ portanto $p|(p-1)!$; agora, se $a = b > 2$ então $a, 2a, \ldots, (a-1)a$ ocorrem em $(p-1)!$, logo $p|(p-1)$, ou seja, se $p > 4$ é composto então $(p-1)! \equiv 0 \pmod{n}$. □

Como consequência desse teorema e da proposição anterior

$$\begin{aligned} a \text{ é um resto quadrático mod } p &\Rightarrow -1 \equiv (p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p} \\ a \text{ não é um resto quadrático mod } p &\Rightarrow -1 \equiv (p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p} \end{aligned}$$

Do Pequeno Torema de Fermat

$$a^{p-1} - 1 \equiv 0 \pmod{p} \Rightarrow (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

portanto $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, de modo que as implicações acima são de fato equivalentes.

Corolário 144 (Critério de Euler)**.** *Sejam p uma primo ímpar e a um inteiro não divisível por p.*

1. *a é um resto quadrático módulo p se, e só se, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;*
2. *a é não um resto quadrático módulo p se, e só se, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.* □

11.2 O símbolo de Legendre

Para $p > 2$ primo e a inteiro

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } p \nmid a \text{ e } a \text{ é um resto quadrático módulo } p \\ 0 & \text{se } p|a \\ -1 & \text{caso contrário.} \end{cases} \tag{93}$$

portanto, pelo critério de Euler

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \tag{94}$$

Proposição 145. *O símbolo de Legendre possui as seguintes popriedades*

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. *$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ se, e só se, $p \equiv 1 \pmod{4}$*
4. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

11.3 Lei da Reciprocidade Quadrática

O seguinte resultado é um importante teorema da Teoria dos Números. Foi demonstrado pela primeira vez (de modo correto, houveram outras "provas" antes, Euler conhecia esse resultado e Legendre deu uma demosntração incompleta) por Gauss em *Disquisitiones Arithmeticae*. Aqui são dadas quase 200 demonstrações desse resultado. Essa lei diz que *se p e q são primos ímpares distintos e pelo menos um deles é congruente a* 1 *módulo* 4, *então p é um resíduo quadrático módulo q se, e só se, q é um resíduo quadrático módulo p; congruente a* 1 *módulo* 4, *então p é um resíduo quadrático módulo q se, e só se, q é um resíduo quadrático módulo p; se ambos são congruentes a* 3 *módulo* 4, *então p é um resíduo quadrático módulo q se, e só se, q não é um resíduo quadrático módulo p;*

Usando o símbolo de Legendre, podemos enunciar a lei da reciprocidade da seguinte maneira; a demonstração fica para a próxima.

Teorema 146 (**Lei da Reciprocidade Quadrática**)**.** *Se $p \neq q$ são primos ímpares então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Em outras palavras, as congruências $X^2 \equiv p \pmod{q}$ e $X^2 \equiv q \pmod{p}$ ou ambas têm solução ou nenhuma tem, exceto quanto $p \equiv 3 \pmod 4$, quando uma tem solução e a outra não.

Exercício 147. *Prove que a lei de reciprocidade é equivalente às seguintes afirmações, enunciadas por Euler:*

1. *se $q \equiv 1 \pmod 4$ então q é um resíduo quadrático módulo p se, e só se, $p \equiv r \pmod q$, em que r é um resíduo quadrático módulo q;*

2. *se $q \equiv 3 \pmod 4$ então p é um resíduo quadrático módulo q se, e só se, $p \equiv \pm b^2 \pmod{4q}$ em que b é ímpar e não divisível por q.*

Exercícios

1. Prove que $6X^2 + 5X + 1 \equiv 0 \pmod m$ tem solução para todo inteiro positivo m.

2. Determine as soluções de $X^2 \equiv 11 \pmod{35}$.(Dica: fatore 35)

3. Seja a um resíduo quadrático módulo $p > 2$. Mostre que

   (a) se $p \equiv 1 \pmod 4$ então $p - a$ é um resíduo quadrático módulo p;

   (b) se $p \equiv 3 \pmod 4$ então $p - a$ não é um resíduo quadrático módulo p.

4. Mostre que $X^2 + 1 \equiv 0 \pmod p$ ($p > 2$ primo) tem solução se, e somente se, $p \equiv 1 \pmod 4$.

5. Use o teorema de Wilson para encontrar o menor resto de $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ módulo 7.

6. Mostre que se p é primo e a inteiro então $p|(a^p + (p-1)!a)$.

7. Mostre que p é o menor primo que divide $(p-1)! + 1$.

8. Mostre que se o primo ímpar p é tal que $p \equiv 1 \pmod 4$ então $X^2 \equiv -1 \pmod p$ tem duas soluções.

9. Mostre que se o primo ímpar p é tal que $p \equiv 3 \pmod 4$ então $((p-1)/2)! \equiv \pm 1 \pmod p$.

10. Mostre que para um primo ímpar p vale $(((p-1)/2)!)^2 \equiv (-1)^{(p+1)/2} \pmod p$.

11. Prove a proposição 145.

12. Use o critério de Euler a reciprocidade quadrática para mostrar que, para p primo,

    (a) se $p = 4n+1$ então $p|n^n - 1$.

    (b) se $p = 4n-1$ então $p|n^n + 2n(-1)^{n+1}$.