Notas de Aulas

Introdução à Teoria dos Números

Profª Maria Julieta Ventura Carvalho de Araujo

Prof. Frederico Sercio Feitosa (colaborador)

Profª Beatriz Casulari da Motta Ribeiro (colaboradora)

2016

Introdução à Teoria dos Números (MAT143)

1. Ementa

   (a) Os Princípios de Indução Matemática e da Boa Ordenação
   (b) Divisibilidade
   (c) Números Primos e o Teorema Fundamental da Aritmética
   (d) Equações Diofantinas Lineares
   (e) Congruências
   (f) Sistema de Congruências Lineares
   (g) Criptografia Básica

2. Bibliografia

   (a) Fernandes, A. M. V. et al. *Fundamentos de Álgebra.* Belo Horizonte: UFMG, 2005.
   (b) Coutinho, S. C. *Números Inteiros e Criptografia RSA.* Série de Computação e Matemática. Rio de Janeiro: IMPA, 2007.
   (c) Hefez, A. *Curso de Álgebra.* Vol. 1. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 1993.
   (d) _____ *Elementos de Aritmética.* Coleção Textos Universitários. Rio de Janeiro: SBM, 2005.
   (e) Alencar Filho, E. *Teoria Elementar dos Números.* São Paulo: Nobel, 1985.
   (f) Milies, F. C. P. *Números: Uma Introdução à Matemática.* São Paulo: EDUSP, 2003.
   (g) Rosen, K. H. *Elementary Number Theory and its Applications.* New York: Addison-Wesley, 1984.
   (h) Koblitz, N. *A Course in Number Theory and Cryptography.* New York: Springer-Verlag, 1987.
   (i) Santos, J. P. O. *Introdução à Teoria dos Números.* Coleção Matemática Universitária. Rio de Janeiro: IMPA, 1998.
   (j) Shokranian, S. *Teoria dos Números.* Brasília: UnB, 1999.
   (k) Gonçalves, A. *Introdução à Álgebra.* Projeto Euclides. Rio de Janeiro: IMPA, 1979.
   (l) Domingues, H. H. et al. *Álgebra Moderna.* São Paulo: Atual, 1982.

3. Avaliações

4. Horário de Atendimento

Índice

1 Os Princípios de Indução Matemática e da Boa Ordenação **1**
1.1 Introdução . . . 1
1.2 Dedução e Indução . . . 1
1.3 Princípio de Indução Matemática - PIM - 1a forma . . . 2
1.4 Princípio de Indução Matemática - PIM - 2a forma . . . 5
1.5 Princípio da Boa Ordenação (PBO) . . . 7
1.6 Exercícios . . . 9

2 Divisibilidade **11**
2.1 Relação de divisibilidade em $\mathbb{Z}$ . . . 11
2.2 Conjunto dos divisores de um inteiro . . . 12
2.3 Divisores comuns de dois inteiros . . . 13
2.3.1 Exercícios . . . 13
2.4 Algoritmo da Divisão . . . 13
2.4.1 Exercícios . . . 14
2.5 Representação de um número em uma base qualquer . . . 15
2.5.1 Exercícios . . . 17
2.6 Alguns critérios de divisibilidade . . . 18
2.6.1 Exercícios . . . 19
2.7 Máximo Divisor Comum . . . 19
2.7.1 Máximo divisor comum de dois inteiros . . . 19
2.7.2 Inteiros primos entre si . . . 20
2.7.3 Caracterização do máximo divisor comum de dois inteiros . . . 22
2.7.4 Máximo divisor comum de vários inteiros . . . 22
2.7.5 Exercícios . . . 23
2.7.6 Algoritmo de Euclides (método para encontrar o máximo divisor comum) . . . 24
2.7.7 Algoritmo euclidiano estendido . . . 27
2.8 Mínimo múltiplo comum . . . 28
2.8.1 Múltiplos comuns de dois inteiros . . . 28
2.8.2 Mínimo múltiplo comum de dois inteiros . . . 29
2.8.3 Relação entre mdc e mmc . . . 29
2.8.4 Exercícios . . . 31

3 Números primos e o Teorema Fundamental da Aritmética **32**
3.1 Números primos e compostos . . . 32
3.2 Crivo de Eratósthenes . . . 33
3.3 Teorema Fundamental da Aritmética . . . 35
3.4 A procura de números primos . . . 36
3.5 Exercícios . . . 37

4 Equações Diofantinas Lineares **39**
4.1 Generalidades . . . 39
4.2 Condição de existência de solução . . . 39
4.3 Soluções da equação diofantina linear $ax + by = c$ . . . 40
4.4 Exercícios . . . 41

5 Congruências **42**
5.1 Inteiros congruentes . . . 42
5.2 Caracterização de inteiros congruentes . . . 42
5.3 Propriedades . . . 43
5.4 Sistema completo de restos . . . 45
5.5 Exercícios . . . 46
5.6 Classes residuais . . . 47
5.6.1 Revisão . . . 47
5.6.2 Definição e propriedades . . . 47
5.6.3 O conjunto das classes residuais . . . 48
5.6.4 Exercícios . . . 50
5.6.5 Adição e Multiplicação em $\mathbb{Z}_m$ . . . 50
5.6.6 Exercícios . . . 51
5.7 Congruências lineares . . . 51
5.7.1 Definição e condição de existência . . . 51
5.7.2 Soluções da congruência linear $ax \equiv b \pmod{m}$ . . . 52
5.8 Resolução de equações diofantinas lineares por congruência . . . 53
5.9 Inverso de um inteiro módulo m . . . 54
5.10 Teoremas de Fermat e de Wilson . . . 54
5.11 Critérios de divisibilidade usando congruências . . . 56
5.12 Exercícios . . . 57
5.13 A função φ de Euler . . . 58
5.14 Exercícios . . . 60

6 Sistemas de congruências lineares **61**
6.1 Introdução . . . 61
6.2 Teorema Chinês do Resto . . . 62
6.3 Representação Gráfica (tabela) . . . 63
6.4 Exercícios . . . 65

7 Criptografia básica **66**
7.1 Introdução . . . 66
7.2 Criptografia RSA . . . 67
7.2.1 Pré-codificação . . . 67
7.2.2 Codificando e decodificando . . . 67
7.2.3 Relembrando e exemplificando . . . 68
7.3 Onde podemos ter problemas? . . . 70
7.3.1 Problema 1: conhecendo $\phi(n)$ . . . 70
7.3.2 Problema 2: p, q grandes, mas $|p - q|$ pequeno . . . 71
7.4 Um exercício resolvido . . . 72
7.5 Exercícios . . . 74

Capítulo 1

Os Princípios de Indução Matemática e da Boa Ordenação

1.1 Introdução

Em 1742, o matemático Christian Goldbach afirmou que todo inteiro par maior que 4 pode ser escrito como a soma de dois primos ímpares. Certamente Goldbach intuiu este resultado depois de observar que ele era verdadeiro para alguns números, como por exemplo, $6 = 3+3$, $8 = 3+5$, $10 = 5+5$, etc. Já foi verificada esta afirmativa para todo inteiro par entre 6 e 10^{14}, entretanto não podemos considerá-la verdadeira a partir deste fato já que 10^{14} é um número insignificante comparado com a "maior parte"dos inteiros. Muitos matemáticos têm procurado demonstrar ou refutar esta conjectura, mas nada foi conseguido até hoje.

Em uma teoria matemática, muitas vezes, resultados são enunciados a partir de considerações de casos particulares, como no exemplo acima, mas eles só são tidos como verdadeiros se puderem ser demonstrados, isto é, deduzidos de proposições já conhecidas e aceitas, como os postulados, que são proposições que não são demonstradas e nos quais está fundamentada a teoria.

Trataremos aqui dos números naturais, $\mathbb{N} = \{1, 2, 3, ...\}$, a partir de um dos postulados que os caracterizam, a saber, o Princípio de Indução Matemática. Veremos como utilizá-lo na demonstração de afirmações a respeito dos números naturais, como por exemplo, o Princípio da Boa Ordenação.

1.2 Dedução e Indução

Consideremos os seguintes exemplos:

Exemplo 1.1

(1) Todo mineiro é brasileiro.
(2) Paulo é mineiro.
(3) Logo, Paulo é brasileiro.

Exemplo 1.2

(1) O trinômio $n^2 + n + 41$ é um número primo para $n = 1$ ou $n = 2$.
(2) Logo, para todo $n \in \mathbb{N}$, o trinômio $n^2 + n + 41$ é um número primo.

No exemplo 1.1, a afirmação (1) é geral e com o auxílio da afirmação particular (2) obtemos a afirmação particular (3).

No exemplo 1.2, a afirmação (1) é particular e estamos tentando generalizá-la através da afirmação (2).

Definição 1.1 *A passagem de uma afirmação geral para uma particular é chamada DEDUÇÃO (exemplo 1.1). A tentativa de generalização de uma afirmação particular, isto é, a passagem de uma afirmação particular para uma geral, é chamada INDUÇÃO (exemplo 1.2).*

Observação 1.1 *Note que a conclusão do exemplo 1.2 é falsa (faça $n = 40$, por exemplo). Temos então a seguinte questão que será resolvida aqui: Como poderíamos usar indução em matemática de forma a obter somente conclusões verdadeiras ?*

1.3 Princípio de Indução Matemática - PIM - $1^{\underline{a}}$ forma

Suponhamos que para cada natural n se tenha uma afirmativa $P(n)$ que satisfaça às seguintes propriedades:

(i) $P(1)$ é verdadeira;

(ii) Sempre que a afirmativa é válida para um número natural arbitrário $n = k$, ela é válida para seu sucessor $n = k + 1$ (isto é, $P(k)$ verdadeira implica $P(k + 1)$ verdadeira).

Então, $P(n)$ é verdadeira para todo natural $n \geqslant 1$.

Observação 1.2 *Aqui admitimos o PIM como axioma dos números naturais, isto é, uma proposição sem demonstração considerada como consenso necessário para a construção da teoria, servindo como ponto inicial para os demais resultados.*

Observação 1.3 *Uma prova baseada no PIM é chamada uma prova pelo método da indução matemática. Tal prova deve consistir da demonstração de dois fatos independentes:*

Fato 1 *a afirmação é válida para $n = 1$.*

Fato 2 *a afirmação é válida para $n = k + 1$ se ela é válida para $n = k$, onde k é um número natural arbitrário.*

Se ambos estes fatos são provados então, com base no PIM, a afirmação é válida para todo número natural n.

Observação 1.4 *Note que o fato 2 contém uma implicação, portanto possui uma hipótese ($P(k)$ é verdadeira) e uma tese ($P(k + 1)$ é verdadeira). Provar o fato 2 significa provar que a hipótese acarreta a tese. A hipótese do fato 2 é chamada Hipótese de Indução (HI).*

Exemplo 1.3 *Calcular a soma*

$$S_n = \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{n(n+1)}.$$

Temos que:

$$\begin{aligned} S_1 &= \frac{1}{2}, \\ S_2 &= \frac{1}{2} + \frac{1}{6} = \frac{2}{3}, \\ S_3 &= \frac{1}{2} + \frac{1}{6} + \frac{1}{12} = \frac{3}{4}, \ \textit{etc.} \end{aligned}$$

Usando o método de indução matemática tentaremos provar que $S_n = \dfrac{n}{n+1}$, para todo natural $n \geqslant 1$.

Fato 1: Para $n = 1$ a afirmação é verdadeira pois $S_1 = \frac{1}{2} = \frac{1}{1+1}$.

Fato 2: Suponhamos que a afirmação seja verdadeira para $n = k$, isto é, $S_k = \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{k(k+1)} = \frac{k}{k+1}$ e vamos provar que a afirmação é verdadeira para $n = k+1$, ou seja, $S_{k+1} = \frac{k+1}{k+1+1} = \frac{k+1}{k+2}$.

De fato,

$$\begin{aligned} S_{k+1} &= \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)} \\ &= S_k + \frac{1}{(k+1)(k+2)} \\ &\overset{HI}{=} \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k^2+2k+1}{(k+1)(k+2)} \\ &= \frac{(k+1)^2}{(k+1)(k+2)} \\ &= \frac{k+1}{k+2} \end{aligned}$$

Portanto, com base no PIM, podemos afirmar que $S_n = \frac{n}{n+1}$, para todo natural $n \geqslant 1$.

Exemplo 1.4 *Vimos, pelo exemplo 1.2, como uma atitude negligente para com o fato 2 pode nos levar a resultados falsos. O exemplo seguinte mostra que tão pouco podemos omitir o fato 1.*

Seja $S_n = 1 + 2 + 3 + ... + n$ e consideremos a conjectura $S_n = \frac{1}{8}(2n+1)^2$.

Fato 2: Suponhamos a afirmativa válida para $n = k$, isto é, $S_k = \frac{1}{8}(2k+1)^2$.

Assim temos:

$$\begin{aligned} S_{k+1} &= 1 + 2 + 3 + ... + k + (k+1) \\ &= S_k + (k+1) \\ &\overset{HI}{=} \frac{1}{8}(2k+1)^2 + (k+1) \\ &= \frac{1}{8}(4k^2 + 4k + 1) + (k+1) \\ &= \frac{1}{8}(4k^2 + 12k + 9) \\ &= \frac{1}{8}\left(2(k+1)+1\right)^2 \end{aligned}$$

Logo, o fato 2 se verifica.

Entretanto, é fácil ver que esta conjectura não é verdadeira para todo número natural n.

De fato, $S_1 = 1 \neq \frac{1}{8}(2+1)^2$.

Observação 1.5 *O fato 1 cria a base para se fazer a indução. O fato 2 nos dá o direito de passar de um número natural para o seu sucessor (de k para $k+1$), ou seja, o direito de uma extensão ilimitada desta base.*

Se o fato 1 não foi provado mas o fato 2 sim, então a base para se iniciar a indução não foi criada e não faz sentido aplicar o fato 2, já que não existe nada para ser estendido. Se o fato 2 não foi provado mas o fato 1 sim, então temos a base para se começar a indução, mas não temos argumentos que nos possibilitem estendê-la.

Observação 1.6 *Se fizermos uma afirmativa incorreta não conseguiremos demonstrá-la pelo método de indução. Por exemplo, examinando a soma*

$$S_n = \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{n(n+1)}$$

para alguns valores de n, obtivemos $S_1 = \frac{1}{2}$, $S_2 = \frac{2}{3}$, $S_3 = \frac{3}{4}$, *... e estes resultados particulares sugeriram a hipótese de que, para todo natural* $n \geqslant 1$, $S_n = \frac{n}{n+1}$, *o que foi provado no exemplo 1.3.*

Poderíamos ter feito a seguinte conjectura: $S_n = \frac{n+1}{3n+1}$. *Esta fórmula é verdadeira para* $n = 1$, *pois* $S_1 = \frac{1}{2}$. *Suponhamos que ela seja verdadeira para* $n = k$, *isto é,* $S_k = \frac{k+1}{3k+1}$ *e tentaremos provar que ela também é verdadeira para* $n = k+1$, *isto é, que* $S_{k+1} = \frac{k+2}{3k+4}$.

Mas,

$$\begin{aligned} S_{k+1} &= S_k + \frac{1}{(k+1)(k+2)} \\ &\overset{HI}{=} \frac{k+1}{3k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k^3+4k^2+8k+3}{(k+1)(k+2)(3k+1)} \end{aligned}$$

o que não confirma a nossa conjectura.

O fato de se começar a indução em $n = 1$ não é importante. Podemos reescrever o PIM da seguinte forma:

Proposição 1.1 *Seja* $a \in \mathbb{N}$. *Suponhamos que para cada natural* $n \geqslant a$ *se tenha uma afirmativa* $P(n)$ *que satisfaça às seguintes propriedades:*

(i) $P(a)$ *é verdadeira;*

(ii) *Sempre que a afirmativa é válida para um número natural arbitrário* $n = k \geqslant a$, *ela é válida para seu sucessor* $n = k+1$ *(isto é,* $P(k)$ *verdadeira implica* $P(k+1)$ *verdadeira).*

Então, $P(n)$ *é verdadeira para todo natural* $n \geqslant a$.

Prova:

■

O processo de indução matemática se baseia no fato de que depois de cada número natural k existe um sucessor $(k+1)$ e que cada número natural n pode ser alcançado mediante um número finito de passos, a partir do 1. Portanto é, muitas vezes, mais conveniente enunciá-lo do seguinte modo:

Proposição 1.2 *Se $S \subset \mathbb{N}$ é um subconjunto tal que:*

(i) $1 \in S$*;*

(ii) *Sempre que $k \in S$ tem-se que $(k+1)$ também pertence a S.*

Então podemos afirmar que $S = \mathbb{N}$.

Prova:

■

Observação 1.7 *Para mostrar que*

$$\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1} \text{ para todo } n \geqslant 1$$

poderíamos ter considerado o conjunto

$$S = \left\{ n \in \mathbb{N} : \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1} \right\}$$

e então pelos mesmos argumentos utilizados no exemplo 1.3, concluiríamos que:

(i) $1 \in S$*;*

(ii) *Se $k \in S$ então $(k+1) \in S$.*

Logo, teríamos que $S = \mathbb{N}$, ou seja, a fórmula

$$\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

é válida para todo $n \geqslant 1$.

1.4 Princípio de Indução Matemática - PIM - $2^{\underline{a}}$ forma

Seja $a \in \mathbb{N}$. Suponhamos que para cada natural $n \geqslant a$ se tenha uma afirmativa $P(n)$ que satisfaça às seguintes propriedades:

(i) $P(a)$ é verdadeira;

(ii) $P(m)$ verdadeira para todo natural m, com $a \leqslant m \leqslant k$, implica $P(k+1)$ verdadeira.

Então $P(n)$ é verdadeira para todo natural $n \geqslant a$.

Observação 1.8 *Note que aqui também a condição (ii) consiste em uma implicação. Sua hipótese é também chamada de hipótese de indução (HI). A diferença entre as duas formas está exatamente na hipótese de indução: na primeira supõe-se que $P(k)$ seja verdadeira e na segunda supõe-se que $P(k)$, $P(k-1), P(k-2), ..., P(a)$ sejam todas verdadeiras.*

Observação 1.9 *Esta forma é útil nos casos em que a validade de $P(k+1)$ não puder ser obtida facilmente da validade de $P(k)$ mas sim, da validade de algum $P(m)$, onde $a \leqslant m \leqslant k$.*

Exemplo 1.5 *Considere a sequência de Fibonacci*

$$1, 1, 2, 3, 5, 8, 13, 21, ...$$

onde cada elemento, a partir do terceiro, é a soma dos dois anteriores.

Se denotarmos por $F(n)$ o n-ésimo termo desta sequência, poderemos defini-la por:
$F(1) = 1$
$F(2) = 1$
$F(n) = F(n-2) + F(n-1)$, *se* $n \geqslant 3$.

Mostre que $F(n) < \left(\frac{7}{4}\right)^n$, *para todo natural* $n \geqslant 1$.

Usando a primeira forma do PIM

Seja $P(n)$ a afirmativa: $F(n) < \left(\frac{7}{4}\right)^n$, $n \in \{1, 2, 3, ...\}$.

Temos que $P(1)$ e $P(2)$ são verdadeiras pois $F(1) = 1 < \frac{7}{4}$ *e* $F(2) = 1 < \left(\frac{7}{4}\right)^2$.

Seja $k \geqslant 2$ e suponhamos que $P(k)$ seja válida, isto é, $F(k) < \left(\frac{7}{4}\right)^k$.

Devemos mostrar que $F(k+1) < \left(\frac{7}{4}\right)^{(k+1)}$.

Como $k+1 \geqslant 3$ então $F(k+1) = F(k-1) + F(k)$ e não fica claro como obter a desigualdade desejada a partir da hipótese de indução.

Observe que $F(k-1) \leqslant F(k)$ e então

$$\begin{aligned} F(k+1) &= F(k-1) + F(k) \\ &\leqslant F(k) + F(k) \\ &< 2\left(\frac{7}{4}\right)^k \\ &= \frac{8}{7}.\left(\frac{7}{4}\right)^{k+1} \end{aligned}$$

que é uma cota maior do que a desejada.

Vamos, então usar a segunda forma do PIM:

Usando a segunda forma do PIM

Já vimos que $P(1)$ e $P(2)$ são verdadeiras. Seja $k \geq 2$ e suponhamos $P(m)$ verdadeira para todo

natural m, $1 \leqslant m \leqslant k$. *Precisamos mostrar que* $P(k+1)$ *é verdadeira, ou seja,* $F(k+1) < \left(\frac{7}{4}\right)^{k+1}$.

Como $F(k+1) = F(k-1) + F(k)$ *e, por HI,* $F(k) < \left(\frac{7}{4}\right)^{k}$ *e* $F(k-1) < \left(\frac{7}{4}\right)^{k-1}$, *então*

$$\begin{aligned} F(k+1) &= F(k-1) + F(k) \\ &< \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k} \\ &= \frac{4}{7}.\left(\frac{7}{4}\right)^{k} + \left(\frac{7}{4}\right)^{k} \\ &= \frac{11}{7}.\left(\frac{7}{4}\right)^{k} \\ &< \frac{7}{4}.\left(\frac{7}{4}\right)^{k} = \left(\frac{7}{4}\right)^{k+1} \end{aligned}$$

Teorema 1.1 (Segunda forma do PIM) *Seja* $a \in \mathbb{N}$. *Suponha que para cada número natural* n *se tenha uma afirmativa* $P(n)$ *que satisfaça às seguintes propriedades:*

(i) $P(a)$ *é verdadeira;*

(ii) *Sempre que* $P(a), P(a+1), ..., P(k)$, *onde* $k \geqslant a$, *são verdadeiras tem-se que* $P(k+1)$ *também é verdadeira.*

Então $P(n)$ *é verdadeira para todo natural* $n \geqslant a$.

Prova:

Vamos usar a primeira forma do PIM.

Seja $S = \{n \in \mathbb{N} : n \geqslant a$ *e* $P(a), P(a+1), ..., P(n)$ *são verdadeiras* $\}$. *Queremos mostrar que* $S = \{n \in \mathbb{N} : n \geqslant a\}$.

Pela condição (i) temos que $P(a)$ *é verdadeira, ou seja,* $a \in S$.

Seja $k \geqslant a$ *tal que* $k \in S$ *(Hipótese de Indução); logo, pela definição de* S, $P(a), P(a+1), ..., P(k)$ *são verdadeiras e, pela condição (ii)* $P(k+1)$ *é também verdadeira. Assim* $(k+1) \in S$.

Portanto pela primeira forma do PIM temos que todos naturais n *tais que* $n \geqslant a$ *pertencem a* S, *isto é,* $S = \{n \in \mathbb{N} : n \geqslant a\}$, *donde* $P(n)$ *é verdadeira para todo* $n \geqslant a$. ■

Exemplo 1.6 *Vamos provar que todo inteiro* $n \geq 8$ *pode ser escrito como soma de 3s e 8s. Primeiro, temos que* $8 = 3 + 5$, *donde a base da indução é válida. Vamos supor como hipótese de indução que a afirmação é válida para* $n = 8, 9, 10, \ldots k$ *(note que a afirmação vale para* $n = 9$*). Vamos provar que a afirmação vale para* $k+1$. *Como* $k \geq 10$, *temos que* $k+1-3 = k-2 \geq 8$, *isto é,* $k+1-3 \in \{8, 9, \ldots k\}$, *donde, por hipótese de indução* $k+1-3$ *pode ser escrito como soma de 3s e 8s. Portanto, existem* $a, b \in \mathbb{N}$ *tais que* $k+1-3 = 3a+8b$ *e, então,* $k+1 = 3(a+1)+8b$ *e a afirmação está provada para todo* $n \geq 8$ *pelo PIM2.*

1.5 Princípio da Boa Ordenação (PBO)

Seja $A \subset \mathbb{R}$, A não-vazio. Chama-se menor elemento de A ou elemento mínimo de A um elemento $a \in A$ tal que $a \in S$ tal que $a \leqslant x$, para todo $x \in A$.

Podemos provar que se A possui um menor elemento, então ele é único.

De fato, suponhamos que existam dois menores elementos, digamos a e b. Então, como a é elemento mínimo e $b \in A$, temos que $a \leq b$. Por outro lado, como b é elemento mínimo e $a \in A$, então $a \geq b$. Logo, $a = b$.

Teorema 1.2 *(Princípio da Boa Ordenação - PBO) Todo subconjunto não vazio $S \subset \mathbb{N}$ possui um menor elemento.*

Prova:

Vamos usar a segunda forma do PIM.

Suponhamos que exista um conjunto $S \subset \mathbb{N}$ que não possua menor elemento. Vamos mostrar que $S = \varnothing$. Consideremos a afirmação: $n \notin S$, vamos provar que ela vale para todo $n \in \mathbb{N}$.

Temos então que $1 \notin S$, pois, do contrário, 1 seria o menor elemento de S. Suponhamos que $1, 2, ..., k$ não pertençam a S (Hipótese de Indução) e vamos mostrar que $(k+1) \notin S$. De fato, se $(k+1) \in S$ então $(k+1)$ seria o menor elemento de S, pois todos os naturais menores do que $(k+1)$ não estão em S, o que seria uma contradição. Logo $(k+1) \notin S$.

Portanto, pela segunda forma do PIM, nenhum elemento de $\mathbb{N}$ está em S. Como $S \subset \mathbb{N}$ temos que $S = \varnothing$. Assim podemos afirmar que se $S \subset \mathbb{N}$, $S \neq \varnothing$, então S possui menor elemento. ∎

Observação 1.10 *O Princípio da Boa Ordenação também é conhecido como Princípio do Menor Inteiro.*

Exemplo 1.7 *No conjunto $\{21, 23, 25, 27, ...\}$ dos números ímpares maiores que 19, temos que 21 é o menor elemento.*

Exemplo 1.8 *O conjunto dos números inteiros $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$ não possui menor elemento, pois se $x \in \mathbb{Z}$ então $(x-1) \in \mathbb{Z}$, ou seja, $\mathbb{Z}$ não é limitado inferiormente. Mas veremos nos exercícios que há um PBO para os inteiros, apenas com mais hipóteses.*

Exemplo 1.9 *Considere o conjunto dos números racionais positivos:*

$$\mathbb{Q}_+^* = \left\{ \frac{m}{n} : m, n \in \mathbb{N} \right\}$$

Note que 0 é menor do que todos os elementos de $\mathbb{Q}_+^*$, donde $\mathbb{Q}_+^*$ é limitado inferiormente. Como $0 \notin \mathbb{Q}_+^*$, 0 não é o menor elemento de $\mathbb{Q}_+^*$. Vamos mostrar que $\mathbb{Q}_+^*$ não possui menor elemento.

Suponhamos, por absurdo, que $a \in \mathbb{Q}_+^*$ seja o menor elemento de $\mathbb{Q}_+^*$. É claro que $\frac{a}{2} \in \mathbb{Q}_+^*$ e como $\frac{a}{2} < a$, chegamos a uma contradição.

Exemplo 1.10 *Usando o PBO mostre que $S_n = \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1}$ para todo natural $n \geqslant 1$.*

Seja $F = \left\{ n \in \mathbb{N} : S_n \neq \frac{n}{n+1} \right\}$. Desejamos mostrar que $F = \varnothing$. Vamos supor que $F \neq \varnothing$. Assim, pelo PBO, existe $a \in F$ tal que a é o menor elemento de F. Como $a \in F$ temos que $S_a \neq \frac{a}{a+1}$ e $a > 1$, pois $S_1 = \frac{1}{2} = \frac{1}{1+1}$, o que implica $1 \notin F$. Sendo a o menor elemento de F então $(a-1) \notin F$, isto é,

$$S_{a-1} = \frac{1}{1.2} + \frac{1}{2.3} + ... + \frac{1}{(a-1)a} = \frac{a-1}{a}$$

.

Assim, temos:

$$S_a = S_{a-1} + \frac{1}{a(a+1)} = \frac{a-1}{a} + \frac{1}{a(a+1)} = \frac{(a-1)(a+1)+1}{a(a+1)} = \frac{a}{a+1}.$$

Mas isso contradiz $S_a \neq \frac{a}{a+1}$. Portanto $F = \varnothing$ e concluímos que não existe $n \in \mathbb{N}$ tal que $S_n \neq \frac{n}{n+1}$, ou seja, $S_n = \frac{n}{n+1}$, para todo natural $n \geqslant 1$.

1.6 Exercícios

1. Verifique, por indução, as seguintes fórmulas para $n \geqslant 1$:

   (a) $1 + 2 + 3 + ... + n = \dfrac{n(n+1)}{2}$

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

   (c) $5 + 9 + 13 + ... + (4n+1) = n(2n+3)$

   (d) $1 + 4 + 9 + ... + n^2 = \dfrac{1}{6}n(n+1)(2n+1)$

   (e) $1.2 + 2.3 + 3.4 + ... + n(n+1) = \dfrac{1}{3}n(n+1)(n+2)$

   (f) $1 + 2^3 + 3^3 + ... + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$

   (g) $(1 + 2^5 + 3^5 + ... + n^5) + (1 + 2^7 + 3^7 + ... + n^7) = 2\left[\dfrac{n(n+1)}{2}\right]^4$

2. Seja $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

   (a) Calcule A^2 e A^3 para determinar uma possível fórmula para A^n, $n \in \{1, 2, 3, ...\}$.

   (b) Demonstre o resultado obtido acima por indução.

3. Considere a progressão aritmética (P.A.) de razão r e primeiro termo a_1.

   (a) Estabeleça uma fórmula para a_n, o n-ésimo termo, e demonstre-a por indução.

   (b) Mostre que a soma S_n dos n primeiros termos desta progressão é dada por $S_n = \dfrac{(a_1 + a_n)n}{2}$.

4. Considere a progressão geométrica (P.G.) de razão $q \neq 1$ e primeiro termo a_1.

   (a) Estabeleça uma fórmula para a_n, o n-ésimo termo, e demonstre-a por indução.

   (b) Mostre que a soma S_n dos n primeiros termos desta progressão é dada por $S_n = \dfrac{a_n q - a_1}{q - 1}$.

5. Encontre a lei geral sugerida e em seguida demonstre-a por indução.

   (a) $1 + \dfrac{1}{2} = 2 - \dfrac{1}{2}$, $1 + \dfrac{1}{2} + \dfrac{1}{4} = 2 - \dfrac{1}{4}$, $1 + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} = 2 - \dfrac{1}{8}$

   (b) $1 - \dfrac{1}{2} = \dfrac{1}{2}$, $\left(1 - \dfrac{1}{2}\right)\left(1 - \dfrac{1}{3}\right) = \dfrac{1}{3}$, $\left(1 - \dfrac{1}{2}\right)\left(1 - \dfrac{1}{3}\right)\left(1 - \dfrac{1}{4}\right) = \dfrac{1}{4}$

6. Mostre por indução que:

   (a) $1 + n \leqslant 2^n$, para todo $n \in \{0, 1, 2, ...\}$.

   (b) $2^n < n!$, para todo $n \geqslant 4$, $n \in \mathbb{N}$.

   (c) Para todo $a \in \mathbb{R}$, $a < 0$ temos $a^{2n} > 0$ e $a^{2n-1} < 0$, $\forall n \in \mathbb{N}$.

   (d) Seja $x \in \mathbb{R}$, $x > 0$. Então $(1 + x)^{2n} > 1 + 2nx$ para todo $n \in \mathbb{N}$.

   (e) Se $a > 0$ e $x > 0$ são números reais então $(a + x)^n \geqslant a^n + nxa^{n-1}$, $\forall n \in \mathbb{N}$.

7. Princípio da Boa Ordenação para os Inteiros: prove que todo subconjunto dos inteiros não-vazio e limitado inferiormente possui elemento mínimo.

8. Use o Princípio da Boa Ordenação para provar que qualquer subconjunto dos inteiros não vazio e limitado superiormente tem um maior elemento.

9. Prove que não existe inteiro m tal que $0 < m < 1$.

10. Se a e b são dois inteiros positivos quaisquer, prove que existe um inteiro positivo n tal que $na \geqslant b$. (Use o PBO).

11. A equivalência dos Princípios de Indução e da Boa Ordenação.

    (a) Prove que a primeira forma do PIM é equivalente ao PBO.

    (b) Conclua que:

        i. a segunda forma do PIM é equivalente ao PBO.

        ii. as duas formas do PIM são equivalentes.

12. Prove que para todo inteiros $n \geq 1$ existem $a_n, b_n \in \mathbb{N}$ tais que $5^n = a_n^2 + b_n^2$.

13. Considere a sequencia definida por

$$\begin{cases} a_0 = 1 \\ a_1 = 2 \\ a_n = 4a_{n-1} - 4a_{n-2} \end{cases}$$

    Mostre que $a_n = 2^n$ para todo $n \geq 0$.

14. Use o PBO para mostrar que:

    (a) Toda função monótona não-crescente $f : \mathbb{N} \to \mathbb{N}$ é constante a partir de certo ponto.

    (b) $\sqrt{2}$ é irracional

Capítulo 2

Divisibilidade

2.1 Relação de divisibilidade em $\mathbb{Z}$

Definição 2.1 *Dados dois inteiros a e b, dizemos que b divide a se, e somente se, existe um inteiro q tal que $a = bq$.*

Observação 2.1 *Se b divide a também dizemos que:*

- *b é um divisor de a.*
- *a é um múltiplo de b.*
- *b é um fator de a.*
- *a é divisível por b.*

Notação: $b \mid a$ (b divide a)
$b \nmid a$ (b não divide a)

Observação 2.2

1. *A notação $b \mid a$ não deve ser confundida com a fração $\frac{b}{a}$.*
2. *A relação R, no conjunto $\mathbb{Z}$ dos números inteiros, definida por: $b\ R\ a \Leftrightarrow b \mid a$, denomina-se **relação de divisibilidade em** $\mathbb{Z}$.*

Exemplo 2.1

1. $2 \mid 6$, *pois,* $6 = 2.3$*;*
2. $-4 \mid 12$, *pois,* $12 = (-4).(-3)$*;*
3. $5 \mid -10$, *pois,* $-10 = 5.(-2)$*;*
4. $-7 \mid -21$, *pois,* $-21 = (-7).3$*;*
5. $3 \nmid 7$, *pois não existe inteiro q tal que* $7 = 3q$*;*
6. $0 \mid 0$, *pois,* $0 = 0.q$ *para todo inteiro q.*

Proposição 2.1 *Sejam a, b, c e d inteiros quaisquer. Podemos afirmar que:*

1. *Se $b \neq 0$, então o inteiro q nas condições da definição é único.*
2. $a \mid 0$, $1 \mid a$ *e* $a \mid a$.

3. $0 \mid a$ *se, e somente se,* $a = 0$.

4. *Se* $b \mid a$ *e* $a \neq 0$, *então* $|b| \leqslant |a|$.

5. *Os únicos divisores de* 1 *são* 1 *e* -1.

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

7. *Se* $b \mid a$, *então* $(-b) \mid a$, $b \mid (-a)$ *e* $(-b) \mid (-a)$.

8. *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

9. *Se* $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$.

10. *Se* $a \mid b$ *e* $a \mid c$, *então* $a \mid (bx + cy)$, *para todo inteiro* x *e* y.

Prova:

■

Observação 2.3

1. *A propriedade* 10 *pode ser generalizada:*
   Se $a \mid b_k$, *para* $k = 1, 2, ..., n$, *então* $a \mid (b_1x_1 + b_2x_2 + ... + b_nx_n)$ *para todo inteiro* $x_1, x_2, ..., x_n$.

2. *De acordo com as propriedades* 2 *e* 8 *temos que a relação de divisibilidade em* $\mathbb{Z}$ *é reflexiva e transitiva, porém não é simétrica, pois* $2 \mid 4$ *e* $4 \nmid 2$, *e nem anti-simétrica pois* $2 \mid (-2)$, $(-2) \mid 2$ *e* $2 \neq (-2)$.

2.2 Conjunto dos divisores de um inteiro

Definição 2.2 *O conjunto de todos os divisores de um inteiro* a, *denotado por* $D(a)$, *é o conjunto*

$$D(a) = \{x \in \mathbb{Z} : x \mid a\}.$$

Exemplo 2.2

1. $D(0) = \{x \in \mathbb{Z} : x \mid 0\} = \mathbb{Z}$

2. $D(1) = \{x \in \mathbb{Z} : x \mid 1\} = \{-1, 1\}$

3. $D(2) = \{x \in \mathbb{Z} : x \mid 2\} = \{\pm 1, \pm 2\}$

4. $D(-8) = \{x \in \mathbb{Z} : x \mid 8\} = \{\pm 1, \pm 2, \pm 4, \pm 8\}$

Observação 2.4

1. *É claro que* $D(a) = D(-a)$.

2. *Como* $a = a.1 = (-a).(-1)$ *temos que* $1, -1, a, -a$ *são divisores de* a, *denominados divisores triviais de* a. *Em particular, o inteiro* 1 *(ou* -1*) só admite divisores triviais.*

3. *Qualquer que seja o inteiro* $a \neq 0$, *se* $x \mid a$, *então* $x \neq 0$ *e* $|x| \leqslant |a|$ *o que implica* $-|a| \leqslant x \leqslant |a|$ *e, portanto,* $D(a) \subset [-|a|, |a|] \cap \mathbb{Z}$. *Isto significa que qualquer inteiro* $a \neq 0$ *tem um número finito de divisores.*

2.3 Divisores comuns de dois inteiros

Definição 2.3 *Chama-se divisor comum de dois inteiros a e b todo inteiro c tal que $c \mid a$ e $c \mid b$, isto é, $c \in D(a) \cap D(b)$. Indica-se por $D(a,b) = D(a) \cap D(b)$.*

Exemplo 2.3
$D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$
$D(-15) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$
$D(12,-15) = D(12) \cap D(-15) = \{\pm 1, \pm 3\}$

Observação 2.5

1. $D(a,b) = D(b,a)$
2. $D(a,b) \neq \varnothing$, *pois* $1 \in D(a) \cap D(b) = D(a,b)$

2.3.1 Exercícios

1. Decida se as afirmações abaixo são verdadeiras ou falsas, dando a demonstração ou um contra-exemplo. Sejam a, b e c inteiros.
   (a) Se $a \mid b$, então $(a+c) \mid (b+c)$.
   (b) Se $a \mid b$, então $ac \mid bc$.
   (c) Se $ac \mid bc$, então $a \mid b$.
   (d) Se $a \mid b$, então $a \mid bx$, para todo $x \in \mathbb{Z}$.
   (e) Se $a \mid (b+c)$, então $a \mid b$ ou $a \mid c$.
   (f) Se $a \mid bc$, então $a \mid b$ ou $a \mid c$.
   (g) Se $a \mid c$ e $b \mid c$, então $ab \mid c$.
   (h) Se $a \mid c$ e $b \mid c$, então $(a+b) \mid c$.
2. Sejam a e b inteiros. Mostre que se $a \mid b$ e $b \mid a$, então $|a| = |b|$.

2.4 Algoritmo da Divisão

Lema 2.1 (Lema da divisão de Euclides) *Sejam a e b inteiros com $a \geqslant 0$ e $b > 0$. Então existem <u>únicos</u> inteiros q e r tais que $a = bq + r$, onde $q \geqslant 0$ e $0 \leqslant r < b$.*

Prova:
<u>Existência:</u>
Faremos a demonstração por indução sobre a.
Se $a = 0$ escolhemos $q = 0$ e $r = 0$ obtendo $0 = b.0 + 0$.
Se $a > 0$, suponhamos por hipótese de indução (HI) que o resultado seja válido para $(a-1)$, ou seja, existem inteiros q' e r' tais que $a - 1 = bq' + r'$, onde $q' \geqslant 0$ e $0 \leqslant r' < b$. Logo $a = bq' + r' + 1$ e $1 \leqslant r' + 1 \leqslant b$. Se $r' + 1 < b$, tomamos $q = q'$ e $r = r' + 1$ o que mostra o resultado. Se $r' + 1 = b$ temos que $a = bq' + b = b(q' + 1)$ e basta tomar neste caso $q = q' + 1$ e $r = 0$.
<u>Unicidade:</u>
Vamos supor que (q, r) e (q', r') sejam dois pares de inteiros tais que $a = bq + r, a = bq' + r'$ com $q, q' \geqslant 0$, $0 \leqslant r, r' < b$ e vamos concluir que $q = q'$ e $r = r'$. Suponha que $q > q'$. Daí segue que $b(q - q') = r' - r$ e como $q - q' > 0$ é um inteiro, então $q - q' \geqslant 1$ e, portanto, $b(q - q') \geqslant b$. Logo teríamos $r' - r \geqslant b$ o que é um absurdo já que $0 \leqslant r < b$ e $0 \leqslant r' < b$. Assim não podemos ter $q > q'$. Analogamente não podemos ter $q' > q$ e, portanto, $q = q'$. Finalmente segue que $r = a - bq = a - bq' = r'$. ∎

Teorema 2.1 (Algoritmo da Divisão) *Sejam a e b inteiros com $b \neq 0$. Então existem <u>únicos</u> inteiros q e r que satisfazem as condições $a = bq + r$ e $0 \leqslant r < |b|$.*

Prova:

Temos quatro casos a considerar:
1º) $a \geqslant 0$ e $b > 0$;
2º) $a \geqslant 0$ e $b < 0$;
3º) $a < 0$ e $b > 0$;
4º) $a < 0$ e $b < 0$.

<u>1º caso:</u> $a \geqslant 0$ e $b > 0$
É o lema da divisão de Euclides mostrado anteriormente.

<u>2º caso:</u> $a \geqslant 0$ e $b < 0$
Como $b < 0$, então $-b > 0$ e $|b| = -b$. Pelo lema da divisão de Euclides aplicado aos inteiros $a \geqslant 0$ e $-b > 0$, existem únicos inteiros q' e r' tais que $a = (-b)q' + r'$, com $0 \leqslant r' < -b$. Assim $a = b(-q') + r'$, com $0 \leqslant r' < |b|$. Logo, neste caso, tomamos $q = -q'$ e $r = r'$.

<u>3º caso:</u> $a < 0$ e $b > 0$
Como $a < 0$, então $-a > 0$ e $|b| = b$. Pelo lema da divisão de Euclides aplicado aos inteiros $-a \geqslant 0$ e $b > 0$, existem únicos inteiros q' e r' tais que $-a = bq' + r'$, com $0 \leqslant r' < b$. Assim $a = b(-q') - r'$, com $0 \leqslant r' < b$. Se $r' = 0$ temos $a = b(-q')$ e, neste caso, tomamos $q = -q'$ e $r = 0$. Se $r' > 0$ temos $a = b(-q') - r' + b - b = b(-q' - 1) + (b - r')$, com $0 < b - r' < b$, e, neste caso, tomamos $q = -q' - 1$ e $r = b - r'$.

<u>4º caso:</u> $a < 0$ e $b < 0$
Como $a < 0$ e $b < 0$, então $-a > 0$, $-b > 0$ e $|b| = -b$. Pelo lema da divisão de Euclides aplicado aos inteiros $-a \geqslant 0$ e $-b > 0$, existem únicos inteiros q' e r' tais que $-a = (-b)q' + r'$, com $0 \leqslant r' < -b$. Assim $a = bq' - r'$, com $0 \leqslant r' < -b$. Se $r' = 0$ temos $a = bq'$ e, neste caso, tomamos $q = q'$ e $r = 0$. Se $r' > 0$ temos $a = bq' - r' + b - b = b(q' + 1) + (-b - r')$, com $0 < -b - r' < -b = |b|$, e, neste caso, tomamos $q = q' + 1$ e $r = -b - r'$. ■

Observação 2.6

1. *Os inteiros q e r são denominados, respectivamente, o quociente e o resto da divisão de a por b.*
2. *b é divisor de a ($b \mid a$) se, e somente se, $r = 0$. Neste caso $a = bq$ e o quociente q na divisão exata de a por b indica-se por $\frac{a}{b}$ ou a/b.*
3. *Na divisão de um inteiro qualquer a por 2 os possíveis restos são $r = 0$ ou $r = 1$. Se $r = 0$, então $a = 2q$ é denominado **par**; se $r = 1$ então $a = 2q + 1$ é denominado **ímpar**.*

2.4.1 Exercícios

1. Encontre q e r na divisão de $a = 59$ por $b = -14$ que satisfaçam as condições do algoritmo da divisão.
2. Idem para $a = -79$ e $b = 11$.
3. Idem para $a = -59$ e $b = -7$.
4. Mostre que o quadrado de um inteiro qualquer é da forma $3k$ ou $3k + 1$, com $k \in \mathbb{Z}$.
5. Mostre que todo inteiro ímpar é da forma $4k + 1$ ou $4k + 3$, com $k \in \mathbb{Z}$.
6. Mostre que o quadrado de qualquer inteiro ímpar é da forma $8k + 1$, com $k \in \mathbb{Z}$.
7. Seja a um inteiro. Prove que um dos inteiros $a, a + 2, a + 4$ é divisível por 3.

8. Sendo a um inteiro qualquer, mostre que:

   (a) $2 \mid a(a+1)$
   (b) $3 \mid a(a+1)(a+2)$

9. Prove que, de n números consecutivos, um é múltiplo de n.

10. Prove que todo inteiro da forma $6k+5$ é também da forma $3k+2$, mas não vale a recíproca.

11. Mostre que o cubo de um inteiro qualquer é de uma das formas: $9k$, $9k+1$ ou $9k+8$.

12. Mostre que, se $a \mid (2x-3y)$ e $a \mid (4x-5y)$, então $a \mid y$, onde a, x e y são inteiros.

13. Determine os inteiros positivos que divididos por 17 deixam um resto igual ao quadrado do quociente.

14. Para todo inteiro a, prove que $4 \nmid (a^2+2)$.

15. Prove que, se a e b são inteiros com $b > 0$, então existem únicos inteiros q e r tais que $a = bq + r$, com $2b \leqslant r < 3b$.

16. Mostre que se a e b são inteiros ímpares, então $a^2 - b^2$ é divisível por 8.

17. Na divisão de dois inteiros positivos o quociente é 16 e o resto é o maior possível. Encontre os dois inteiros, sabendo que a sua soma é 341.

18. Mostre que o produto de dois inteiros ímpares é um inteiro ímpar.

19. Sendo a um inteiro, mostre que a^2 deixa resto $0, 1$ ou 4 quando dividido por 8.

20. Mostre que todo inteiro ímpar pode ser escrito como diferença de dois quadrados.

21. Sejam $a, b, m \in \mathbb{Z}$, com $m \neq 0$. Mostre que se $m \mid b-a$, então a e b deixam o mesmo resto quando divididos por m.

22. Prove que:

    (a) A soma dos quadrados de dois inteiros ímpares não pode ser um quadrado perfeito.
    (b) A diferença de dois cubos de inteiros consecutivos não é divisível por 2.

23. (a) Demonstre que todo quadrado perfeito é da forma $5k$ ou $5k \pm 1$.
    (b) Como aplicação, indique em quais algarismos pode terminar um quadrado perfeito.
    (c) Demonstre que, se três inteiros positivos a, b, c verificam a condição $a^2 = b^2 + c^2$, então, entre eles há um múltiplo de 5 e um múltiplo de 2.

2.5 Representação de um número em uma base qualquer

Teorema 2.2 (Representação em uma base) *Dado um inteiro qualquer $b \geqslant 2$, todo inteiro positivo n admite uma única representação da forma:*

$$n = a_m b^m + a_{m-1} b^{m-1} + ... + a_2 b^2 + a_1 b + a_0 \qquad (*)$$

onde $a_i \in \mathbb{Z}$ e $0 \leqslant a_i < b$, para todo $i = 0, 1, 2, ..., m$.

A ideia da demonstração é a seguinte:

Pelo algoritmo da divisão aplicados aos inteiros n e b, existem inteiros q_0 e a_0 tais que
$n = bq_0 + a_0$ com $q_0 > 0$, $0 \leqslant a_0 < b$ e $n \geqslant bq_0 > q_0$.
Agora, aplicando o algoritmo da divisão aos inteiros q_0 e b, existem inteiros q_1 e a_1 tais que
$q_0 = bq_1 + a_1$ com $q_1 > 0$, $0 \leqslant a_1 < b$ e $q_0 > q_1$ (1)
Continuando a aplicar o algoritmo da divisão aos quocientes $q_i's$ e ao inteiro b, temos:
$q_1 = bq_2 + a_2$ com $q_2 > 0$, $0 \leqslant a_2 < b$ e $q_1 > q_2$ (2)
$q_2 = bq_3 + a_3$ com $q_3 > 0$, $0 \leqslant a_3 < b$ e $q_2 > q_3$ (3)
e assim por diante.

Como $n > q_0 > q_1 > q_2 > ....$ e $q_i > 0$ para todo i, esta sequência decrescente é finita, isto é, existe um índice m tal que:
$q_{m-2} = bq_{m-1} + a_{m-1}$ com $q_{m-1} > 0$, $0 \leqslant a_{m-1} < b$ (m-1)
$q_{m-1} = bq_m + a_m$ com $q_m = 0$, $0 \leqslant a_m < b$ (m)

Multiplicando a equação (1) por b, a equação (2) por b^2, a equação (3) por b^3, ..., e a equação (m-1) por b^{m-1}, obtemos o seguinte conjunto de igualdades:

$$n = bq_0 + a_0, \quad 0 \leqslant a_0 < b$$

$$bq_0 = b^2q_1 + a_1b, \quad 0 \leqslant a_1 < b$$
$$b^2q_1 = b^3q_2 + a_2b^2, \quad 0 \leqslant a_2 < b$$
$$b^3q_2 = b^4q_3 + a_3b^3, \quad 0 \leqslant a_3 < b$$

$$.....$$

$$b^{m-1}q_{m-2} = b^m a_m + a_{m-1}b^{m-1}, \quad 0 \leqslant a_{m-1} < b$$

Somando membro a membro essas m igualdades obtemos:

$$n + bq_0 + b^2q_1 + b^3q_2 + ... + b^{m-1}q_{m-2} =$$
$$bq_0 + b^2q_1 + b^3q_2 + ... + b^{m-1}q_{m-2} + b^m a_m + a_0 + a_1b + a_2b^2 + a_3b^3 + ... + a_{m-1}b^{m-1}$$

ou seja,

$$n = a_m b^m + a_{m-1}b^{m-1} + ... + a_3b^3 + a_2b^2 + a_1b + a_0$$

onde $a_i \in \mathbb{Z}$, para todo $i \in \{0, 1, ..., m\}$, $0 < a_m < b$; $0 \leqslant a_i < b$, para todo $i \in \{0, 1, ..., m-1\}$.

A unicidade desta representação é uma consequência imediata da unicidade do algoritmo da divisão.

Formalmente, usando a segunda forma do PIM, temos a seguinte demonstração:

Prova:
Para $n = 1$ o resultado é trivialmente verdadeiro.
Para $n > 1$ suponha, por hipótese de indução, que para todo inteiro c, com $1 \leqslant c < n$, o resultado seja verdadeiro, isto é, c pode ser escrito de maneira única como

$$c = a_m b^m + ... + a_1b + a_0, \text{ onde } 0 \leqslant a_i < b$$

Devemos mostrar que o resultado é válido para n.
Pelo algoritmo da divisão de n por b, sabemos que existem únicos inteiros $q \geqslant 0$ e $0 \leqslant r < b$ tais que $n = bq + r$.
Se $q = 0$ então $n = r$ e n está na forma de representação (*).

Se $q > 0$, como $b \geqslant 2$, temos que $n = bq + r \geqslant 2q + r \geqslant 2q > q$. Logo, pela hipótese de indução aplicada a q, podemos escrever:

$$q = a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b + a_0, \text{ onde } 0 \leqslant a_i < b$$

e, portanto,

$$n = bq + r = a_m b^{m+1} + a_{m-1} b^m + ... + a_1 b^2 + a_0 b + r \text{ com } 0 \leqslant r < b$$

Obtivemos, então, uma representação de n na forma (*) e sua unicidade segue da unicidade de q e r pelo algoritmo da divisão e da unicidade da representação de q pela hipótese de indução.

■

Observação 2.7

1. *Pelo teorema anterior, dado um inteiro qualquer $b \geqslant 2$, todo inteiro positivo n pode ser representado por um polinômio inteiro em b de grau m (pois $a_m \neq 0$) ordenado segundo as potências decrescentes de b e cujos coeficientes a_i são inteiros que satisfazem $0 \leqslant a_i < b$ ($i = 0, 1, 2, ..., m$), sendo $a_m \neq 0$.*
2. *Notação: $n = (a_m a_{m-1} ... a_2 a_1 a_0)_b$.*
3. *O inteiro b chama-se base. Convencionamos não escrever o subscrito b quando estamos utilizando a base usual 10.*
4. *Se $n = (a_m a_{m-1} ... a_2 a_1 a_0)_b$ dizemos que n está escrito no sistema de base b.*

2.5.1 Exercícios

1. Escreva 105 no sistema de base 2.
2. Escreva $(100111)_2$ no sistema de base 10.
3. Escreva 31415 no sistema de base 8.
4. Escreva $(3531)_6$ no sistema de base 10.
5. Escreva $(6165)_7$ no sistema de base 12.
6. Prove que as adivinhações abaixo estão corretas:
   (a) Peça a alguém para pensar em um número com dois dígitos, a, depois peça para multiplicar o algarismo das dezenas de a por 5, somar 7, dobrá-lo e somar ao algarismo das unidades de a. Peça-lhe que diga o resultado obtido, b. Agora você pode descobrir o número pensado afirmando que $a = b - 14$.
   (b) Pense em um número com três algarismos, a. Agora multiplique o algarismo das centanas por 2, some 3, multiplique por 5, some 7, some o algarismo das dezenas de a, multiplique por 2, some 3, multiplique por 5, some o algarismo das unidades e diga o resultado, b. Se você subtrair 235 de b, você obterá o número pensado a.
7. Prove que todo número com três algarismos iguais é divisível por 37.
8. Escreva $(7645)_8$ no sistema de base 5 e $(a3b)_{12}$ no sistema de base 7.
9. Resolva a seguinte equação: $(123)_x = (1002)_4$.
10. Determine a base b do sistema no qual 73 se escreve $(243)_b$.

2.6 Alguns critérios de divisibilidade

Proposição 2.2 (Critério de divisibilidade por 2**)** *Um inteiro positivo n é divisível por* 2 *se, e somente se, o algarismo das unidades for divisível por* 2*.*

Prova:

■

Proposição 2.3 (Critério de divisibilidade por 9**)** *Um inteiro positivo n é divisível por* 9 *se, e somente se, a soma de seus algarismos é divisível por* 9*.*

Prova:

■

Proposição 2.4 (Critério de divisibilidade por 7**)** *Um inteiro $n = 10k + i$ onde i é o seu algarismo das unidades, é divisível por* 7 *se, e somente se, $k - 2i$ é divisível por* 7*.*

Prova:

■

Observação 2.8 *Para descrever melhor o critério de divisibilidade por* 7*, vejamos um exemplo.*

Seja $n = 59325$*. Separamos o dígito* 5 *das unidades e, do número restante* 5932*, subtraímos o dobro deste dígito, isto é,* $5932 - 10 = 5922$*.*

Em seguida repetimos este procedimento até a obtenção de um número suficientemente pequeno que possamos reconhecer, facilmente, se é ou não divisível por 7*, como segue:* $592 - 4 = 588$*;* $58 - 16 = 42$*.*

Como 42 *é divisível por* 7 *então* 588 *também é. Como* 588 *é divisível por* 7 *então* 5922 *também é, o que implica* 59325 *ser divisível por* 7*.*

2.6.1 Exercícios

1. Prove os seguintes critérios de divisibilidade:

   (a) Critério de divisibilidade por 3:
   Um inteiro positivo n é divisível por 3 se, e somente se, a soma de seus algarismos é divisível por 3.

   (b) Critério de divisibilidade por 4:
   Um inteiro positivo n é divisível por 4 se, e somente se, o número formado pelos dois últimos algarismos de n é divisível por 4.

   (c) Critério de divisibilidade por 5:
   Um inteiro positivo n é divisível por 5 se o algarismo das unidades for 0 ou 5.

   (d) Critério de divisibilidade por 11:
   Um inteiro positivo $n = a_m a_{m-1}...a_2 a_1 a_0$ é divisível por 11 se, e somente se, a soma alternada T dos seus algarismos, $T = a_0 - a_1 + a_2 - ... + (-1)^m a_m$, é divisível por 11.
   (Sugestão: Mostre por indução que, para todo $j \geqslant 1$, $10^j = 11c_j + (-1)^j$, onde c_j é um inteiro.)

2. Enuncie e demonstre um critério de divisibilidade por 8.

3. Usando o critério de divisibilidade por 9 e por 11, determine se os inteiros 176521221 e 349235678 são divisíveis por 9 ou por 11.

2.7 Máximo Divisor Comum

2.7.1 Máximo divisor comum de dois inteiros

Definição 2.4 *Sejam* a *e* b *dois inteiros não simultaneamente nulos, isto é,* $a \neq 0$ *ou* $b \neq 0$*. Chama-se máximo divisor comum de* a *e* b *o inteiro positivo* d *que satisfaz as condições:*

1. $d \mid a$ *e* $d \mid b$*; (*d *é um divisor comum de* a *e* b*)*
2. *Se* c *é um inteiro tal que* $c \mid a$ *e* $c \mid b$*, então* $c \leq d$*. (*d *é o maior dos divisores comuns de* a *e* b*)*

Notação: $d =$ mdc(a, b) ou, simplesmente, $d = (a, b)$

Observação 2.9 *Sejam* a *e* b *inteiros não simultaneamente nulos.*

1. *O conjunto* $D(a, b)$ *de todos os divisores comuns de* a *e* b *é não vazio, pois* $1 \in D(a, b)$*, e limitado superiormente, pois se* $a \neq 0$ *ou* $b \neq 0$*, então, para todo elemento* $c \in D(a, b)$*, temos* $c \leq |a|$ *ou* $c \leq |b|$*. Consequentemente,* $D(a, b)$ *possui maior elemento e* $mdc(a, b)$ *sempre existe e é único.*
2. *Na definição de máximo divisor comum exigimos* a *e* b *não simultaneamente nulos porque, caso contrário, qualquer inteiro* c *seria divisor comum de* a *e* b*, o que tornaria impossível tomar o maior desses números.*
3. $mdc(a, b) = mdc(b, a)$*.*

4. $mdc(a, 1) = 1$.

5. $a \neq 0 \Rightarrow mdc(a, 0) = |a|$.

6. $a \mid b$ *e* $a \neq 0 \Rightarrow mdc(a, b) = |a|$.

7. $mdc(a, b) = mdc(|a|, |b|)$.

Exemplo 2.4 *Calcular* $mdc(24, -18)$.
$D(24) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm24\}$
$D(-18) = \{\pm1, \pm2, \pm3, \pm6, \pm9, \pm18\}$
$D(24, -18) = \{\pm1, \pm2, \pm3, \pm6\}$
$mdc(24, -18) = 6$

Teorema 2.3 (Teorema de Bézout) *Sejam* a *e* b *inteiros não simultaneamente nulos e* $d = mdc(a, b)$. *Então existem inteiros* x *e* y *tais que* $d = ax + by$, *isto é, o máximo divisor comum de* a *e* b *é uma combinação linear de* a *e* b.

Prova:
Seja $S = \{au + bv : u, v \in \mathbb{Z} \text{ e } au + bv > 0\}$.
Supondo $a \neq 0$ temos que um dos inteiros $a = a.1 + b.0$ ou $-a = a.(-1) + b.0$ é positivo e, portanto, pertence a S.
Supondo $b \neq 0$ temos que um dos inteiros $b = a.0 + b.1$ ou $-b = a.0 + b.(-1)$ é positivo e, portanto, pertence a S.
Logo $S \neq \varnothing$ e, pelo PBO, S admite menor elemento s. Assim, existem inteiros x e y tais que $s = ax + by$.
Vamos mostrar que $s \mid a$ e $s \mid b$.
Pelo algoritmo da divisão de a por s, existem inteiros q e r tais que $a = sq + r$, com $0 \leq r < s$. Assim, $r = a - sq = a - (ax + by)q = a - axq - byq = a(1 - xq) + b(-yq)$. Supondo $r > 0$ temos que $r \in S$, mas isto é um absurdo pois $r < s$ e s é o menor elemento de S. Logo, $r = 0$ e $a = sq$, isto é, $s \mid a$.
Analogamente conclui-se que $s \mid b$.
Como $s \mid a$, $s \mid b$ e $d = \text{mdc}(a, b)$, então $s \leq d$.
Além disso, como $d \mid a$ e $d \mid b$ temos que $d \mid ax + by$, ou seja, $d \mid s$. Sendo $d > 0$ e $s > 0$ obtemos $d = |d| \leq |s| = s$, isto é, $d \leq s$.
De $s \leq d$ e $d \leq s$ concluimos que $d = s = ax + by$. ■

Observação 2.10

1. *A demonstração do teorema anterior mostra que* $d = mdc(a, b)$ *é o menor inteiro positivo da forma* $ax + by$, *isto é, que pode ser expresso como combinação linear de* a *e* b. *Mas esta representação do máximo divisor de* a *e* b *como combinação linear de* a *e* b *não é única, pois*

$$mdc(a, b) = d = ax + by = ax + abt - abt + by = a(x + bt) + b(y - at)$$

para todo $t \in \mathbb{Z}$.

2. *Se* $d = ar + bs$, *para algum par de inteiros* r *e* s, *então* d *não é necessariamente o máximo divisor comum de* a *e* b. *Por exemplo,* $4 = 6.2 + 4.(-2)$ *e* $4 \neq mdc(6, 4)$.

2.7.2 Inteiros primos entre si

Definição 2.5 *Sejam* a *e* b *inteiros não simultaneamente nulos. Dizemos que* a *e* b *são inteiros primos entre si ou relativamente primos se, e somente se,* $mdc(a, b) = 1$.

Exemplo 2.5
2 *e* 5 *são inteiros primos entre si.*
9 *e* -16 *são inteiros relativamente primos.*

Observação 2.11
Dois inteiros a e b primos entre si admitem como únicos divisores comuns 1 e -1.

Teorema 2.4 *Dois inteiros a e b não simultaneamente nulos são primos entre si se, e somente se, existem inteiros x e y tais que $ax + by = 1$.*

Prova:

■

Corolário 2.1 *Se $mdc(a, b) = d$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$*

Prova:

■

Corolário 2.2 *Se $a \mid c$, $b \mid c$ e $mdc(a, b) = 1$, então $ab \mid c$.*

Prova:

■

Observação 2.12 *Esse resultado não se estende a três inteiros. Por exemplo,* $mdc(6, 10, 15) = 1$ *e 6, 10, 15 dividem 30, porém* $6 \cdot 10 \cdot 15 \nmid 30$.

Corolário 2.3 (Teorema de Euclides) *Se* $a \mid bc$ *e* $mdc(a, b) = 1$*, então* $a \mid c$

Prova:

■

2.7.3 Caracterização do máximo divisor comum de dois inteiros

Teorema 2.5 *Sejam a e b inteiros não simultaneamente nulos. Um inteiro positivo d é o máximo divisor comum de a e b se, e somente se, satisfaz as seguintes condições:*

(i) $d \mid a$ *e* $d \mid b$*;*

(ii) Se c é um inteiro tal que $c \mid a$ *e* $c \mid b$*, então* $c \mid d$.

Prova:
($\Rightarrow$) Seja $d = \text{mdc}(a, b)$. Então, obviamente, d satisfaz a condição (i). Além disso, existem inteiros x e y tais que $d = ax + by$. Se $c \mid a$ e $c \mid b$ então $c \mid ax + by$ e, portanto, $c \mid d$, isto é, a condição (ii) também é satisfeita.

($\Leftarrow$) Seja d um inteiro positivo satisfazendo (i) e (ii). Desejamos mostrar que $d = \text{mdc}(a, b)$, ou seja:
(1) $d \mid a$ e $d \mid b$;
(2) Se c é um inteiro tal que $c \mid a$ e $c \mid b$ então $c \leq d$.
A condição (1) é satisfeita por (i).
Se $c \mid a$ e $c \mid b$, então $c \mid d$ por (ii) e, como $d > 0$, temos $c \leq |c| \leq |d| = d$, desta forma a condição (2) também é satisfeita.
Logo, $d = \text{mdc}(a, b)$. ■

2.7.4 Máximo divisor comum de vários inteiros

O conceito de máximo divisor comum definido para dois inteiros a e b estende-se de maneira natural a mais de dois inteiros.

Por exemplo:

Sejam a, b e c inteiros não todos nulos. O máximo divisor comum de a, b e c, denotado por $\text{mdc}(a, b, c)$, é o inteiro positivo d que satisfaz as seguintes condições:

(1) $d \mid a$, $d \mid b$ e $d \mid c$;

(2) Se e é um inteiro tal que $e \mid a$, $e \mid b$ e $e \mid c$, então $e \leq d$.

Observação 2.13 *Três inteiros* a, b *e c podem ser primos entre si, isto é,* $mdc(a, b, c) = 1$*, sem que sejam primos entre si dois a dois.*

Por exemplo: $mdc(6, 10, 15) = 1$*,* $mdc(6, 10) = 2$*,* $mdc(6, 15) = 3$ *e* $mdc(10, 15) = 5$.

Teorema 2.6 *Sejam a, b e c inteiros com $a \neq 0$. Então $mdc(a, b, c) = mdc(mdc(a, b), c)$.*

Prova:
Sejam $d = \text{mdc}(a, b, c)$ e $e = \text{mdc}(a, b)$. Desejamos mostrar que $d = \text{mdc}(e, c)$.
Temos que $d \mid a$, $d \mid b$ e $d \mid c$, então, pelo teorema (2.5), $d \mid e$. Logo $d \mid e$ e $d \mid c$.
Se f é um inteiro tal que $f \mid e$ e $f \mid c$ então, como $e \mid a$ e $e \mid b$, temos $f \mid a$, $f \mid b$ e $f \mid c$. Logo $f \leq d$, e, portanto, $d = \text{mdc}(e, c)$. ∎

Exemplo 2.6 $mdc(10, 15, 30) = mdc(mdc(10, 15), 30) = mdc(5, 30) = 5$.

2.7.5 Exercícios

1. Sejam a, b e c inteiros com $a \neq 0$. Verifique se as afirmações abaixo são verdadeiras ou falsas, dando a demonstração ou um contra-exemplo:

   (a) $\text{mdc}(\text{mdc}(a, b), c) = \text{mdc}(b, \text{mdc}(a, c))$
   (b) $\text{mdc}(a, b + c) = \text{mdc}(a, b) + \text{mdc}(a, c)$
   (c) $\text{mdc}(a, bc) = \text{mdc}(a, b).\text{mdc}(a, c)$
   (d) $\text{mdc}(a, a) = |a|$
   (e) $\text{mdc}(a, bc) = b.\text{mdc}(a, c)$

2. Mostre que se a é um inteiro ímpar, então $24 \mid a(a^2 - 1)$.

3. Demonstre que $30 \mid (n^5 - n)$, para todo inteiro n.

4. Sabendo que $\text{mdc}(a, 0) = 13$, encontre os valores do inteiro a.

5. Encontre o menor inteiro positivo c da forma $c = 22x + 55y$, onde x e y são inteiros.

6. Sendo n um inteiro qualquer, calcule $\text{mdc}(n, n + 1)$.

7. Calcule:

   (a) $\text{mdc}(n, n + 2)$, sendo n um inteiro par;
   (b) $\text{mdc}(n, n + 2)$, sendo n um inteiro ímpar.

8. Sendo n um inteiro, encontre os possíveis valores de $\text{mdc}(n, n + 10)$.

9. Sendo n um inteiro, calcule $\text{mdc}(n - 1, n^2 + n + 1)$.

10. Calcule $\text{mdc}(a + b, a - b)$, sabendo que a e b são inteiros primos entre si.

11. O máximo divisor comum de dois inteiros positivos é 10 e o maior deles é 120. Determine o outro inteiro.

12. Determine os inteiros positivos a e b sabendo que:

    (a) $a + b = 63$ e $\text{mdc}(a, b) = 9$;
    (b) $ab = 756$ e $\text{mdc}(a, b) = 6$.

13. Sejam a e b inteiros não simultaneamente nulos, $d = \text{mdc}(a, b)$ e k um inteiro não nulo. Prove que:

    (a) $\text{mdc}(ka, kb) = |k|.d$;
    (b) Se $k \mid a$ e $k \mid b$, então $\text{mdc}\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{d}{|k|}$.

14. Sejam a, b e c inteiros. Prove que:

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

15. Sejam a, b e c inteiros. Prove que:

    (a) Se $\text{mdc}(a, b) = 1$, então $\text{mdc}(ac, b) = \text{mdc}(b, c)$.
    (b) Se $\text{mdc}(a, b) = 1$ e se $c \mid a + b$, então $\text{mdc}(a, c) = 1 = \text{mdc}(b, c)$.
    (c) Se $b \mid c$, então $\text{mdc}(a, b) = \text{mdc}(a + c, b)$.
    (d) Se $\text{mdc}(a, b) = 1$, então $\text{mdc}(a^m, b^n) = 1$ onde m e n são inteiros positivos.

16. Se $\text{mdc}(a, 4) = 2 = \text{mdc}(b, 4)$, mostre que $\text{mdc}(a + b, 4) = 4$.

17. Se $\text{mdc}(n, 6) = 1$, mostre que $12 \mid n^2 - 1$.

18. Sabendo que $\text{mdc}(a, b) = 1$, demonstre que:

    (a) $\text{mdc}(2a + b, a + 2b) = 1$ ou 3;
    (b) $\text{mdc}(a + b, a^2 + b^2) = 1$ ou 2;
    (c) $\text{mdc}(a + b, a^2 - ab + b^2) = 1$ ou 3.

19. Sejam a e b inteiros não simultaneamente nulos e $d = \text{mdc}(a, b)$. Dado um inteiro c tal que $a \mid c$ e $b \mid c$, prove que $\dfrac{ab}{d} \mid c$.

20. Mostrar que $D(a, b) = D(d)$, onde $d = mdc(a, b)$ ($a \neq 0$ ou $b \neq 0$).

2.7.6 Algoritmo de Euclides (método para encontrar o máximo divisor comum)

Lema 2.2 *Sejam a e b inteiros com $b \neq 0$ e sejam q e r o quociente e o resto da divisão de a por b, respectiamente, ou seja, $a = bq + r$. Então $mdc(a, b) = mdc(b, r)$.*

Prova:

■

Sejam a e b inteiros não simultaneamente nulos. Desejamos determinar o máximo divisor comum de a e b. É imediato:

1. Se $a \neq 0$, então $\text{mdc}(a, 0) = |a|$.
2. Se $a \neq 0$, então $\text{mdc}(a, a) = |a|$.
3. Se $b \mid a$ e $b \neq 0$, então $\text{mdc}(a, b) = |b|$.

Além disso, como $\text{mdc}(a,b) = \text{mdc}(|a|,|b|) = \text{mdc}(b,a)$, a determinação do máximo divisor comum de reduz ao caso $a > b > 0$ e $b \nmid a$. Nestas condições, a aplicação repetida do algoritmo da divisão nos dá as seguintes igualdades:

$$a = bq_1 + r_1 \quad , \quad 0 < r_1 < b$$
$$b = r_1q_2 + r_2 \quad , \quad 0 < r_2 < r_1$$
$$r_1 = r_2q_3 + r_3 \quad , \quad 0 < r_3 < r_2$$
$$r_2 = r_3q_4 + r_4 \quad , \quad 0 < r_4 < r_3$$
$$\text{.....}$$

Como os restos $r_1, r_2, r_3, r_4, ...$ são todos inteiros positivos tais que $b > r_1 > r_2 > r_3 > r_4 > ...$ e existem apenas $b-1$ inteiros positios menores do que b, então necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, para algum $n \in \mathbb{N}$, isto é:

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

O último resto $r_n \neq 0$ que aparece nesta sequência de divisões é o máximo divisor comum de a e b, pois, pelo lema anterior, temos:

$$\text{mdc}(a,b) = \text{mdc}(b,r_1) = \text{mdc}(r_1,r_2) = ... = \text{mdc}(r_{n-2},r_{n-1}) = \text{mdc}(r_{n-1},r_n) = r_n$$

pois $r_n \mid r_{n-1}$

Rigorosamente, temos:

Algoritmo de Euclides:

Sejam a e b inteiros $a > b > 0$ e $b \nmid a$. Aplicando o algoritmo mencionado anteriormente a eles, ou seja, aplicação sucessiva do algoritmo da divisão até obter resto nulo, tem-se que o máximo divisor comum de a e b é o último resto não nulo obtido.

Prova: A demonstração será feita por indução no número de passos do algoritmo citado. Para isso, consideremos a seguinte afirmação:

$P(n)$: se ao aplicarmos o algoritmo de Euclides aos inteiros a e b obtivermos o primeiro resto nulo após $(n+1)$ passos, então $mdc(a,b)$ é igual ao último resto não nulo obdito.

Se $n = 1$, então $mdc(a,b) = mdc(b,r_1) = r_1$. Logo, $P(1)$ é verdadeira.

Suponhamos então, por hipótese de indução, que $P(n)$ seja verdadeira e mostremos que $P(n+1)$ é verdadeira.

Sejam a, b inteiros tais que, aplicando-se o algoritmo acima a eles obtemos o primeiro resto nulo após $(n+1)+1 = n+2$ passos, isto é,

$$a = bq_1 + r_1 \quad , \quad 0 < r_1 < b$$
$$b = r_1q_2 + r_2 \quad , \quad 0 < r_2 < r_1$$
$$r_1 = r_2q_3 + r_3 \quad , \quad 0 < r_3 < r_2$$
$$r_2 = r_3q_4 + r_4 \quad , \quad 0 < r_4 < r_3$$
$$\text{.....}$$
$$r_{n-2} = r_{n-1}q_n + r_n \quad , \quad 0 < r_n < r_{n-1}$$
$$r_{n-1} = r_nq_{n+1} + r_{n+1} \quad , \quad 0 < r_{n+1} < r_n$$

$$r_n = r_{n+1}q_{n+2}$$

Queremos provar que $mdc(a,b) = r_{n+1}$. Vemos que se aplicamos o mesmo algoritmo aos inteiros b e r_1, temos o primeiro resto nulo após $(n+2)-1 = n+1$ passos e, portanto, pela hipótese de indução, $mdc(b,r_1) = r_{n+1}$. Mas, pelo lema, temos que $mdc(a,b) = mdc(b,r_1)$. Logo, $mdc(a,b) = r_{n+1}$ e $P(n+1)$ é verdadeira.

■

Dispositivo prático para o Algoritmo de Euclides:

	q_1	q_2	q_3				q_n	q_{n+1}
a	b	r_1	r_2	r_3	...	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4			r_n	0	

Tabela 2.1: $a > b > 0$ e $b \nmid a \Rightarrow \text{mdc}(a,b) = r_n$

Observação 2.14

1. *O Algoritmo de Euclides é também denominado de Processo das Divisões Sucessivas.*
2. *O Algoritmo de Euclides também pode ser usado para encontrar uma expressão do $mdc(a,b) = r_n$ como combinação linear de a e b. Basta eliminar sucessivamente os restos $r_{n-1}, r_{n-2}, ..., r_3, r_2, r_1$ entre as n primeiras igualdades anteriores.*

Exemplo 2.7

(a) Encontre o $mdc(726, -275)$ pelo algoritmo de Euclides e sua expressão como combinação linear de 726 e -275.

(b) O máximo divisor comum de dois inteiros positivos a e b é 74 e na sua determinação pelo algoritmo de Euclides os quocientes obtidos foram $1, 2, 2, 5, 1$ e 3. Calcule a e b.

2.7.7 Algoritmo euclidiano estendido

Se $d = \text{mdc}(a, b)$, como encontrar x e y inteiros tais que $d = ax + by$ de uma maneira mais simples?

Calculando o máximo divisor comum entre a e b, obtemos a sequência de divisões, que vamos reescrever na forma:

$$a = bq_1 + r_1 \quad e \quad r_1 = ax_1 + by_1$$

$$b = r_1q_2 + r_2 \quad e \quad r_2 = ax_2 + by_2$$

$$r_1 = r_2q_3 + r_3 \quad e \quad r_3 = ax_3 + by_3$$

$$r_2 = r_3q_4 + r_4 \quad e \quad r_4 = ax_4 + by_4$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1}q_n + r_n \quad e \quad r_n = ax_n + by_n$$

$$r_{n-1} = r_nq_{n+1} \quad e \quad r_{n+1} = 0$$

Os números $x_1, x_2, ..., x_n$ e $y_1, y_2, ..., y_n$ são inteiros a determinar.

Vamos condensar a informação acima em uma tabela:

restos	**quocientes**	**x**	**y**
a	$*$	x_{-1}	y_{-1}
b	$*$	x_0	y_0
r_1	q_1	x_1	y_1
r_2	q_2	x_2	y_2
r_3	q_3	x_3	y_3
...	...	...	...
r_{j-2}	q_{j-2}	x_{j-2}	y_{j-2}
r_{j-1}	q_{j-1}	x_{j-1}	y_{j-1}
$\mathbf{r_j}$	$\mathbf{q_j}$	$\mathbf{x_j}$	$\mathbf{y_j}$
...	...	...	...
r_{n-2}	q_{n-2}	x_{n-2}	y_{n-2}
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}
r_n	q_n	x_n	y_n

Tabela 2.2: Algoritmo euclidiano estendido

Observação 2.15

1. *As duas primeiras linhas da tabela, denominadas linha* -1 *e linha* 0*, "legalmente"não deveriam existir, pois nem* a *e nem* b *são restos.*

2. *Preenchimento das colunas* $\boldsymbol{x}$ *e* $\boldsymbol{y}$*:*
   Vamos supor que já recebemos a tabela preenchida até a $(j-1)$*-ésima linha. Começamos a preencher a* j*-ésima linha dividindo* r_{j-2} *por* r_{j-1} *para encontrar* $\mathbf{r_j}$ *e* $\mathbf{q_j}$*, de forma que* $r_{j-2} = r_{j-1}q_j + r_j$ *e* $0 \leq r_j < r_{j-1}$*. Assim* $r_j = r_{j-2} - r_{j-1}q_j$*.* ***(I)***

3. *Lendo nas linhas* $(j-1)$ *e* $(j-2)$ *os valores de* $x_{j-2}, x_{j-1}, y_{j-2}$ *e* y_{j-1}*, podemos escrever* $r_{j-2} = ax_{j-2} + by_{j-2}$ *e* $r_{j-1} = ax_{j-1} + by_{j-1}$*.*
   Substituindo estes valores em ***(I)****, obtemos:*
   $r_j = (ax_{j-2} + by_{j-2}) - (ax_{j-1} + by_{j-1})q_j = a(x_{j-2} - q_jx_{j-1}) + b(y_{j-2} - q_jy_{j-1})$
   Portanto, $\mathbf{x_j} = x_{j-2} - q_jx_{j-1} \quad e \quad \mathbf{y_j} = y_{j-2} - q_jy_{j-1}$*.*

4. *Para calcular* x_j *e* y_j*, usamos apenas valores contidos nas duas linhas imediatamente anteriores à linha* j*, além do quociente* q_j*.*

5. *Concluindo: sabemos preencher qualquer linha da tabela, desde que as duas que a precedem sejam conhecidas.*

6. *Para preencher as linhas* -1 *e* 0 *usamos o mesmo procedimento. Devemos ter* $a = ax_{-1} + by_{-1}$ *e* $b = ax_0 + by_0$ *o que nos sugere escolher* $x_{-1} = 1, y_{-1} = 0, x_0 = 0$ *e* $y_0 = 1$*, o que nos possibilita começar o processo recursivo para determinar a tabela acima.*

7. *Finalizado o preenchimento da tabela e descoberto o mdc entre* a *e* b*, obtemos, também,* $d = r_n = ax_n + by_n$*, ou seja,* $x = x_n$ *e* $y = y_n$ *são os inteiros procurados.*

Exemplo 2.8 *Encontre uma expressão do* $mdc(726, -275)$ *como combinação linear de* 726 *e* -275*, usando o algoritmo euclidiano estendido.*

2.8 Mínimo múltiplo comum

2.8.1 Múltiplos comuns de dois inteiros

O conjunto de todos os múltiplos de um inteiro qualquer a indica-se por $M(a) = \{x \in \mathbb{Z} : a \mid x\} = \{aq : q \in \mathbb{Z}\}$.

Exemplo 2.9
$M(1) = \mathbb{Z}$
$M(0) = \{0\}$
$M(-5) = \{-5q : q \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, \pm 15, ...\}$
$M(a) = M(-a),\ \forall a \in \mathbb{Z}$

Definição 2.6 *Chama-se múltiplo comum dos inteiros* a *e* b*, todo inteiro* x *tal que* $a \mid x$ *e* $b \mid x$*. Em outras palavras, múltiplo comum de* a *e* b *é todo inteiro que pertence simultaneamente aos conjuntos* $M(a)$ *e* $M(b)$*. O conjunto de todos os múltiplos comuns de* a *e* b *indica-se por* $M(a, b)$*, isto é,*

$$M(a,b) = \{x \in \mathbb{Z} : a \mid x \text{ e } b \mid x\} = \{x \in \mathbb{Z} : x \in M(a) \text{ e } x \in M(b)\} = M(a) \cap M(b)$$

Observação 2.16

1. $M(a,b) = M(b,a)$
2. $M(a,b) \neq \varnothing$, *pois* $0 \in M(a) \cap M(b) = M(a,b)$

Exemplo 2.10
$M(6) = \{0, \pm6, \pm12, \pm18, \pm24, \pm30, \pm36, \pm48, ...\}$
$M(-8) = \{0, \pm8, \pm16, \pm32, \pm40, \pm48, ...\}$
$M(6,-8) = M(6) \cap M(-8) = \{0, \pm24, \pm48, ...\}$

2.8.2 Mínimo múltiplo comum de dois inteiros

Definição 2.7 *Sejam a e b inteiros não nulos. Um inteiro positivo m é mínimo múltiplo comum de a e b se, e somente se, satisfaz as seguintes condições:*

1. $a \mid m$ *e* $b \mid m$; *(m é múltiplo comum de a e b)*
2. *Se c é um inteiro positivo tal que $a \mid c$ e $b \mid c$, então $m \leq c$. (m é o menor múltiplo comum positivo de a e b)*

Notação: $m = \text{mmc}(a,b)$

Observação 2.17 *Sejam a e b inteiros não nulos.*

1. *O conjunto $M_+^*(a,b)$ dos múltiplos comuns positivos de a e b é não vazio, pois $|ab| \in M_+^*(a,b)$. Assim, pelo PBO, $M_+^*(a,b)$ possui menor elemento e, portanto, o mínimo múltiplo comum de a e b sempre existe e é único.*
2. $mmc(a,b) \leq |ab|$, *pois* $|ab| \in M_+^*(a,b)$.
3. $mmc(a,b) = mmc(b,a)$.
4. $mmc(a,b) = mmc(|a|,|b|)$.
5. *Se* $a \mid b$, *então* $mmc(a,b) = |b|$.

Exemplo 2.11
$M(12) = \{0, \pm12, \pm24, \pm36, \pm48, \pm60, \pm72, ...\}$
$M(-18) = \{0, \pm18, \pm36, \pm54, \pm72, \pm90, ...\}$
$M(12,-18) = \{0, \pm36, \pm72, ...\}$
$mmc(12,-18) = 36$

2.8.3 Relação entre mdc e mmc

Lema 2.3 *Sejam a e b inteiros não nulos e $mmc(a,b) = m$. Então $M(m) = M(a,b)$.*

Prova:
Seja $x \in M(m)$. Então $m \mid x$. Como $m = \text{mmc}(a,b)$ temos $a \mid m$ e $b \mid m$ e, como $m \mid x$, obtemos $a \mid x$ e $b \mid x$. Logo $x \in M(a,b)$ e, portanto, $M(m) \subset M(a,b)$.

Seja $x \in M(a,b)$. Então $a \mid x$ e $b \mid x$. Pelo algoritmo da divisão de x por m, existem inteiros q e r tais que $x = mq + r$, com $0 \leq r < m$. Como $a \mid x$, $b \mid x$, $a \mid m$ e $b \mid m$, então $a \mid x - mq$ e $b \mid x - mq$, isto é, $a \mid r$ e $b \mid r$. Supondo $r > 0$ temos que $m \leq r$, pois $m = \text{mmc}(a,b)$, o que é um absurdo já que $r < m$. Logo $r = 0$ e $x = mq$, ou seja, $x \in M(m)$. Portanto $M(a,b) \subset M(m)$. ∎

Teorema 2.7 *Se a e b são inteiros não nulos, então $mdc(a,b).mmc(a,b) = |ab|$.*

Prova:
Sejam $d = \text{mdc}(a,b)$ e $m = \text{mmc}(a,b)$. Temos:
$a \mid a.\frac{b}{d}$ e $b \mid b.\frac{a}{d} \Rightarrow \frac{ab}{d} \in M(a,b) \Rightarrow \frac{|ab|}{d} \in M(a,b) = M(m) \Rightarrow \exists k \in \mathbb{Z}$ tal que $\frac{|ab|}{d} = k.m$.
Como $|ab| > 0, d > 0$ e $m > 0$, então $k > 0$.
Temos também: $\frac{|a|}{d} = \frac{m}{|b|}.k$ e $\frac{|b|}{d} = \frac{m}{|a|}.k$, o que implica $k \in D\left(\frac{|a|}{d}\right) \cap D\left(\frac{|b|}{d}\right)$. Mas $\text{mdc}\left(\frac{|a|}{d}, \frac{|b|}{d}\right) = \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Assim k é um inteiro tal que $0 < k \leq 1$, ou seja, $k = 1$.
Logo, $\frac{|ab|}{d} = k.m = 1.m = m$ e, portanto, $|ab| = d.m$, isto é, $|ab| = \text{mdc}(a,b).\text{mmc}(a,b)$. ■

Exemplo 2.12
Determinar $mmc(726, -275)$.
Pelo algoritmo de Euclides temos que $mdc(726, -275) = 11$
Logo $mmc(726, -275) = \frac{726 \times 275}{11} = 18.150$

Corolário 2.4 *Para todo par de inteiros positivos a e b, $mmc(a,b) = ab$ se, e somente se, $mdc(a,b) = 1$.*

Prova: Aplicação direta do teorema anterior. ■

Teorema 2.8 (Teorema de caracterização do mmc) *Sejam a e b inteiros não nulos. O inteiro positivo m é $mmc(a,b)$ se, e somente se, m satisfaz as seguintes condições:*

(i) $a \mid m$ *e* $b \mid m$*;*

(ii) Se c é um inteiro tal que $a \mid c$ e $b \mid c$, então $m \mid c$.

Prova:
($\Rightarrow$) Seja $m = \text{mmc}(a,b)$. Então m satisfaz a condição (i).
Se c é um inteiro tal que $a \mid c$ e $b \mid c$, então $c \in M(a,b) = M(m)$, pelo lema. Logo $m \mid c$ e, portanto, a condição (ii) também é satisfeita.
($\Leftarrow$) Seja m um inteiro positivo satisfazendo (i) e (ii). Desejamos mostrar que $m = \text{mmc}(a,b)$, ou seja:

(1) $a \mid m$ e $b \mid m$;

(2) Se c é um inteiro positivo tal que $a \mid c$ e $b \mid c$, então $m \leq c$.

A condição (1) é satisfeita por (i).
Se c é um inteiro positivo tal que $a \mid c$ e $b \mid c$, então $m \mid c$ por (ii) e, obtemos $m = |m| \leq |c| = c$.
Logo, $m = \text{mmc}(a,b)$. ■

Observação 2.18 *O conceito de mínimo múltiplo comum definido para dois inteiros a e b não nulos estende-se de maneira natural a mais de dois inteiros. Por exemplo, para a, b e c inteiros não nulos, o mínimo múltiplo comum de a, b e c, denotado por $mmc(a,b,c)$, é o inteiro positivo m que satisfaz as seguintes condições:*

1. $a \mid m$, $b \mid m$ e $c \mid m$;

2. Se e é um inteiro positivo tal que $a \mid e$, $b \mid e$ e $c \mid e$, então $m \leq e$.

2.8.4 Exercícios

1. Encontre o máximo divisor comum dos seguintes inteiros e sua expressão como combinação linear desses inteiros pelo Algoritmo de Euclides:

   (a) 232 e 136;

   (b) -187 e -221.

2. Usando a relação existente entre mdc e mmc, calcule o mínimo múltiplo comum dos pares de inteiros do exercício anterior.

3. Sendo a e b inteiros não nulos, mostre que $\text{mdc}(a, b)$ divide $\text{mmc}(a, b)$.

4. Mostre que se a e b são inteiros positivos tais que $\text{mdc}(a, b) = \text{mmc}(a, b)$, então $a = b$.

5. Determine os inteiros positivos a e b sabendo que:

   (a) $ab = 4.032$ e $\text{mmc}(a, b) = 336$

   (b) $\text{mdc}(a, b) = 8$ e $\text{mmc}(a, b) = 560$

   (c) $a + b = 589$ e $\dfrac{\text{mmc}(a, b)}{\text{mdc}(a, b)} = 84$

6. Para todo $n \in \mathbb{Z}$, $n \neq 0, -1$, calcule:

   (a) $\text{mmc}(n, n + 1)$

   (b) $\text{mmc}(2n - 1, 2n + 1)$

   (c) $\text{mmc}(2n, 2n + 2)$

7. Dados os inteiros não nulos a e b, prove que:

   (a) $\text{mdc}(a, b) = \text{mmc}(a, b)$ se, e somente se, $|a| = |b|$.

   (b) Para todo $k \in \mathbb{Z}$, $k \neq 0$, $\text{mmc}(ka, kb) = |k|.\text{mmc}(a, b)$.

   (c) Se $k \mid a$ e $k \mid b$, então $\text{mmc}\left(\dfrac{a}{k}, \dfrac{b}{k}\right) = \dfrac{\text{mmc}(a, b)}{|k|}$.

Capítulo 3

Números primos e o Teorema Fundamental da Aritmética

3.1 Números primos e compostos

Definição 3.1 *Seja $n \in \mathbb{N}$, com $n > 1$. Dizemos que n é um número primo se seus únicos divisores positivos são a unidade e ele mesmo. Caso contrário, dizemos que n é composto.*

Em outras palavras, um número natural $n > 1$ é primo se sempre que escrevermos $n = a.b$, com $a, b \in \mathbb{N}$, temos necessariamente $a = 1, b = n$ ou $a = n, b = 1$. Consequentemente um número natural $n > 1$ é composto se existem $a, b \in \mathbb{N}$, com $1 < a < n$ e $1 < b < n$, tais que $n = ab$.

Exemplo 3.1 $2, 3, 5, 7, 11$ *são números primos.*
$4, 6, 8, 9, 10$ *são números compostos.*

Observação 3.1

1. *O número* 1 *não é primo nem composto.*
2. *Se $a \in \mathbb{Z}$, $a > 0$, então ou a é primo, ou a é composto, ou $a = 1$.*
3. *O número* 2 *é o único natural par que é primo. (Verifique isto!)*
4. *De acordo com a definição acima, para decidir se um dado número n é primo é necessário verificar a divisibilidade dele por todos os números naturais menores que ele, o que fica extremamente trabalhoso à medida que avançamos na sequência dos números naturais. Os resultados a seguir nos garantem que é suficiente testar a divisibilidade de n pelos primos menores que a sua raiz quadrada.*

Proposição 3.1 *Seja $n \in \mathbb{N}$, com $n \geqslant 2$. Então n admite pelo menos um divisor primo.*

Prova:
Seja $S = \{x \in \mathbb{N} : x \geqslant 2 \text{ e } x \mid n\}$.
Temos que $S \subset \mathbb{N}$ e $S \neq \varnothing$, pois $n \in S$. Logo, pelo PBO, S admite menor elemento p.
Vamos mostrar que p é primo.
De fato, se p não fosse primo e como $p \geqslant 2$, existiriam naturais a e b tais que $p = ab$, onde $1 < a < p$ e $1 < b < p$.
Como $a \mid p$ e $p \mid n$, então $a \mid n$. Temos também que $a \in \mathbb{N}$ e $a \geqslant 2$. Logo $a \in S$, contrariando a minimalidade de p, pois $a < p$.
Portanto, p é primo. ∎

Proposição 3.2 *Seja $n \in \mathbb{N}$, com $n \geqslant 2$. Se n é composto, então n admite pelo menos um fator primo $p \leqslant \sqrt{n}$.*

Prova:
Como n é composto então existem naturais a e b tais que $n = a.b$, onde $1 < a < n$ e $1 < b < n$.
Supondo $a \leqslant b$ temos $a^2 \leqslant a.b = n$, isto é, $a \leqslant \sqrt{n}$. Pela proposição anterior existe p primo tal que $p \mid a$.
Como $p \mid a$ e $a \mid n$, então $p \mid n$ e temos também que $p \leqslant a \leqslant \sqrt{n}$.
Logo, n possui um divisor primo $p \leqslant \sqrt{n}$. ■

Observação 3.2

1. *A proposição anterior fornece um processo que permite reconhecer se um dado natural $n > 1$ é primo ou é composto. Basta dividir n sucessivamente pelos primos $\leq \sqrt{n}$; se a divisão for exata para algum primo $\leq \sqrt{n}$, então n é composto, caso contrário n é primo.*

   Exemplo 3.2 *Determine se $n = 1969$ é primo.*

2. *É conveniente então termos à nossa disposição uma lista de primos. Várias tabelas de números primos, até certo limite, já foram calculadas. O cálculo destas tabelas baseia-se num algoritmo ou crivo, desenvolvido por Eratósthenes (276-194 a.c.), que consiste no seguinte:*

3.2 Crivo de Eratósthenes

Escrevem-se na ordem natural todos os números naturais a partir de 2 até n e, em seguida, eliminam-se todos os inteiros compostos que são múltiplos dos primos p tais que $p \leqslant \sqrt{n}$, isto é, $2p, 3p, 4p, ...$, até n. Os números que sobrarem na tabela são todos os primos entre 2 e n.

Exemplo 3.3 *Contrua a tabela de todos os primos menores que* 100.

	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

Teorema 3.1 *Se um número primo p não divide um inteiro a, então a e p são inteiros primos entre si.*

Prova:

■

Corolário 3.1 *Se p é um número primo tal que $p \mid ab$, onde $a, b \in \mathbb{Z}$, então $p \mid a$ ou $p \mid b$.*

Prova:

■

Corolário 3.2 *Se p é um número primo tal que $p \mid a_1.a_2.....a_n$, onde $a_i \in \mathbb{Z}$, para todo $i \in \{1, 2, 3, ..., n\}$, então $p \mid a_k$ para algum $k \in \{1, 2, 3, ..., n\}$.*

Prova:

■

Corolário 3.3 *Se os inteiros $p, q_1, q_2, ..., q_n$ são todos números primos e se $p \mid q_1.q_2....q_n$, então $p = q_k$ para algum $k \in \{1, 2, 3, ..., n\}$.*

Prova:

■

Teorema 3.2 (Euclides) *Existem infinitos números primos.*

Prova:

■

Proposição 3.3 *Dado um número natural $n \geqslant 2$, existem n números compostos consecutivos.*

Prova:

■

Observação 3.3 *Sabendo-se que existem infinitos números primos coloca-se a questão da distribuição deles na sequência dos números naturais e a proposição anterior parece indicar que os números primos não estão distribuídos de maneira regular e que eles são cada vez mais raros a medida que se avança na sequência numérica. Por outro lado, dizemos que dois primos são gêmeos se eles são números ímpares consecutivos, como por exemplo,* 3 *e* 5, 5 *e* 7, 11 *e* 13, 239 *e* 241 *e um antigo problema que até hoje não foi resolvido é se existe ou não um número infinito de primos gêmeos.*

Um resultado importante sobre a distribuição dos números primos diz respeito à função $\Pi : \mathbb{N} \to \mathbb{Z}$ definida por $\Pi(n) = n^o$ de primos positivos menores ou iguais a n. O Teorema de Euclides (teorema 3.2) nos diz que $\lim_{n\to\infty} \Pi(n) = \infty$. Gauss (1777-1855) conjecturou empiricamente que, para valores grandes de n, $\Pi(n)$ era aproximadamente $\frac{n}{\ln n}$ e este resultado foi demonstrado em 1896 por Jacques Hadamard e Charles Jean de la Vallée-Poussin, chamado de Teorema dos Números Primos. Posteriormente uma prova mais elementar foi dada pelos matemáticos Atle Selberg e Paul Erdös.

A tabela seguinte compara os valores de $\Pi(x)$ com as aproximações x/lnx.

x	$\Pi(x)$	$\Pi(x) - x/\ln x$	$\Pi(x)/(x/\ln x)$
10	4	(0,3)	0,921
10^3	168	23	1,161
10^5	9.592	906	1,104
10^7	664.579	44.158	1,071
10^9	50.847.534	2.592.592	1,054
10^{11}	4.118.054.813	169.923.159	1,043
10^{13}	346.065.536.839	11.992.858.452	1,034
10^{15}	29.844.570.422.669	891.604.962.452	1,031

3.3 Teorema Fundamental da Aritmética

Teorema 3.3 (Fundamental da Aritmética) *Um número natural $n \geqslant 2$ ou é primo ou pode ser escrito de maneira única, a menos da ordem dos fatores, como um produto de números primos.*

Prova:

Existência: (Por indução sobre n)

Seja $P(n)$ a afirmativa: n é um número primo ou pode ser escrito como um produto de números primos.

$P(2)$ é verdadeira, pois 2 é primo.

Suponhamos a afirmativa verdadeira para todo natural m com $2 \leqslant m \leqslant k$ e provemos que $P(k+1)$ é verdadeira.

Se $k+1$ é primo , então $P(k+1)$ é verdadeira.

Se $k+1$ não é primo, então $k+1$ pode ser escrito como $k+1 = a.b$, onde $a, b \in \mathbb{N}$, $2 \leqslant a \leqslant k$ e $2 \leqslant b \leqslant k$. Pela hipótese de indução, a e b são primos ou podem ser escritos como produto de primos. Logo, $k+1 = a.b$ é também um produto de números primos, ou seja, $P(k+1)$ é verdadeira.

Unicidade:

Seja $S = \{n \in \mathbb{N} : n$ tem duas decomposições distintas como produto de primos$\}$ e suponhamos, por absurdo, que $S \neq \varnothing$. Logo, pelo PBO, S tem menor elemento m. Assim, $m = p_1p_2...p_r = q_1q_2...q_s$, onde p_i, q_j são primos para $i = 1, 2, ..., r$ e $j = 1, 2, ..., s$ e ainda $p_1 \leqslant p_2 \leqslant ... \leqslant p_r$ e $q_1 \leqslant q_2 \leqslant ... \leqslant q_s$.

Daí segue que:

$p_1 \mid m \Rightarrow p_1 \mid q_1q_2...q_s \Rightarrow p_1 = q_k$, para algum $k \in \{1, 2, ..., s\} \Rightarrow p_1 \geqslant q_1$

$q_1 \mid m \Rightarrow q_1 \mid p_1p_2...p_r \Rightarrow q_1 = p_h$, para algum $h \in \{1, 2, ..., r\} \Rightarrow q_1 \geqslant p_1$

Segue que $p_1 = q_1$ e, portanto, $p_2p_3...p_r = q_2q_3...q_s$ representando duas decomposições diferentes como produto de primos para um natural menor do que m, contrariando, assim, o fato de m ser o elemento mínimo de S.

Portanto $S = \varnothing$. ∎

Corolário 3.4 *Todo número inteiro não nulo diferente de* ± 1 *pode ser escrito como* ± 1 *vezes um número primo ou um produto de números primos. Esta expressão é única exceto pela ordem na qual os fatores primos aparecem.*

Observação 3.4

1. *Um número negativo q cujo simétrico $-q$ é um número natural primo é chamado de primo negativo. Por exemplo,* $2, 3, 5$ *são números primos enquanto* $-2, -3, -5$ *são primos negativos.*

2. *Na fatoração de um número natural $a > 1$, o mesmo primo p pode aparecer várias vezes e, então, agrupando estes primos, podemos escrever a decomposição de a em fatores primos como:*

$$a = p_1^{r_1}p_2^{r_2}...p_n^{r_n}$$

onde para cada $i = 1, 2, ..., n$, r_i é um inteiro positivo e p_i é um primo com $p_1 < p_2 < ... < p_n$.
Esta decomposição é denominada ***decomposição canônica*** *do natural $a > 1$.*
Exemplo: $360 = 2^3.3^2.5$

3. *Conhecidas as decomposições canônicas de dois naturais $a > 1$ e $b > 1$, o $mdc(a, b)$ é o produto dos fatores primos comuns às duas decomposições canônicas tomados cada um com o menor expoente e o $mmc(a, b)$ é o produto dos fatores primos comuns e não comuns às duas decomposições canônicas tomados cada um com o maior expoente. (exercício 13)*
Exemplo: $588 = 2^2.3.7^2$ *e* $936 = 2^3.3^2.13$

$$mdc(588, 936) = 2^2 \cdot 3 = 12 \text{ e } mmc(588, 936) = 2^3 \cdot 3^2 \cdot 7^2 \cdot 13 = 45864$$

3.4 A procura de números primos

Um dos problemas mais antigos de que se tem notícia é a procura de um polinômio que gerasse todos os números primos ou cujos valores fossem somente números primos. Alguns matemáticos da Idade Média acreditavam, por exemplo, que o polinômio $p(x) = x^2 + x + 41$ assumisse valores primos para qualquer número inteiro $x \geqslant 0$. Como já foi visto, este resultado é verdadeiro para $x = 0, 1, ..., 39$ mas $p(40)$ é composto.

Nas diversas tentativas de se obter uma fórmula que gerasse primos, a maioria das afirmações feitas neste sentido revelaram-se erradas, mas esta procura contribuiu de maneira significativa para o desenvolvimento da Teoria dos Números.

Fermat observou que para $n = 0, 1, 2, 3$ e 4 os números $F_n = 2^{2^n} + 1$ eram primos e, a partir daí, conjecturou, em 1640, que para qualquer $n \in \mathbb{N}$, F_n era um número primo. Mas, em 1739, Euler mostrou que F_5 era divisível por 641. Desde então tentou-se descobrir outros números primos de Fermat (nome

dado hoje aos números da forma acima) além dos cinco primeiros. Hoje já se sabe que F_n não é primo para $5 \leqslant n \leqslant 16$, mas ainda não foi provado se o número de primos de Fermat é finito ou não.

Um processo para determinar números primos grandes é através dos números da forma $M_k = 2^k - 1$ que são chamados números primos de Mersenne (1588-1648). Não é difícil provar que se M_k é um número primo, então k é também primo.

Em 1644, Mersenne afirmou o seguinte: "Todo número M_p é primo para $p = 2, 3, 5, 7, 13, 17, 31, 67, 127$ e 257 e é composto para os outros primos p tais que $2 < p < 257$". Observe que $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{13} = 8.191$, $M_17 = 131.071$, $M_{19} = 524.287$, $M_{31} = 2.147.483.647$ e mesmo naquela época tinham dúvidas em relação a esta afirmação pois não existiam processos práticos para verificar, por exemplo, se M_{31} era primo ou não. De fato, para isto necessitava-se de uma tábua de números primos até 46.340 e, no entanto, a maior tábua conhecida por Mersenne só continha primos menores do que 750. Sua conjectura não era correta; ele errou ao incluir os números 67 e 257 e ao excluir os primos 19, 61, 89 e 107.

O maior primo conhecido até Maio de 2013 é $M_{48} = 2^{57885161} - 1$ que possui 17.425.170 (mais de 17 milhões) de dígitos!! (fonte: http://primes.utm.edu e http://www.mersenne.org - acessados em 06/05/2013)

Em 1639, Pierre de Fermat enunciou a seguinte conjectura: "Um número natural $n > 1$ é primo se, e somente se, $2^n - 2$ é divisível por n". Em 1819, Pierre Frédéric Sarrus, matemático francês, descobriu que 341 satisfaz as condições da conjectura e nâo é um número primo ($341 = 11 \times 31$). Mais tarde, outros números, como 15 e 91, foram descobertos. Entretanto uma parte da conjectura é verdadeira e o teorema de Fermat, o qual demonstraremos no Capítulo 5, é uma generalização deste fato: "Se p é primo e $a \in \mathbb{N}$, $a > 1$, então $a^p - a$ é divisível por p".

3.5 Exercícios

1. Ache todos os pares de primos p e q tais que $p - q = 3$.

2. Ache todos os primos que são iguais a um quadrado perfeito menos 1.

3. Ache todos os primos que são iguais a um cubo perfeito menos 1.

   Solução:

   Suponha $p = n^3 - 1$. Temos que $n^3 - 1 = (n-1)(n^2 + n + 1)$. Como p deve ser primo, tevemos ter $n - 1 = 1$ ou $n^2 + n + 1 = 1$. No primeiro caso, temos $n = 2$ e $p = 7$. No segundo caso, temos $n = 0$ ou $n = -1$ e, respectivamente, $p = -1$ e $p = -2$, que não são primos. Assim, o único primo dessa forma é 7.

4. Determine todos os primos p tais que $3p + 1$ é um quadrado perfeito.

5. Determine todos os inteiros positivos n tais que $n, n + 2$ e $n + 4$ são todos primos.

6. Mostre que a soma de dois inteiros positivos ímpares e consecutivos é sempre um inteiro composto.

7. Ache o menor inteiro positivo n pelo qual se deve dividir 3.720 para se obter um quadrado perfeito.

8. Ache todos os primos que são divisores de 50!.

9. Mostre que se $n \in \mathbb{Z}$, $n \neq \pm 1$, $n^2 + 2$ é primo, então $3 \mid n$.

10. Mostre que se $p > 1$ divide $(p-1)! + 1$, então p é primo.

11. Mostre que:

    (a) $\sqrt{2}$ é irracional.

    (b) Se p é primo, então $\sqrt{p}$ é irracional.

12. Sejam a e b inteiros positivos tais que

$$a = p_1^{r_1} p_2^{r_2} ... p_k^{r_k} \text{ e } b = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$$

onde p_i é primo, $r_i, s_i \in \mathbb{Z}+$, para $i = 1, 2, ..., k$ e $p_i \neq p_j$ se $i \neq j$.
Mostre que $b|a \iff s_i \leq r_i$ para todo i.

13. Sejam a e b inteiros positivos tais que

$$a = p_1^{r_1} p_2^{r_2} ... p_k^{r_k} \text{ e } b = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$$

onde p_i é primo, $r_i, s_i \in \mathbb{Z}$, $r_i \geqslant 0$, $s_i \geqslant 0$ para $i = 1, 2, ..., k$ e $p_i \neq p_j$ se $i \neq j$.
Mostre que $\text{mdc}(a, b) = p_1^{t_1} p_2^{t_2} ... p_k^{t_k}$ e $\text{mmc}(a, b) = p_1^{u_1} p_2^{u_2} ... p_k^{u_k}$ onde $t_i = \min\{r_i, s_i\}$ e $u_i = \max\{r_i, s_i\}$, para $i = 1, 2, ..., k$.

14. Sejam $a, b, n \in \mathbb{Z}_+^*$. Prove que se $mdc(a, n) = mdc(b, n) = 1$, então $mdc(ab, n) = 1$. Dica: use o exercício anterior.

15. Demonstre que todo primo, exceto 2 e 3, é da forma $6k - 1$ ou $6k + 1$ onde k é um inteiro positivo.

16. Mostre que todo inteiro da forma $n^4 + 4$, com $n > 1$, é composto.

17. Mostre que todo inteiro da forma $8^n + 1$, com $n \geqslant 1$, é composto.

18. Mostre que existem infinitos primos da forma $6n + 5$.

Capítulo 4

Equações Diofantinas Lineares

4.1 Generalidades

Estamos interessados em procurar soluções inteiras de equações lineares com duas incógnitas, x e y, do tipo $ax + by = c$, onde a, b e c são inteiros dados com $a \neq 0$ e $b \neq 0$. Em $\mathbb{R}$ temos infinitas soluções, pois $ax + by = c$ representa uma reta, daí o nome linear.

Equações onde olhamos para suas soluções em uma classe restrita de números, como os números inteiros, inteiros positivos, inteiros negativos, racionais, etc., são chamadas equações diofantinas. Este nome é devido ao matemático grego Diofanto ($\pm$300 d. C.) por causa do seu interesse em resolver problemas cujas soluções fossem números inteiros ou racionais.

Outros tipos de equações diofantinas:

$$x^2 + y^2 = z^2, \quad x^2 + 2y^2 = 1, \quad x^4 - y^4 = z^4$$

Definição 4.1 *Uma equação diofantina linear é uma expressão da forma $ax + by = c$, na qual a, b e c são inteiros com $ab \neq 0$ e cujas soluções estão restritas aos números inteiros.*

Uma solução dessa equação é um par de inteiros (x_0, y_0) tal que $ax_0 + by_0 = c$.

Exemplo 4.1

a) $2x + 3y = 5$

b) $4x - 2y = 7$

4.2 Condição de existência de solução

Teorema 4.1 *A equação diofantina linear $ax + by = c$ tem solução se, e somente se, $d \mid c$, sendo $d = mdc(a, b)$.*

Prova:

■

4.3 Soluções da equação diofantina linear $ax + by = c$

Teorema 4.2 *Se $d \mid c$, sendo $d = mdc(a, b)$, e se o par de inteiros (x_0, y_0) é uma solução particular da equação diofantina linear $ax + by = c$, então todas as soluções deta equação são dadas pelas fórmulas:*

$$x = x_0 + \left(\frac{b}{d}\right) t$$

$$y = y_0 - \left(\frac{a}{d}\right) t$$

onde t é um inteiro arbitrário.

Prova:

■

Observação 4.1

1. *Podemos concluir que se $d = mdc(a, b)$ e $d \mid c$ então a equação diofantina linear $ax + by = c$ admite um número infinito de soluções, uma para cada valor do inteiro arbitrário t.*

2. *Se $mdc(a, b) = 1$ e se (x_0, y_0) é uma solução da equação diofantina linear $ax + by = c$, então todas as soluções desta equação são dadas pelas fórmulas:*

$$x = x_0 + b.t$$

$$y = y_0 - a.t$$

onde t é um inteiro arbitrário.

3. *Uma solução particular da equação diofantina linear é obtida por tentativas ou pelo algoritmo de Euclides e a solução geral é obtida pelo teorema anterior.*

4.4 Exercícios

1. Determine todas as soluções inteiras da equação diofantina linear $172x + 20y = 1000$.
2. Determine todas as soluções inteiras e positivas da equação diofantina linear $18x + 5y = 48$.
3. Resolva a equação diofantina linear $39x + 26y = 105$.
4. Resolva a equação diofantina linear $14x + 22y = 50$.
5. Encontre a solução geral, caso exista, das seguintes equações diofantinas:
   (a) $56x + 72y = 40$
   (b) $84x - 438y = 156$
   (c) $57x - 99y = 77$
   (d) $17x + 54y = 8$
6. Encontre as soluções inteiras e positivas de:
   (a) $5x - 11y = 29$
   (b) $32x + 55y = 771$
   (c) $62x + 11y = 788$
   (d) $158x - 57y = 7$
7. Encontre as soluções inteiras e negativas de:
   (a) $6x - 15y = 51$
   (b) $6x + 15y = 51$
8. Determine o menor inteiro positivo que dividido por 8 e por 15 deixa restos 6 e 13, respectivamente.
9. Exprima 100 como soma de dois inteiros positivos de modo que o primeiro seja divisível por 7 e o segundo seja divisível por 11.
10. Determine as duas menores frações positivas que tenham 13 e 17 para denominadores e cuja soma seja igual a $\frac{305}{221}$.
11. Demonstre que, se a e b são inteiros positivos primos entre si, então a equação diofantina linear $ax - by = c$ tem um número infinito de soluções inteiras e positivas.

Capítulo 5

Congruências

5.1 Inteiros congruentes

Definição 5.1 *Sejam a e b inteiros quaisquer e seja m um inteiro fixo não nulo. Dizemos que a é congruente a b módulo m se, e somente se, $m \mid a - b$.*

Notação: $a \equiv b \pmod{m}$

Observação 5.1

1. $a \equiv b \,(mod\, m) \Leftrightarrow m \mid a - b \Leftrightarrow \exists k \in \mathbb{Z}$ *tal que* $a - b = km$
2. $a \equiv b \,(mod\, 1)$, *para quaisquer inteiros* a *e* b.
3. $a \equiv 0 \,(mod\, m) \Leftrightarrow m \mid a$.
4. $a \equiv b \,(mod\, m) \Leftrightarrow a \equiv b \,(mod\, -m)$
   Em vista desta observação, podemos, daqui para frente, considerar sempre $m > 0$.
5. *Se* $m \nmid a - b$, *dizemos que* a *é incongruente a* b *módulo* m, *ou* a *não é congruente a* b *módulo* m *e denotamos* $a \not\equiv b \,(mod\, m)$.

Exemplo 5.1

1. $15 \equiv 3 \,(mod\, 4)$, *pois* $15 - 3 = 3.4$
2. $-4 \equiv 2 \,(mod\, 3)$, *pois* $3 \mid (-4 - 2)$.
3. $-30 \not\equiv 4 \,(mod\, 5)$, *pois* $5 \nmid (-30 - 4)$.
4. *Mostre que se* $n \equiv 7 \,(mod\, 12)$, *então* $n \equiv 3 \,(mod\, 4)$, $\forall n \in \mathbb{Z}$.
5. *Mostre que se* $n \in \mathbb{Z}$, *então* $n^2 \equiv 0 \,(mod\, 4)$ *ou* $n^2 \equiv 1 \,(mod\, 4)$.

5.2 Caracterização de inteiros congruentes

Proposição 5.1 *Dois inteiros* a *e* b *são congruentes módulo* m *se, e somente se,* a *e* b *deixam o mesmo resto quando divididos por* m

Prova:

■

Exemplo 5.2

1. $-56 = 9(-7) + 7$ *e* $-11 = 9(-2) + 7$*; logo* $-56 \equiv -11 \ (mod\, 9)$.
2. $-31 \equiv 11 \ (mod\ 7)$*; logo* -31 *e* 11 *deixam o mesmo resto quando divididos por* 7*. Realmente:* $-31 = 7(-5) + 4$ *e* $11 = 7(1) + 4$.

5.3 Propriedades

Proposição 5.2 *Seja* m *um inteiro positivo fixo* $(m > 0)$ *e sejam* a, b, c, d *e* k *inteiros quaisquer, com* $k > 0$*. Então temos:*

1. $a \equiv a \ (mod\, m)$ *(Reflexiva)*
2. $a \equiv b \ (mod\, m) \Rightarrow b \equiv a \ (mod\, m)$ *(Simétrica)*
3. $a \equiv b \ (mod\, m)$ *e* $b \equiv c \ (mod\, m) \Rightarrow a \equiv c \ (mod\, m)$ *(Transitiva)*
4. $a \equiv b \ (mod\, m)$ *e* $k \mid m \Rightarrow a \equiv b \ (mod\, k)$
5. $a \equiv b \ (mod\, m) \Rightarrow ak \equiv bk \ (mod\, mk)$
6. $a \equiv b \ (mod\, m)$ *e* a, b, m *são divisíveis por* $k \Rightarrow \dfrac{a}{k} \equiv \dfrac{b}{k} \ (mod\, \dfrac{m}{k})$
7. $a \equiv b \ (mod\, m)$ *e* $c \equiv d \ (mod\, m) \Rightarrow a + c \equiv b + d \ (mod\, m)$
8. $a \equiv b \ (mod\, m)$ *e* $c \equiv d \ (mod\, m) \Rightarrow ac \equiv bd \ (mod\, m)$
9. $a \equiv b \ (mod\, m) \Rightarrow a + c \equiv b + c \ (mod\, m)$
10. $a \equiv b \ (mod\, m) \Rightarrow ac \equiv bc \ (mod\, m)$
11. $a \equiv b \ (mod\, m) \Rightarrow a^n \equiv b^n \ (mod\, m)$, $\forall n \in \{1, 2, 3, ...\}$

Prova:

■

Observação 5.2

1. *A relação R no conjunto $\mathbb{Z}$ definida por $a\ R\ b \Leftrightarrow a \equiv b\ (mod\ m)$ é reflexiva, simétrica e transitiva, ou seja, R é uma relação de equivalência em $\mathbb{Z}$. Esta relação de equivalência R em $\mathbb{Z}$ é denominada "congruência módulo m".*

2. *A notação $a \equiv b\ (mod\ m)$ introduzida por Gauss e convenientemente semelhante à igualdade, como vimos, satisfaz várias regras da álgebra elementar. Uma regra que é válida para a igualdade, mas que não é válida para a congruência módulo m é a do cancelamento:*
   Se $ac \equiv bc\ (mod\ m)$ e $c \neq 0$ não é necessariamente verdade que $a \equiv b\ (mod\ m)$.
   De fato, $4.3 \equiv 8.3\ (mod\ 12)$ mas $4 \not\equiv 8\ (mod\ 12)$.
   A proposição a seguir nos garante em que condições a lei do cancelamento pode ser utilizada.

Proposição 5.3 *Se* $ac \equiv bc \pmod{m}$ *e se* $mdc(c, m) = 1$*, então* $a \equiv b \pmod{m}$*.*

Prova:

■

Corolário 5.1 *Se* $ac \equiv bc \pmod{m}$ *e se* $mdc(c, m) = d$*, então* $a \equiv b \pmod{\frac{m}{d}}$*.*

Prova:

■

Corolário 5.2 *Se* $ac \equiv bc \pmod{p}$*,* p *primo, e se* $p \nmid c$*, então* $a \equiv b \pmod{p}$*.*

Prova:

■

5.4 Sistema completo de restos

Definição 5.2 *Seja* m *um inteiro positivo fixo. Chama-se sistema completo de restos módulo* m *(SCR mod* m*) todo conjunto* $S = \{r_1, r_2, ..., r_m\}$ *de* m *inteiros tal que um inteiro qualquer* a *é congruente módulo* m *a um único elemento de* S*.*

Proposição 5.4 *O conjunto* $S = \{0, 1, 2, ..., m-1\}$ *é um sistema completo de restos módulo* m *(ou SCR mod* m*)*

Prova:

Queremos mostrar que todo inteiro a é congruente módulo m a exatamente um dos valores $0, 1, 2, ..., m-1$.

Seja $a \in \mathbb{Z}$. Pelo algoritmo da divisão de a por m, existem únicos inteiros q e r tais que $a = mq + r$ com $0 \leqslant r \leqslant m-1$. Logo, $a - r = mq$ e $a \equiv r \pmod{m}$. Pela unicidade de r, obtemos o resultado. ■

Corolário 5.3 *$S' = \{r_1, r_2, ..., r_m\} \subset \mathbb{Z}$ é um SCR mod m se, e somente se, cada elemento de $S = \{0, 1, 2, \ldots, m-1\}$ é congruente módulo m a um único elemento de S'.*

Prova:
($\Rightarrow$) Seja $s \in S$. Então $s \equiv r \pmod{m}$ para um único $r \in S'$, pois S' é um SCR mod m por hipótese.
($\Leftarrow$) Seja $a \in \mathbb{Z}$. Então $a \equiv k \pmod{m}$ para um único $k \in S$, pois S é um SCR mod m pela proposição anterior. Por hipótese existe um único $r \in S'$ tal que $k \equiv r \pmod{m}$; logo existe um único $r \in S'$ tal que $a \equiv r \pmod{m}$. Portanto S' é um SCR mod m. ■

Exemplo 5.3 *$S = \{-12, -4, 11, 13, 22, 82, 91\}$ é um SCR mod 7, pois*
$0 \equiv 91 \ (mod\ 7)$, $1 \equiv 22 \ (mod\ 7)$, $2 \equiv -12 \ (mod\ 7)$, $3 \equiv -4 \ (mod\ 7)$, $4 \equiv 11 \ (mod\ 7)$, $5 \equiv 82 \ (mod\ 7)$ *e* $6 \equiv 13 \ (mod\ 7)$.

5.5 Exercícios

1. Mostre que se $a \equiv b \pmod{m}$, então $-a \equiv -b \pmod{m}$.
2. Mostre que se $a + b \equiv c \pmod{m}$, então $a \equiv c - b \pmod{m}$.
3. Sabendo que $1066 \equiv 1776 \pmod{m}$, ache todos os possíveis valores de m.
4. Reescreva a expressão "n é ímpar" de três outras maneiras.
5. Ache todos os inteiros x tais que $0 \leqslant x \leqslant 15$ e $3x \equiv 6 \pmod{15}$.
6. Ache todos os inteiros x tais que $1 \leqslant x \leqslant 100$ e $x \equiv 7 \pmod{17}$.
7. Sabendo que $k \equiv 1 \pmod{4}$, mostre que $6k + 5 \equiv 3 \pmod{4}$.
8. Mostre, mediante um exemplo, que $a^2 \equiv b^2 \pmod{m}$ não implica $a \equiv b \pmod{m}$.
9. Mostre que todo primo (exceto 2) é congruente módulo 4 a 1 ou 3.
10. Mostre que todo primo (exceto 2 e 3) é congruente módulo 6 a 1 ou 5.
11. Mostre que $11^{10} \equiv 1 \pmod{100}$.
12. Mostre que 41 divide $2^{20} - 1$.
13. Ache os restos das divisões de 2^{50} e 41^{65} por 7.
14. Mostre:
    (a) $89 \mid (2^{44} - 1)$
    (b) $97 \mid (2^{48} - 1)$
15. Demonstre que se $a \equiv b \pmod{m}$, então $\text{mdc}(a, m) = \text{mdc}(b, m)$.
16. Mostre, mediante um exemplo, que $a^k \equiv b^k \pmod{m}$ e $k \equiv j \pmod{m}$ não implica $a^j \equiv b^j \pmod{m}$.
17. Demonstre as seguintes proposições:
    (a) Se a é um inteiro ímpar, então $a^2 \equiv 1 \pmod{8}$
    (b) Se a é um inteiro qualquer, então a^3 é congruente a 0 ou 1 ou 8 módulo 9.
    (c) Se a é um inteiro qualquer, então $a^3 \equiv a \pmod{6}$.
18. Mostre que se $a \equiv b \pmod{r}$ e $a \equiv b \pmod{s}$, então $a \equiv b \pmod{m}$, onde $m = \text{mmc}(r, s)$.

5.6 Classes residuais

5.6.1 Revisão

Sejam A e B dois conjuntos não vazios.
Uma relação de A em B é qualquer subconjunto do produto cartesiano $A \times B$.
Uma relação sobre A é uma relação de A em A.
Uma relação de equivalência R sobre A é uma relação sobre A que satisfaz as seguintes propriedades:

1. Reflexiva: $(\forall x \in A)\ (x\ R\ x)$
2. Simétrica: $(\forall x \in A)(\forall y \in A)\ (x\ R\ y \to y\ R\ x)$
3. Transitiva: $(\forall x \in A)(\forall y \in A)(\forall z \in A)\ (x\ R\ y \text{ e } y\ R\ z \to x\ R\ z)$

Se R é uma relação de equivalência sobre A e $a \in A$ definimos:
$\text{Cl}(a) = \overline{a} = \{x \in A : x\ R\ a\}$ (classe de equivalência de $a \in A$ pela relação de equivalência R)
$A/R = \{\overline{a} : a \in A\}$ (conjunto quociente de A pela relação de equivalência R)

5.6.2 Definição e propriedades

Definição 5.3 *Seja m um inteiro positivo fixo. Se a é um inteiro qualquer então a classe residual módulo m de a, denotada por $\overline{a}$ (ou $[a]_m$ ou a_m), consiste do conjunto formado por todos os inteiros que são congruentes ao inteiro a módulo m, isto é,*

$$\overline{a} = \{x \in \mathbb{Z} : x \equiv a\ (mod\, m)\} = \{x \in \mathbb{Z} : m \mid x - a\} = \{a + km : k \in \mathbb{Z}\}.$$

Observação 5.3

1. *A notação $\overline{a}$ deve ser usada somente quando ficar claro, pelo contexto, o valor do inteiro m utilizado, do contrário a notação $[a]_m$ é a mais indicada.*
2. *A classe residual de um inteiro é a classe de equivalência deste inteiro pela relação de congruência (que é uma relação de equivalência como visto anteriormente).*
3. *Se $m = 1$ e $a \in \mathbb{Z}$ temos $\overline{a} = \{x \in \mathbb{Z} : 1 \mid x - a\} = \mathbb{Z}$.*
4. *As classes residuais módulo m também são denominadas inteiros módulo m ou classes de restos módulo m ou classes de congruência módulo m.*
5. *Se $a \in \mathbb{Z}$, então $\overline{a} \neq \varnothing$, pois como $a \equiv a\ (mod\, m)$ temos que $a \in \overline{a}$.*

Exemplo 5.4 *Seja $m = 12$. Temos:*

- $\overline{3} = \{x \in \mathbb{Z} : x \equiv 3\ (mod\, 12)\} = \{x \in \mathbb{Z} : 12 \mid x - 3\} = \{x \in \mathbb{Z} : x = 12k + 3,\ \text{para algum } k \in \mathbb{Z}\} = \{..., -21, -9, 3, 15, ...\}$
- $\overline{15} = \{x \in \mathbb{Z} : x \equiv 15\ (mod\, 12)\}$
  Como $15 \equiv 3\ (mod\, 12)$ *então* $x \equiv 15\ (mod\, 12)$ *se, e somente se,* $x \equiv 3\ (mod\, 12)$.
  Logo, $\overline{15} = \{x \in \mathbb{Z} : x \equiv 3\ (mod\, 12)\} = \overline{3}$

Proposição 5.5 *Seja m um inteiro positivo fixo e sejam $\overline{a}$ e $\overline{b}$ as classes residuais módulo m de dois inteiros quaisquer a e b. Então:*

1. $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \,(mod\, m)$
2. $\overline{a} \cap \overline{b} = \emptyset$ *ou* $\overline{a} = \overline{b}$

Prova:

■

Observação 5.4 *A classe residual $\overline{a}$ diz-se determinada ou definida pelo inteiro a, o qual chama-se um representante de $\overline{a}$. Pelo resultado anterior, dois inteiros são representantes de uma mesma classe residual módulo m ($\overline{a} = \overline{b}$) se, e somente se, são congruentes módulo m ($a \equiv b \,(mod\, m)$).*

5.6.3 O conjunto das classes residuais

O conjunto formado por todas as classes residuais módulo m, ou seja, $\{\overline{a} : a \in \mathbb{Z}\}$ é indicado por $\mathbb{Z}_m$ (ou $\mathbb{Z}/m\mathbb{Z}$).

Observação 5.5

1. *A notação $\mathbb{Z}_m$, comumente usada no Brasil, é também utilizada para denotar o conjunto dos inteiros p-ádicos estudados em Teoria Analítica dos Números. Como no nosso curso não trataremos de inteiros p-ádicos usaremos a notação acima para o conjunto das classes residuais módulo m.*
2. *Se $m = 1$, então $\overline{a} = \mathbb{Z}$, $\forall a \in \mathbb{Z}$; logo $\mathbb{Z}_1 = \{\mathbb{Z}\}$.*
3. *$\mathbb{Z}_m$ é o conjunto quociente de $\mathbb{Z}$ pela relação de equivalência congruência módulo m.*

Proposição 5.6 *O conjunto $\mathbb{Z}_m$ tem exatamente m elementos.*

Prova:
Vamos mostrar que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ e que $\{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ tem exatamente m elementos.
1) É claro que $\{\overline{0}, \overline{1}, ..., \overline{m-1}\} \subset \mathbb{Z}_m$.

2) Seja $\overline{a} \in \mathbb{Z}_m$, onde $a \in \mathbb{Z}$. Pelo algoritmo da divisão de a por m, existem inteiros q e r tais que $a = mq + r$, $0 \leqslant r \leqslant m-1$. Assim $a - r = mq$, donde $m \mid a - r$. Logo $a \equiv r \pmod{m}$ e, pela proposição anterior, temos $\overline{a} = \overline{r}$. Como $0 \leqslant r \leqslant m-1$ então $\overline{a} = \overline{r} \in \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$. Portanto, $\mathbb{Z}_m \subset \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$.
De 1) e 2) concluímos que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$.

3) Suponha que $\overline{r} = \overline{s}$, onde $r, s \in \mathbb{Z}$ tais que $0 \leqslant r < s \leqslant m-1$. Pela proposição anterior temos que $r \equiv s \pmod{m}$. Assim $s \equiv r \pmod{m}$ e $m \mid s - r$. Mas isto é um absurdo, pois $0 < s - r < m$. Portanto $\{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ tem exatamente m elementos. ∎

Observação 5.6

1. *$\mathbb{Z}_m$ é um conjunto finito embora $\mathbb{Z}$ seja um conjunto infinito.*
2. *Para achar a classe residual módulo m de um inteiro qualquer y, basta determinar o resto r da divisão de y por m, pois $\overline{y} = \overline{r}$ com $0 \leqslant r \leqslant m-1$*
3. *As classes residuais $\overline{0}, \overline{1}, ..., \overline{m-1}$ que formam o conjunto $\mathbb{Z}_m$ são subconjuntos não vazios de $\mathbb{Z}$, disjuntos dois a dois e sua reunião é o conjunto $\mathbb{Z}$. Logo, $\mathbb{Z}_m$ é uma partição de $\mathbb{Z}$.*
4. *O conjunto de m representantes, um de cada uma das classes residuais $\overline{0}, \overline{1}, ..., \overline{m-1}$, é um sistema completo de restos módulo m.*
5. *A imagem geométrica correspondente a $\mathbb{Z}_m$ é de uma circunferência onde estão marcados m pontos equidistantes. Cada ponto corresponde a uma das classes de equivalência de $\mathbb{Z}_m$.*
   (Enrolamos $\mathbb{Z}$, na reta, em uma circunferência.
   Colamos o ponto m ao ponto 0.
   Como a reta é infinita, continuamos a enrolá-la na circunferência)

Exemplo 5.5 1. *Qual é a classe residual módulo 8 de 75?*
Temos que $75 = 8 \cdot 9 + 3$, donde $75 \equiv 3 \pmod{8}$ e, então, $\overline{75} = \overline{3} = \{3 + 8k : k \in \mathbb{Z}\}$.

2. *$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, onde*
$$\overline{0} = \{2k : k \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$
$$\overline{1} = \{2k+1 : k \in \mathbb{Z}\} = \{\ldots, -3, -1, 0, 1, 3, \ldots\}$$
Observe que $\overline{0} \cap \overline{1} = \emptyset$ e $\overline{0} \cup \overline{1} = \mathbb{Z}$.

3. *$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, onde*
$$\overline{0} = \{5k : k \in \mathbb{Z}\}$$
$$\overline{1} = \{5k+1 : k \in \mathbb{Z}\}$$
$$\overline{2} = \{5k+2 : k \in \mathbb{Z}\}$$
$$\overline{3} = \{5k+3 : k \in \mathbb{Z}\}$$
$$\overline{4} = \{5k+4 : k \in \mathbb{Z}\}$$
Essas classes são duas a duas disjuntas e sua reunião é o conjunto $\mathbb{Z}$.

5.6.4 Exercícios

1. *Achar a classe residual módulo 8 de -5.*
2. *Achar a classe residual módeulo 9 de 1913.*
3. *O inteiro 17 pertence à classe residual módulo m de 24. Determinar m.*
4. *Os inteiros 29 e 41 pertencem a uma mesma classe residual módulo m. Determinar m.*
5. *Mostrar que*

   (a) $[10]_3 = [1]_3$
   (b) $[84]_{19} = [8]_{19}$.
   (c) $[-8]_7 = [20]_7$.

5.6.5 Adição e Multiplicação em $\mathbb{Z}_m$

Seja m um inteiro positivo fixo.
Vamos definir as operações de adição e multiplicação no conjunto $\mathbb{Z}_m$ das classes residuais módulo m.
Sejam $\overline{a}, \overline{x}, \overline{b}, \overline{y} \in \mathbb{Z}_m$.
Temos que se $\overline{a} = \overline{x}$ e $\overline{b} = \overline{y}$, então $a \equiv x \pmod{m}$ e $b \equiv y \pmod{m}$; logo $a + b \equiv x + y \pmod{m}$ e $ab \equiv xy \pmod{m}$ e, consequentemente, $\overline{a+b} = \overline{x+y}$ e $\overline{ab} = \overline{xy}$.
Isto torna lícitas as seguintes definições:

Definição 5.4

1. *Dadas duas classes $\overline{a}, \overline{b} \in \mathbb{Z}_m$, chama-se soma $\overline{a} + \overline{b}$ a classe $\overline{a+b}$ (que é única, independentemente do representante tomado para $\overline{a}$ ou para $\overline{b}$).*

$$\begin{array}{rccc} + : & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} + \overline{b} = \overline{a+b} \end{array}$$

2. *Dadas duas classes $\overline{a}, \overline{b} \in \mathbb{Z}_m$, chama-se produto $\overline{a}.\overline{b}$ a classe $\overline{ab}$ (que é única, independentemente do representante tomado para $\overline{a}$ ou para $\overline{b}$).*

$$\begin{array}{rccc} . : & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a}.\overline{b} = \overline{ab} \end{array}$$

Proposição 5.7 *Sejam $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.*

1. ***Associatividade da soma:*** $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
2. ***Comutatividade da soma:*** $\overline{a} + \overline{b} = \overline{b} + \overline{a}$
3. ***Elemento neutro para a soma:*** $\overline{a} + \overline{0} = \overline{a}$
4. ***Elemento simétrico para a soma:*** $\overline{a} + \overline{m-a} = \overline{0}$
5. ***Associatividade do produto:*** $(\overline{a}.\overline{b}).\overline{c} = \overline{a}.(\overline{b}.\overline{c})$
6. ***Comutatividade do produto:*** $\overline{a}.\overline{b} = \overline{b}.\overline{a}$
7. ***Elemento neutro para o produto:*** $\overline{a}.\overline{1} = \overline{a}$
8. ***Distributividade da multiplicação em relação à adição:*** $\overline{a}.(\overline{b} + \overline{c}) = \overline{a}.\overline{b} + \overline{a}.\overline{c}$

Prova:

■

Proposição 5.8 *$\overline{a} \in \mathbb{Z}_m$ é simetrizável para a multiplicação, isto é, admite inverso multiplicativo se, e somente se, $mdc(a, m) = 1$*

Prova:
($\Rightarrow$) $\overline{a} \in \mathbb{Z}_m$ admite inverso multiplicativo $\Rightarrow \exists \overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}.\overline{b} = \overline{1} \Rightarrow \overline{ab} = \overline{1} \Rightarrow ab \equiv 1 \pmod{m} \Rightarrow$
$\Rightarrow m \mid ab - 1 \Rightarrow \exists q \in \mathbb{Z}$ tal que $ab - 1 = mq \Rightarrow ab - mq = 1 \Rightarrow ab + m(-q) = 1 \Rightarrow \text{mdc}(a, m) = 1$.
($\Leftarrow$) $\text{mdc}(a, m) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ tal que $ax + my = 1 \Rightarrow ax - 1 = m(-y) \Rightarrow m \mid ax - 1 \Rightarrow$
$\Rightarrow ax \equiv 1 \pmod{m} \Rightarrow \overline{ax} = \overline{1} \Rightarrow \overline{a}.\overline{x} = \overline{1} \Rightarrow \overline{a}$ admite inverso multiplicativo. ■

Observação 5.7 *O conjunto dos elementos de $\mathbb{Z}_m$ que têm inverso multiplicativo será denotado por $\mathcal{U}(m)$, isto é, $\mathcal{U}(m) = \{\overline{a} \in \mathbb{Z}_m : mdc(a, m) = 1\}$.*
Exemplos: Para p primo temos $\mathcal{U}(p) = \{\overline{a} \in \mathbb{Z}_p : mdc(a, p) = 1\} = \mathbb{Z}_p - \{\overline{0}\}$
$\mathcal{U}(4) = \{\overline{1}, \overline{3}\}$
$\mathcal{U}(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

5.6.6 Exercícios

1. Construa as tabelas de adição de $\mathbb{Z}_4$ e $\mathbb{Z}_5$.
2. Construa as tabelas de multiplicação para $\mathbb{Z}_4$ e $\mathbb{Z}_5$.
3. Determine todos os elementos inversíveis de $\mathbb{Z}_9$ e encontre os seus respectivos inversos multiplicativos.

5.7 Congruências lineares

5.7.1 Definição e condição de existência

Definição 5.5 *Chama-se congruência linear toda equação da forma $ax \equiv b \ (mod\, m)$, onde $a, b, m \in \mathbb{Z}$, $m > 0$.*

Todo inteiro x_0 tal que $ax_0 \equiv b \,(mod\, m)$ diz-se uma solução da congruência linear $ax \equiv b \,(mod\, m)$.

Observação 5.8

1. $ax_0 \equiv b \,(mod\, m) \Leftrightarrow m \mid (ax_0 - b) \Leftrightarrow \exists y_0 \in \mathbb{Z}$ *tal que* $ax_0 - b = my_0 \Leftrightarrow ax_0 - my_0 = b$.
   Isto mostra que o problema de achar todos os inteiros que satisfaçam a congruência linear $ax \equiv b \,(mod\, m)$ reduz-se ao de obter todas as soluções da equação diofantina linear $ax - my = b$.

2. *Se x_0 é solução de $ax \equiv b \,(mod\, m)$ então todos os inteiros da forma $x_0 + km$, com $k \in \mathbb{Z}$, são também soluções desta congruência linear. Note que tais soluções são mutuamente congruentes módulo m.*
   Por exemplo, na congruência linear $3x \equiv 9 \;(mod\; 12)$ temos que $x_0 = 3$ é solução pois $3.3 \equiv 9 \;(mod\; 12)$; assim todos os inteiros da forma $3 + 12k$, com $k \in \mathbb{Z}$, são soluções de $3x \equiv 9 \,(mod\, 12)$.

3. *Duas soluções quaisquer, x_0 e x_1, de $ax \equiv b \;(mod\; m)$ que são congruentes módulo m ($x_0 \equiv x_1 \;(mod\; m)$) não são consideradas soluções distintas, isto é, o número de soluções de $ax \equiv b \,(mod\, m)$ é dado pelo número de soluções mutuamente não congruentes módulo m que a satisfazem.*
   Por exemplo, 3 e -9 são soluções de $3x \equiv 9 \,(mod\, 12)$, porém, como $3 \equiv -9 \,(mod\, 12)$, estas não são consideradas soluções diferentes para a congruência linear $3x \equiv 9 \,(mod\, 12)$.

Teorema 5.1 *A congruência linear $ax \equiv b \;(mod\; m)$ tem solução se, e somente se, $d \mid b$, onde $d = mdc(a, m)$.*

Prova:

■

5.7.2 Soluções da congruência linear $ax \equiv b$ (mod m)

Teorema 5.2 *Se $d \mid b$, onde $d = mdc(a, m)$, então a congruência linear $ax \equiv b \,(mod\, m)$ tem exatamente d soluções mutuamente não congruentes módulo m.*

Prova:

Sabemos que a congruência linear $ax \equiv b \pmod{m}$ **(I)** é equivalente à equação diofantina $ax - my = b$ **(II)**.

Se $d \mid b$, então $ax \equiv b \pmod{m}$ tem uma solução $x_0 \in \mathbb{Z}$. Assim existe $y_0 \in \mathbb{Z}$ tal que (x_0, y_0) é uma solução particular da equação diofantina **(II)** e todas as suas soluções são dadas pelas fórmulas:

$$x = x_0 + \frac{m}{d}t \quad \text{e} \quad y = y_0 + \frac{a}{d}t, \quad t \in \mathbb{Z}$$

.

Em $x = x_0 + \frac{m}{d}t,\ t \in \mathbb{Z}$, atribua a t os valores $0, 1, 2, ..., d-1$, isto é, considere as seguintes d soluções de **(I)**:

$$x_0,\ \ x_0 + \frac{m}{d},\ \ x_0 + 2\frac{m}{d},\ \ ...,\ \ x_0 + (d-1)\frac{m}{d}$$

Vamos mostrar que estas d soluções de **(I)** são mutuamente não congruentes módulo m e que qualquer outra solução de **(I)** é congruente módulo m a algum desses d inteiros.

Suponhamos que $x_0+\frac{m}{d}t_1 \equiv x_0+\frac{m}{d}t_2 \pmod{m}$, onde $0 \leq t_1 < t_2 \leq d-1$. Então $\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod{m}$ e como $\text{mdc}\left(\frac{m}{d}, m\right) = \frac{m}{d}$ temos que $t_1 \equiv t_2 \pmod{d}$. Isto significa que $d \mid t_2 - t_1$ e $0 < t_2 - t_1 < d$, o que é um absurdo. Portanto as d soluções de **(I)**, enumeradas acima, são mutuamente não congruentes módulo m.

Seja $x_1 \in \mathbb{Z}$, solução de **(I)**. Então $\exists y_1 \in \mathbb{Z}$ tal que (x_1, y_1) é solução de $ax-my = b$. Logo $x_1 = x_0+\frac{m}{d}t$, para algum $t \in \mathbb{Z}$. Pelo algoritmo da divisão de t por d, existem inteiros q e r tais que $t = dq + r$, onde $0 \leq r \leq d-1$. Assim temos:

$$x_1 = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(dq + r) = x_0 + mq = \frac{m}{d}r$$

donde segue que:

$$x_1 - \left(x_0 + \frac{m}{d}r\right) = mq \Rightarrow x_1 \equiv x_0 + \frac{m}{d}r \pmod{m}$$

sendo $x_0 + \frac{m}{d}r$ um dos d inteiros enumerados acima. ∎

Observação 5.9 *Pela demonstração do teorema anterior concluímos que se x_0 é uma solução qualquer de $ax \equiv b\ (mod\ m)$, então as suas $d = mdc(a, m)$ soluções mutuamente não congruentes módulo m são os inteiros:*

$$x_0,\ \ x_0 + \frac{m}{d},\ \ x_0 + 2\frac{m}{d},\ \ ...,\ \ x_0 + (d-1)\frac{m}{d}$$

Corolário 5.4 *Se $mdc(a, m) = 1$, então a congruência linear $ax \equiv b\ (mod\ m)$ tem uma "única" solução.*

Exemplo 5.6 *Resolver as seguintes congruências lineares:*

(a) $18x \equiv 30\ (mod\ 42)$

(b) $11x \equiv 2\ (mod\ 317)$

(c) $35x \equiv 5\ (mod\ 14)$

(d) $64x \equiv 16\ (mod\ 84)$

5.8 Resolução de equações diofantinas lineares por congruência

Sabemos que a equação diofantina linear $ax + by = c$ **(I)** tem solução se, e somente se, $d \mid c$, onde $d = \text{mdc}(a, b)$.

Se (x_0, y_0) é uma solução particular desta equação, então $ax_0 + by_0 = c$, o que é equivalente a $ax_0 \equiv c \pmod{b}$.

Portanto para obter uma solução particular de **(I)** basta determinar uma solução x_0 da congruência linear $ax \equiv c \pmod{b}$ e substituir este valor x_0 de x em **(I)**, a fim de encontrar o valor correspondente y_0 de y, isto é, $ax_0 + by_0 = c$.

Observação 5.10 *Do mesmo modo pode-se obter uma solução particular de **(I)** determinando uma solução qualquer y_0 da congruência linear $by \equiv c\ (mod\ a)$.*

Exemplo 5.7 *Resolver as seguintes equações diofantinas por congruência:*

(a) $48x + 7y = 17$

(b) $9x + 16y = 35$

5.9 Inverso de um inteiro módulo m

Seja $a \in \mathbb{Z}$. Chama-se inverso de a módulo m todo inteiro a^* tal que $a.a^* \equiv 1 \pmod{m}$.

Observação 5.11

1. *Nem todo inteiro tem inverso módulo m. Por exemplo, 2 não tem inverso módulo 4, pois $2x \equiv 1 \ (mod\, 4)$ não tem solução.*
2. *Se $a^* \in \mathbb{Z}$ é inverso de a módulo m, então $a' \in \mathbb{Z}$ tal que $a' \equiv a^* \ (mod\, m)$ é também inverso de a módulo m e na contagem é considerado como um inverso apenas.*
3. *$a \in \mathbb{Z}$ tem inverso módulo m se, e somente se, $mdc(a.m) = 1$.*
4. *Se $mdc(a, m) = 1$, então a tem um "único" inverso módulo m.*

Exemplo 5.8

1. *Ache o inverso de 5 módulo 8.*
2. *Ache o inverso de 2 módulo 5.*

5.10 Teoremas de Fermat e de Wilson

Teorema 5.3 ("pequeno teorema de Fermat")
Se p é um número primo e $p \nmid a$, então $a^{p-1} \equiv 1 \ (mod\, p)$.

Prova:
Considere os seguintes $p-1$ múltiplos de a: $a, 2a, 3a, ..., (p-1)a$.

Afirmação 1: $p \nmid ra$, $\forall r \in \{1, 2, 3, ..., p-1\}$.
De fato, se $p \mid ra$ para algum $r \in \{1, 2, 3, ..., p-1\}$, então $p \mid r$ ou $p \mid a$, pois p é primo. Mas $p \nmid r$, pois $0 < r < p$, e $p \nmid a$ por hipótese. Assim $p \nmid ra$, $\forall r \in \{1, 2, 3, ..., p-1\}$, e $ra \not\equiv 0 \pmod{p}$, $\forall r \in \{1, 2, 3, ..., p-1\}$.

Afirmação 2: $ra \not\equiv sa \pmod{p}$, para $r, s \in \{1, 2, ..., p-1\}$ e $r \neq s$.
Com efeito, suponha que $ra \equiv sa \pmod{p}$, $1 \leq r < s \leq p-1$. Então $r \equiv s \pmod{p}$, pois $\text{mdc}(a, p) = 1$. Assim $s \equiv r \pmod{p}$ e segue que $s - r$ é um múltiplo de p. Mas isto é um absurdo pois $0 < s - r < p$.

Das afirmações anteriores concluímos que cada um dos inteiros $a, 2a, 3a, ..., (p-1)a$ é congruente módulo p a um único inteiro da sequência $1, 2, 3, ..., p-1$ considerados numa certa ordem.
Assim, temos:

$$a.2a.3a...(p-1)a \equiv 1.2.3...(p-1) \pmod{p}$$

ou seja,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

pois $\text{mdc}(p, (p-1)!) = 1$. ■

Observação 5.12 *Se p é primo e $p \mid a$ não é verdade que $a^{p-1} \equiv 1 \ (mod\, p)$. Por exemplo, fazendo $p = 2$ e $a = 4$, é fácil ver que $2 \mid 4$ e $4^{2-1} \not\equiv 1 \ (mod\, 2)$.*

Corolário 5.5 *Se p é um número primo, então $a^p \equiv a \ (mod\, p)$, qualquer que seja o inteiro a.*

Prova:

■

Teorema 5.4 *Seja $a \in \mathbb{Z}$. Se p e q são primos distintos tais que $a^p \equiv a \ (mod\, q)$ e $a^q \equiv a \ (mod\, p)$, então $a^{pq} \equiv a \ (mod\, pq)$.*

Prova:

■

Lema 5.1 *Seja p um número primo. Então $a^2 \equiv 1 \ (mod\, p)$ implica $a \equiv 1 \ (mod\, p)$ ou $a \equiv p-1 \ (mod\, p)$. Ou seja, os únicos elementos de $\mathbb{Z}_p$ que são iguais ao seu inverso são 1 e $p-1$.*

Prova:

■

Teorema 5.5 (Wilson) *Se p é um número primo, então $(p-1)! \equiv -1 \ (mod\, p)$.*

Prova:
O teorema é verdadeira para $p = 2$ e $p = 3$, pois:

$$(2-1)! = 1! = 1 \equiv -1 \ (\text{mod } 2)$$

$$(3-1)! = 2! = 2 \equiv -1 \pmod 3$$

de modo que vamos supor $p \geq 5$.

Pelo lema anterior os únicos elementos que são iguais ao seu inverso são 1 e $p-1$ e como em $\mathbb{Z}_p$ todos os elementos não nulos são inversíveis temos que:

$$2.3...(p-2) \equiv 1 \pmod p$$

Desta forma temos:

$$2.3...(p-2)(p-1) \equiv (p-1) \pmod p$$

e, portanto,

$$(p-1)! \equiv -1 \pmod p$$

■

Teorema 5.6 (Recíproco do teorema de Wilson) *Seja $n \in \mathbb{Z}$, $n > 1$. Se $(n-1)! \equiv -1$ $(mod\ n)$, então n é primo.*

Prova:

Suponha que n seja composto. Então n tem um divisor d tal que $1 < d < n$. Como $1 < d \leq n-1$, então d é um dos fatores de $(n-1)!$ e, portanto, $d \mid (n-1)!$.

Por hipótese $n \mid (n-1)!+1$ e como $d \mid n$ temos $d \mid (n-1)!+1$.

Como $d \mid (n-1)!+1$ e $d \mid (n-1)!$, então $d \mid 1$. Logo $d = \pm 1$, o que contradiz o fato de $d > 1$. Portanto n é primo. ■

Observação 5.13 *O teorema de Wilson e seu recíproco dão um critério para reconhecer se um dado inteiro é primo: "Um inteiro $n > 1$ é primo se, e somente se, $(n-1)! \equiv -1$ $(mod\, n)$."*

Note que para inteiros grandes este critério é impraticável.

5.11 Critérios de divisibilidade usando congruências

Lema 5.2 *Se $a \equiv b$ $(mod\ m)$ e se $P(x) = \sum_{k=0}^{n} c_k x^k = c_0 + c_1 x + c_2 x^2 + ... + c_n x^n$ é um polinômio em x com coeficientes c_k inteiros, então $P(a) \equiv P(b)$ $(mod\, m)$.*

Prova:

Temos:

$a \equiv b \pmod m \Rightarrow a^k \equiv b^k \pmod m$, $\forall k \in \{0,1,2,...,n\} \Rightarrow c_k a^k \equiv c_k b^k \pmod m$, $\forall k \in \{0,1,2,...,n\} \Rightarrow \sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \pmod m \Rightarrow P(a) \equiv P(b) \pmod m$. ■

Proposição 5.9 (Critério de divisibilidade por 2) *Um inteiro positivo n é divisível por 2 se, e somente se, o algarismo das unidades for divisível por 2*

Prova:

Seja $n = a_m a_{m-1}...a_1 a_0$ a representação de n na base 10 e considere o polinômio na variável x com coeficientes inteiros: $P(x) = \sum_{k=0}^{m} a_k x^k$.

Como $10 \equiv 0 \pmod 2$ temos, pelo lema anterior, $P(10) \equiv P(0) \pmod 2$. Mas $P(10) = n$ e $P(0) = a_0$; logo $n \equiv a_0 \pmod 2$. Assim, $n \equiv 0 \pmod 2$ se, e somente se, o algarismo das unidades de n for divisível por 2. ■

Proposição 5.10 (Critério de divisibilidade por 3) *Um inteiro positivo n é divisível por 3 se, e somente se, a soma de seus algarismos é divisível por 3.*

Prova:

Seja $n = a_m a_{m-1}...a_1 a_0$ a representação de n na base 10 e considere o polinômio na variável x com coeficientes inteiros: $P(x) = \sum_{k=0}^{m} a_k x^k$.

Como $10 \equiv 1 \pmod 3$ temos, pelo lema anterior, $P(10) \equiv P(1) \pmod 3$. Sendo $S = a_0 + a_1 + ... + a_m$ temos $P(1) = S$ e como $P(10) \equiv P(1) \pmod 3$, então $n \equiv S \pmod 3$. Assim, $n \equiv 0 \pmod 3$ se, e somente se, $S \equiv 0 \pmod 3$, isto é, n é divisível por 3 se, e somente se, a soma de seus algarismos é divisível por 3. ■

5.12 Exercícios

1. Resolva as seguintes congruências lineares:
   (a) $2x \equiv 1 \pmod{17}$
   (b) $3x \equiv 6 \pmod{18}$
   (c) $5x \equiv 2 \pmod{26}$
   (d) $36x \equiv 8 \pmod{102}$
   (e) $8x \equiv 16 \pmod{12}$
2. Resolva, por congruências, as seguintes equações diofantinas:
   (a) $4x + 51y = 9$
   (b) $5x - 53y = 17$
   (c) $11x + 27y = 4$
   (d) $39x + 26y = 104$
   (e) $65x + 77y = 200$
3. Verifique o teorema de Fermat para:
   (a) $a = 3$ e $p = 7$
   (b) $a = 3$ e $p = 17$
4. Mostre que $5^{38} \equiv 4 \pmod{11}$.
5. Mostre que $2^{340} \equiv 1 \pmod{341}$
6. Verifique o teorema de Wilson para $p = 7$.
7. Verifique se o inteiro 11 é primo.
8. Qual é o resto da divisão de 18! por 19?
9. Ache o resto da divisão de 15! por 17.
10. Mostre que $a^{13} \equiv a \pmod 7$ para todo inteiro a.
11. Mostre que, se o $\text{mdc}(a, 35) = 1$, então $a^{12} \equiv 1 \pmod{35}$.
12. Demonstre que, para todo inteiro a, se tem:
    (a) $a^{37} \equiv a \pmod{13}$
    (b) $a^{21} \equiv a \pmod{15}$
    (c) $a^7 \equiv a \pmod{42}$

13. Mostre que $18! + 1 \equiv 0 \pmod{437}$.

14. Mostre que:

    (a) $561 \mid 2^{561} - 2$

    (b) $561 \mid 3^{561} - 3$

15. Ache o algarismo das unidades de 3^{100}.

16. Ache o algarismo das unidades de 7^{7^7} e 9^{9^9}.

17. Ache o algarismo das unidades de $222^{333} + 333^{222}$

18. Ache os dois últimos algarismos de $7^{7^{1000}}$.

19. Enuncie e prove, usando congruências, os critérios de divisibilidade por 5, 9 e 11.

5.13 A função φ de Euler

Definição 5.6 *A função φ (fi) de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ onde $\varphi(n)$ é o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n, ou seja,*

$$\varphi(n) = \#\{t \in \mathbb{Z} : 1 \leq t \leq n \ \ e \ \ mdc(t, n) = 1\}$$

Observação 5.14 *A função acima é uma função aritmética.*

Exemplo 5.9 *Calcule $\varphi(1)$, $\varphi(2)$ e $\varphi(8)$.*

Definição 5.7 *Um sistema reduzido de resíduos módulo m é um conjunto de $\varphi(m)$ inteiros $r_1, r_2, ..., r_{\varphi(m)}$ tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \pmod{m}$*

Exemplo 5.10 *O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um SCR módulo 8 e o conjunto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8 (SRR módulo 8)*

Observação 5.15 *A fim de se obter um SRR de um SCR módulo m, basta retirar os elementos do sistema completo que não são relativamente primos com m.*

Teorema 5.7 *Se $\{r_1, r_2, ..., r_m\}$ é um SCR módulo m e a, b inteiros tais que $mdc(a, m) = 1$, então $\{ar_1 + b, ar_2 + b, ..., ar_m + b\}$ também é um SCR módulo m.*

Teorema 5.8 *Seja a um inteiro tal que $mdc(a,m)=1$. Se $\{r_1,r_2,...,r_{\varphi(m)}\}$ é um SRR módulo m, então $\{ar_1,ar_2,...,ar_{\varphi(m)}\}$ é, também, um SRR módulo m.*

Teorema 5.9 (Euler) *Sejam a e m inteiros, com $m>0$.*
Se $mdc(a,m)=1$, então $a^{\varphi(m)}\equiv 1\ (mod\ m)$.

Prova:
Seja $\{r_1,r_2,...,r_{\varphi(m)}\}$ um SRR módulo m. Como $\text{mdc}(a,m)=1$ então $\{ar_1,ar_2,...,ar_{\varphi(m)}\}$ é, também, um SRR módulo m.

Assim, cada elemento de $\{ar_1,ar_2,...,ar_{\varphi(m)}\}$ deve ser congruente a um (e só um) elemento de $\{r_1,r_2,...,r_{\varphi(m)}\}$ (Por quê?). Logo,

$$ar_1.ar_2...ar_{\varphi(m)}\equiv r_1.r_2...r_{\varphi(m)}\ (\text{mod}\ m)$$

ou seja,

$$a^{\varphi(m)}(r_1.r_2...r_{\varphi(m)})\equiv (r_1.r_2...r_{\varphi(m)})\ (\text{mod}\ m)$$

Como $\text{mdc}(r_i,m)=1$ para $i\in\{1,2,...,\varphi(m)\}$, conclui-se que $a^{\varphi(m)}\equiv 1\ (\text{mod}\ m)$. ■

Observação 5.16 *Para p primo temos $\varphi(p)=p-1$ e o Teorema de Euler é uma generalização do Teorema de Fermat.*

Teorema 5.10 *Para p primo e a um inteiro positivo temos $\varphi(p^a)=p^a-p^{a-1}$.*

Prova:
Pela definição de $\varphi(n)$ temos que $\varphi(p^a)$ é o número de inteiros positivos não superiores a p^a e relativamente primos com p^a. Mas os únicos números não relativamente primos com p^a e menores do que ou iguais a p^a são aqueles divisíveis por p. Como os múltiplos de p não superiores a p^a são: $p,2p,...,p^{a-1}p$, então $\varphi(p^a)=p^a-p^{a-1}$. ■

Exemplo 5.11 *Calcule $\varphi(4)$ e $\varphi(27)$.*

Teorema 5.11 *A função φ de Euler é multiplicativa, isto é, $\varphi(m.n)=\varphi(m).\varphi(n)$ para inteiros positivos m e n primos entre si.*

Teorema 5.12 *Se $n=p_1^{a_1}.p_2^{a_2}...p_r^{a_r}$ é a decomposição canônica do inteiro positivo $n>1$, então $\varphi(n)=p_1^{a_1-1}.p_2^{a_2-1}...p_r^{a_r-1}.(p_1-1).(p_2-1)...(p_r-1)$.*

Prova: Por indução, podemos generalizar o teorema anterior, isto é, se $\text{mdc}(m_i,m_j)=1$ para $i\neq j$, então $\varphi(m_1.m_2...m_r)=\varphi(m_1).\varphi(m_2)...\varphi(m_r)$. Assim, $\varphi(n)=\varphi(p_1^{a_1}.p_2^{a_2}...p_r^{a_r})=\varphi(p_1^{a_1}).\varphi(p_2^{a_2})...\varphi(p_r^{a_r})=(p_1^{a_1}-p_1^{a_1-1}).(p_2^{a_2}-p_2^{a_2-1})...(p_r^{a_r}-p_r^{a_r-1})=p_1^{a_1-1}.p_2^{a_2-1}...p_r^{a_r-1}.(p_1-1).(p_2-1)...(p_r-1)$. ■

Exemplo 5.12 *Calcule $\varphi(7865)$*

5.14 Exercícios

1. Calcule a forma reduzida de 7^{9876} módulo 60.
2. Mostre que $\varphi(m)$ é par se $m > 2$.
3. Mostre que se m e n são inteiros positivos tais que $m \mid n$, então $\varphi(m) \mid \varphi(n)$.
4. Mostre que existem infinitos inteiros m para os quais $\varphi(m)$ é um quadrado perfeito.
5. Mostre que existem infinitos inteiros m para os quais $10 \mid \varphi(m)$.
6. Mostre que se n é um inteiro positivo, então $\varphi(2n) = \begin{cases} \varphi(n) & \text{se} \quad n \text{ é ímpar} \\ 2\varphi(n) & \text{se} \quad n \text{ é par} \end{cases}$
7. Mostre que para a e b inteiros positivos primos entre si, temos $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

Capítulo 6

Sistemas de congruências lineares

6.1 Introdução

Definição 6.1 *Um sistema de congruências lineares é uma coleção de congruências lineares. Por exemplo,* $\begin{cases} x \equiv 1 \ (mod\, 3) \\ x \equiv 2 \ (mod\, 5) \\ x \equiv 3 \ (mod\, 7) \end{cases}$ *é um sistema de congruências lineares.*

Uma solução do sistema de congruências lineares é um inteiro x_0 *que satisfaz a cada uma das congruências lineares do sistema.*

Observação 6.1 *Um sistema de congruências lineares não tem necessariamente solução, mesmo que cada uma das congruências do sistema, isoladamente, tenha solução. Por exemplo, não existe inteiro* x_0 *que verifique simultaneamente as congruências lineares* $x \equiv 1 \ (mod\, 2)$ *e* $x \equiv 0 \ (mod\, 4)$*, embora cada uma delas, isoladamente, tenha solução.*

É claro que se alguma das congruências do sistema não tem solução então o sistema também não tem solução.

Exemplo 6.1 *Resolva o sistema de congruências lineares* $\begin{cases} x \equiv 1 \ (mod\, 3) \\ x \equiv 2 \ (mod\, 5) \\ x \equiv 3 \ (mod\, 7) \end{cases}$.

A primeira congruência nos dá $x = 1 + 3t$*, onde* $t \in \mathbb{Z}$*. Substituindo este valor de* x *na segunda congruência, obtemos:*

$$1 + 3t \equiv 2 \ (mod\, 5) \Rightarrow 3t \equiv 1 \ (mod\, 5) \Rightarrow 6t \equiv 2 \ (mod\, 5) \Rightarrow t \equiv 2 \ (mod\, 5)$$

pois $6 \equiv 1 \ (mod\, 5)$.

Logo, $t = 2 + 5u$*, com* $u \in \mathbb{Z}$ *e,* $x = 1 + 3t = 1 + 3(2 + 5u) = 7 + 15u$.

Note que qualquer inteiro da forma $7 + 15u$ *satisfaz as duas primeiras congruências do sistema.*

Substituindo este valor de x *na terceira congruência obtemos:*

$$7 + 15u \equiv 3 \ (mod\, 7) \Rightarrow 15u \equiv 3 \ (mod\, 7) \Rightarrow u \equiv 3 \ (mod\, 7)$$

pois $15 \equiv 1 \ (mod\, 7)$.

Portanto, $u = 3 + 7v$*, onde* $v \in \mathbb{Z}$ *e,* $x = 7 + 15u = 7 + 15(3 + 7v) = 52 + 105v$*. Isto significa que todo inteiro* $x \equiv 52 \ (mod\, 105)$ *é solução do sistema de congruências lineares dado.*

Observação 6.2 *Note que dividimos a solução deste sistema de três congruências lineares, de modo a resolver dois sistemas de duas congruências lineares. De fato, resolvendo as duas primeiras congruências obtivemos* $x = 7 + 15u$*. Isto corresponde a uma nova congruência linear,* $x \equiv 7 \ (mod\, 15)$*. Para obter o valor final de* x*, resolvemos o sistema* $\begin{cases} x \equiv 7 \ (mod\, 15) \\ x \equiv 3 \ (mod\, 7) \end{cases}$.

Observe também que os módulos $3, 5$ *e* 7 *são dois a dois primos entre si e que* $mmc(3, 5, 7) = 105$.

6.2 Teorema Chinês do Resto

Teorema 6.1 (Teorema Chinês do Resto) *Sejam $m_1, m_2, ..., m_r$ inteiros positivos dois a dois primos entre si, isto é, $mdc(m_i, m_j) = 1$ se $i \neq j$. Então o sistema* $\begin{cases} x \equiv a_1 \ (mod\, m_1) \\ x \equiv a_2 \ (mod\, m_2) \\ \quad\quad ... \\ x \equiv a_r \ (mod\, m_r) \end{cases}$ *possui uma única solução módulo $M = m_1.m_2...m_r$, ou seja, o sistema possui uma única solução em $\mathbb{Z}_M$.*

Prova:

Para cada $k = 1, 2, ..., r$, seja $n_k = \dfrac{M}{m_k} = m_1.m_2...m_{k-1}.m_{k+1}...m_r$.

Temos que $\text{mdc}(n_k, m_k) = 1$, pois, por hipótese, $\text{mdc}(m_i, m_j) = 1$ se $i \neq j$; logo a congruência linear $n_k x \equiv 1 \pmod{m_k}$ tem uma única solução x_k.

Vamos mostrar que o inteiro $X_0 = a_1 n_1 x_1 + a_2 n_2 x_2 + ... + a_r n_r x_r$ satisfaz cada uma das congruências lineares do sistema considerado, ou seja, X_0 é uma solução deste sistema.

De fato, se $i \neq k$ então $m_k \mid n_i$ e $n_i \equiv 0 \pmod{m_k}$, o que implica

$$X_0 = a_1 n_1 x_1 + a_2 n_2 x_2 + ... + a_r n_r x_r \equiv a_k n_k x_k \pmod{m_k}$$

Como x_k é uma solução da congruência $n_k x \equiv 1 \pmod{m_k}$, temos $n_k x_k \equiv 1 \pmod{m_k}$; logo $X_0 \equiv a_k \pmod{m_k}$, $k = 1, 2, ..., r$, e isto prova que X_0 é uma solução do sistema de congruências lineares considerado.

Suponhamos agora que X_1 é outra solução do sistema. Então $X_0 \equiv a_k \equiv X_1 \pmod{m_k}$, $k = 1, 2, ..., r$, de modo que $m_k \mid X_0 - X_1$, para cada valor de k. Como $\text{mdc}(m_i, m_j) = 1$ se $i \neq j$, segue que $m_1.m_2...m_r \mid X_0 - X_1$, isto é, $M \mid X_0 - X_1$ e $X_0 \equiv X_1 \pmod{M}$. ∎

Exemplo 6.2 *Resolva o sistema de congruências lineares* $\begin{cases} x \equiv 8 \ (mod\, 5) \\ x \equiv 5 \ (mod\, 3) \\ x \equiv 11 \ (mod\, 7) \\ x \equiv 2 \ (mod\, 4) \end{cases}$

Teorema 6.2 *Sejam $m_1, m_2, ..., m_r$ inteiros positivos dois a dois primos entre si, isto é, $mdc(m_i, m_j) = 1$ se $i \neq j$ e sejam $a_1, a_2, ..., a_r$ inteiros tais que $mdc(a_k, m_k) = 1$ para $k = 1, 2, ..., r$. Então o sistema* $\begin{cases} a_1x \equiv b_1 \ (mod\, m_1) \\ a_2x \equiv b_2 \ (mod\, m_2) \\ \quad\quad ... \\ a_rx \equiv b_r \ (mod\, m_r) \end{cases}$ *possui uma única solução módulo $M = m_1.m_2...m_r$.*

Prova:

Como $\text{mdc}(a_k, m_k) = 1$ a congruência linear $a_kx \equiv 1 \pmod{m_k}$ possui uma única solução a_k^* módulo m_k, de modo que $a_ka_k^* \equiv 1 \pmod{m_k}$. Logo a congruência $a_kx \equiv b_k \pmod{m_k}$ é equivalente à congruência $x \equiv b_ka_k^* \pmod{m_k}$ e, por conseguinte, o sistema dado é equivalente ao sistema $\begin{cases} x \equiv b_1a_1^* \pmod{m_1} \\ x \equiv b_2a_2^* \pmod{m_2} \\ \quad\quad ... \\ x \equiv b_ra_r^* \pmod{m_r} \end{cases}$, o qual possui, pelo teorema chinês do resto, uma única solução módulo M. ■

Exemplo 6.3 *Resolva o sistema de congruências lineares* $\begin{cases} 2x \equiv 1 \ (mod\, 5) \\ 3x \equiv 2 \ (mod\, 7) \\ 4x \equiv 3 \ (mod\, 11) \end{cases}$.

6.3 Representação Gráfica (tabela)

Em geral, a solução de um sistema de muitas congruências lineares pode ser obtida através da solução de vários sistemas de duas congruências, como foi feito no exemplo (6.1).

Assim, vamos interpretar o conteúdo do teorema chinês do resto para um sistema de duas congruências lineares $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ (*), onde $\text{mdc}(m, n) = 1$, através de uma tabela com $m.n$ casas.

No alto da tabela, ao longo da horizontal, escrevemos os elementos de $\mathbb{Z}_m$ e à esquerda, ao longo da vertical, escrevemos os elementos de $\mathbb{Z}_n$. A casa da tabela que fica no encontro da coluna indexada por $\overline{a} \in \mathbb{Z}_m$ com a linha indexada por $\overline{b} \in \mathbb{Z}_n$ será ocupada pelo inteiro x tal que:

1. $0 \leq x \leq mn - 1$;
2. $x \equiv a \pmod{m}$ e $x \equiv b \pmod{n}$.

Diremos, neste caso, que x tem coordenadas $(\overline{a}, \overline{b})$ na tabela.

Como $\text{mdc}(m,n) = 1$, o teorema chinês do resto afirma que toda casa da tabela é preenchida por algum inteiro no intervalo entre 0 e $mn-1$, porque todos os sistemas do tipo (*) têm uma única solução em $\mathbb{Z}_{mn}$. Além disso, duas casas com coordenadas distintas são preenchidas por elementos distintos de $\mathbb{Z}_{mn}$.

A tabela corresponde ao produto cartesiano $\mathbb{Z}_m \times \mathbb{Z}_n$.

Para preencher a tabela não é necessário resolver $m.n$ sistemas de congruências lineares. Basta lembrar que temos uma interpretação geométrica de $\mathbb{Z}_m$: suas classes estão dispostas ao longo de uma circunferência. E o mesmo vale para $\mathbb{Z}_n$. Assim a tabela é como um mapa. Colando o lado esquerdo e o direito da tabela temos um cilindro. Colando as cinrcunferências que formam as extremidades do cilindro obtemos uma superfície parecida com uma câmara de ar cheia, chamada de toro. Logo a verdadeira tabela $\mathbb{Z}_m \times \mathbb{Z}_n$ só pode ser representada sobre a superfície de um toro e entendemos o resultado sobre um plano.

Para fixar as ideias, vamos construir a tabela quando $m = 3$ e $n = 5$:

	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	0	10	5
$\overline{1}$	6	1	11
$\overline{2}$	12	7	2
$\overline{3}$	3	13	8
$\overline{4}$	9	4	14

É fácil achar as casas correspondentes a $0, 1$ e 2. Elas aparecem ao longo da "diagonal" da tabela, que são as casas com coordenadas iguais. As outras casas são preenchidas, continuando a "diagonal", observando a superfície do toro. Por exemplo, a solução do sistema $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases}$ é $x \equiv 7 \pmod{15}$.

Quando o mdc dos módulos é diferente de 1, nem todos os sistemas de congruências lineares que podemos escrever tem solução. Se pensarmos em termos da representação gráfica (tabela), isto significa que nem todas as casas da tabela serão preenchidas. Mais uma vez não é necessário resolver nenhum sistema para preencher a tabela . Basta ir preenchendo a "diagonal" e lembrando que a tabela habita a superfície de um toro. Fazendo isto, quando os módulos não são primos entre si, voltamos à casa de coordenadas $(\overline{0}, \overline{0})$ antes de esgotar os números de 0 a $mn-1$. É por isso que há casas que não são preenchidas.

A tabela no caso em que $m = 4$ e $n = 6$ é a seguinte:

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	0		6	
$\overline{1}$		1		7
$\overline{2}$	8		2	
$\overline{3}$		9		3
$\overline{4}$	4		10	
$\overline{5}$		5		11

É fácil verificar que se $\text{mdc}(m,n) \neq 1$ e se o sistema $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ tem solução então esta solução é única modulo o mmc entre m e n.

6.4 Exercícios

1. Três satélites passarão sobre o Rio esta noite. O primeiro à 1 horas da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo 15 horas e o terceiro 19 horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre o Rio.

2. Qual é o resto da divisão de 2^{6754} por 1155? (Aplicar o Teorema chinês do resto)

3. Resolva o sistema $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod{12} \end{cases}$.

4. Determine o menor inteiro positivo que deixa resto 2 na divisão por 5, resto 4 na divisão por 7 e resto 5 na divisão por 11.

5. Resolva a equação $x^2 + 42x + 21 \equiv 0 \pmod{105}$.

Capítulo 7

Criptografia básica

7.1 Introdução

- CRYPTOS = secreto, oculto
- *Criptografia*
  - Estuda os métodos para codificar uma mensagem de modo que só o seu destinatário legítimo consiga interpretá-la.
  - É a arte dos códigos secretos.
  - É a arte de escrever em cifras ou códigos.
- *Criptologia* é a arte de decifrar os códigos secretos.
- Um código vem acompanhado de duas receitas
  - uma para codificar a mensagem
  - outra para decodificar a mensagem
- *Decodificar* é o que o usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la.
- *Decifrar* significa ler uma mensagem codificada sem ser um usuário legítimo (isto é, quebrar o código - "hacker").

Exemplo 7.1 *A cifra de César é um dos primeiros tipos de criptografia conhecidos. Foi utilizada por Julio César para trocar mensagens secretas com seus exércitos e consistia de uma simples substituição de letras como abaixo, as letras da primeira linha eram substituídas pelas da segunda linha (e, para decodificar, bastava fazer o inverso).*

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e

Assim, a mensagem "nsnrnltwjhzfsit"enviada pelo exército era lida por Julio César como "inimigo recuando". Porém, esse tipo de criptografia é facilmente quebrado.

- *Código de chave pública*: saber codificar não implica saber decodificar.
- Criptografia RSA (Ron Rivest, Adi Shamir e Leonard Adleman - 1978)
  - Escolher dois primos muito grandes p e q (mais de 150 algarismos!).
  - Para codificar a mensagem, usamos o produto $n = pq$ (chave de codificação - chave pública).
  - Para decodificar a mensagem precisamos conhecer p e q (chave de decodificação - chave secreta).
  - A segurança do método vem do fato de que é difícil fatorar n para descobrir p e q.

7.2 Criptografia RSA

Aula 1

7.2.1 Pré-codificação

Vamos considerar duas pessoas, João e Maria, que desejam trocar mensagens secretas por um canal não seguro (isto é, um canal que outras pessoas - intrusos - podem acessar facilmente). Se Maria quer enviar uma mensagem codificada para João, ela deve começar pedindo para ele "fabricar"a chave secreta. Assim, João deve escolher os *parâmetros* do sistema RSA, dois primos distintos p e q (muito grandes) e calcular o produto $n = pq$. Ele também deve escolher $e \in \mathbb{N}$ tal que $mdc(e, \varphi(n)) = 1$. Os números p e q devem ser mantidos em segredo por João (em um cofre, por exemplo), já a dupla (n, e) é transmitida por um canal não seguro para Maria (e, como qualquer pessoa pode ver esse par, ele é chamado chave pública). Pode-se, por exemplo, postar esse (n, e) em um site.

De posse da chave pública, Maria escreve a mensagem. Em seguida, ela precisa transformá-la em um número α de acordo com a seguinte tabela

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

e, para cada espaço entre palavras, usar o número 99.

O próximo passo é quebrar o número α em blocos formados por números positivos menores do que n, que não comecem por zero e não correspondam a nenhuma letra segundo a tabela acima.

Exemplo 7.2 *A frase "Paraty é linda"é convertida por Maria no número*

$$\alpha = 25102710293499149921182313 10$$

Se João escolhe os parâmetros $p = 11$ e $q = 13$ (pequenos, mas é só um exemplo!), então $n = 143$. Maria, então, pode separar α em blocos

$$25 - 102 - 7 - 102 - 93 - 49 - 91 - 49 - 92 - 118 - 23 - 13 - 10$$

7.2.2 Codificando e decodificando

Codificação

A chave de codificação do sistema RSA é (n, e), onde $n = pq$ e $e \in \mathbb{N}$ tal que $mdc(e, \varphi(n)) = 1$.

Observação 7.1 *1. Temos que e é invertível módulo $\varphi(n)$*

2. $e \neq 1$, por questão de segurança, como veremos a seguir.

3. $e \neq 2$, pois $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$ é par.

4. Assim, $e > 2$ e e é ímpar.

Maria deve codificar cada bloco separadamente da seguinte maneira

$$\boxed{b = \text{bloco oriundo da pré-codificação}}$$

$$\boxed{C(b) = \text{bloco } b \text{ codificado} = \text{resto da divisão de } b^e \text{ por } n, \text{ isto é, } C(b) \equiv b^e \pmod{n}}$$

Observação 7.2 *Aqui fica claro porque $e \neq 1$. De fato, caso contrário, teríamos $C(b) = b$, afetando a segurança.*

Então, a mensagem codificada será a sequência dos blocos codificados (mas sem reuni-los formando um só número) e Maria pode passá-la para João por qualquer canal público.

Decodificação

A chave de decodificação do sistema RSA é (n, d), onde $n = pq$ e $d \in \mathbb{N}$ é o inverso de e módulo $\varphi(n)$.

Observação 7.3 *Para calcular d, João pode usar o algorítmo euclidiano estendido para $\varphi(n)$ e e, pois $mdc(e, \varphi(n)) = 1$ e $ed \equiv 1 \pmod{\varphi(n)}$. Aqui, calcular $\varphi(n)$ depende de conhecer p e q, mas esses dois foram escolhidos e guardados em segredo por João, então a princípio somente ele pode efetuar o cálculo. Mais a frente, veremos, no entanto, que se um intruso conseguir descobrir $\varphi(n)$, ele pode calcular p e q e decifrar qualquer mensagem enviada utilizando n como chave RSA.*

Se a é um bloco codificado, então $D(a)$ é o resultado do processo de decodificação, sendo

$$\boxed{D(a) = \text{resto da divisão de } a^d \text{ por } n, \text{ isto é, } D(a) \equiv a^d \pmod{n}}$$

Os processos de pré-codificação, codificação e decodificação estão resumidos na tabela a seguir

	João	Maria
Criação das chaves	Escolhe primos secretos p e q, calcula $n = pq$ e escolhe $e \in \mathbb{N}$ tal que $mdc(e, \varphi(n)) = 1$. Divulga (n, e)	
Codificação		Separa a mensagem α em blocos b e calcula $C(b) \equiv b^e \pmod{n}$. Envia $C(b)$ a João.
Decodificação	Calcula $d \in \mathbb{N}$ inverso de e módulo $\varphi(n)$. Calcula $C(b)^d \equiv D(C(b)) \pmod{n}$ e obtém a mensagem.	

Aula 2

7.2.3 Relembrando e exemplificando

Como vimos na aula passada, o esquema para codificar e decodificar uma mensagem de A para B é:

Passo 1:

- B escolhe primos p e q (grandes), $n = pq$.
- B escolhe ainda $e \in \mathbb{N}$ tal que $mdc(e, \phi(n)) = 1$.

$$\boxed{\textbf{Chave pública}: (n, e).}$$

Passo 2:

- **Codificação:** A calcula $\boxed{C(b) \equiv b^e \pmod{n}}$ para cada bloco b de mensagem (já transformada em número usando uma tabela como a da apostila e separada em blocos de tamanho menor que n, sem começar com 0 e sem ser igual a nenhuma entrada da tabela).
- A envia todos os $C(b)$ (em ordem, sem juntar) a B.

Passo 3:

- B calcula $d \in \mathbb{N}$ tal que $de \equiv 1 \pmod{\phi(n)}$.
- **Decodificação:** B calcula $\boxed{D(C(b)) \equiv C(b)^d \pmod{n}}$ para cada bloco $D(b)$ recebido.

Vimos também que $\boxed{D(C(b)) \equiv b \pmod{n}}$. De fato:

Prova:
Temos que

$$D(C(b)) = C(b)^d \equiv (b^e)^d \equiv b^{ed} \pmod{n}$$

Além disso, como d é o inverso de e módulo $\varphi(n)$, então $ed \equiv 1 \pmod{\varphi(n)}$, donde existe $k \in \mathbb{Z}_+^*$ tal que $ed = 1 + k\varphi(n)$, pois e e d são inteiros maiores que 2 e $\varphi(n) > 0$. Assim, $ed = 1 + k(p-1)(q-1)$ e, então

$$D(C(b)) \equiv b^{ed} \equiv b^{1+k(p-1)(q-1)} \equiv b\,(b^{(p-1)(q-1)})^k \pmod{n}$$

Se $p \nmid b$, então $b^{p-1} \equiv 1 \pmod{p}$ pelo Teorema de Fermat, donde

$$b^{ed} \equiv b\,(b^{(p-1)})^{(q-1)k} \equiv b \pmod{p}$$

Se $p|b$, então $b \equiv 0 \pmod{p}$ e $b^{ed} \equiv 0 \pmod{p}$, logo $b^{ed} \equiv b \pmod{p}$.

Analogamente, $b^{ed} \equiv b \pmod{q}$. Como $mdc(p,q) = 1$ e $n = pq$, segue que $b^{ed} \equiv b \pmod{n}$, isto é, $D(C(b)) \equiv b \pmod{n}$.

■

Exemplo 7.3 *Queremos usar o esquema acima para codificar e, em seguida, recuperar a mensagem* $\boxed{\textit{DOIS É PRIMO}}$. *Usando a tabela da apostila, temos que a mensagem é*

$$m = 1324182899014992527182224$$

Separando em blocos, temos

$$1324 - 182 - 899 - 1499 - 252 - 718 - 222 - 4$$

Sejam $p = 17$ *e* $q = 101$, *então* $n = 1717$ *(por que não é uma boa escolha?) e* $\phi(n) = 16 \times 100 = 1600$. *Escolhemos ainda* $e = 13$, *pois* $mdc(13, 1600) = 1$. *Para codificar a mensagem, fazemos* $\boxed{C(b_i) \equiv b_i^e \pmod{n}}$ *para cada bloco* b_i. *Assim*

$$\begin{aligned}
C(1324) &\equiv 1324^{13} \equiv 104 \pmod{1717} \\
C(182) &\equiv 182^{13} \equiv 1102 \pmod{1717} \\
C(899) &\equiv 899^{13} \equiv 495 \pmod{1717} \\
C(1499) &\equiv 1499^{13} \equiv 104 \pmod{1717} \\
C(252) &\equiv 252^{13} \equiv 1671 \pmod{1717} \\
C(718) &\equiv 718^{13} \equiv 1619 \pmod{1717} \\
C(222) &\equiv 222^{13} \equiv 817 \pmod{1717} \\
C(4) &\equiv 4^{13} \equiv 1636 \pmod{1717}
\end{aligned}$$

E a mensagem codificada é

$$104 - 1102 - 495 - 913 - 1671 - 1619 - 817 - 1636$$

Para decodificar, precisamos primeiro encontrar d tal que $de \equiv 1 \pmod{\phi(n)}$, isto é, $13d \equiv 1 \pmod{1600}$. Note que isso é equivalente a encontrar d, k tais que $13d+1600k = 1$. Como $1599 = 13 \times 123$, temos que $13 \times (-123) + 1600 \times 1 = 1$, assim $d \equiv -123 \pmod{1600}$, isto é, $d = 1477$.

Fazemos, então, $D(C(b_i)) \equiv C(b_i)^d \pmod{n}$ para cada $C(b_i)$ recebido. Por exemplo, para $i = 1$:

$$D(104) \equiv 104^{1477} \equiv 1324 \pmod{1717}$$

Exemplo 7.4 *A mensagem $6355 - 5075$ foi codificada pelo método RSA usando a senha $n = 7597$ e $e = 4947$. Além disso, sabe-se que $\varphi(n) = 7420$. Decodifique a mensagem.*

Solução: *Para encontrar d fazemos o algoritmo euclidiano estendido para $\varphi(n)$ e e.*

restos	*quocientes*	x	y
7420	-	*1*	*0*
4947	-	*0*	*1*
2473	*1*	*1*	*-1*
1	*2*	*-2*	*3*
0	*2473*	-	-

Donde $7420 \times (-2) + 4947 \times 3 = 1$, isto é, $4947 \times 3 \equiv 1 \pmod{7420}$ e $d = 3$. Para decodificar fazemos

$6355^2 = 40386025 \equiv 373 \pmod{7597}$
$6355^3 \equiv 2370415 \equiv 151 \pmod{7597}$
$D(6355) = 151$

$5075^2 = 25755625 \equiv 1795 \pmod{7597}$
$5075^3 \equiv 9109625 \equiv 822 \pmod{7597}$
$D(5075) = 822$

E obtemos

15	*18*	*22*
F	*I*	*M*

7.3 Onde podemos ter problemas?

Vamos ver dois casos em que podemos ter problemas com a segurança do RSA, que, como vimos, está baseada na dificuldade de fatorar números inteiros em tempo "curto".

7.3.1 Problema 1: conhecendo $\phi(n)$

Temos que $n = pq$ e $\phi(n) = (p-1)(q-1)$. Assim, se, além de n (é público), um invasor souber $\phi(n)$, é fácil calcular p e q utilizando um sistema. Como $\phi(n) = n - q - p + 1$, então

$$\begin{cases} pq = n \\ p + q = n - \phi(n) + 1 \end{cases}$$

Exemplo 7.5 *Sabendo-se que $n = 3552377$ é igual ao produto de dois números primos e que $\varphi(n) = 3548580$, fatore n.*

Solução: *Temos* $n = pq$ *e* $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$, *isto é,* $p + q = n - \varphi(n) + 1$. *Assim, precisamos resolver o sistema*

$$\begin{cases} p + q = 3798 \Rightarrow p = 3798 - q \\ pq = 3552377 \end{cases}$$

Temos

$$(3798 - q)q = 3552377$$
$$3798q - q^2 = 3552377$$
$$q^2 - 3798q + 3552377 = 0$$
$$q = \frac{3798 \pm \sqrt{215296}}{2}$$

$$q_1 = 2131 \Rightarrow p_1 = 1667$$
$$q_2 = 1667 \Rightarrow p_2 = 2131$$

Logo, $n = 1667 \times 2131$.

7.3.2 Problema 2: p, q grandes, mas $|p - q|$ pequeno

Nesse caso, pode-se fatorar $n = pq$ usando o *algoritmo de Fermat.*

- **Entrada:** n inteiro positivo ímpar.
- **Saída:** fatoração de n ou n é primo.
- **Passo 1:** Seja $x = [\sqrt{n}]$ (parte inteira). Se $n = x^2$, paramos. (não vai ser nosso caso, pois $p \neq q$)
- **Passo 2:** $x := x + 1$ e $y = \sqrt{x^2 - n}$.
- **Passo 3:** repita o passo 2 até y ser inteiro (nesse caso, $n = (x + y)(x - y)$) ou até que $x = \frac{n+1}{2}$ (nesse caso, n é primo).

Exemplo 7.6 *Seja* $n = 1342127$.

- *Passo 1: Temos que* $x = [\sqrt{n}] = 1158$. *Como* $x^2 = 1158^2 = 1340964 < n$, *continuamos.*
- *Passos 2 e 3:*

x	$\sqrt{x^2 - n}$
1159	*33,97*
1160	*58,93*
1161	*76,11*
1162	*90,09*
1163	*102,18*
1164	*113*

Assim: $x = 1164$ *e* $y = 113$*, donde:*

$$p = x + y = 1277$$
$$q = x - y = 1051$$

Exemplo 7.7 *Vamos considerar dois primos* p, q *tais que* $|p - q|$ *seja pequeno. Por exemplo,* $p = 907$ *e* $q = 911$*. Então* $n = pq = 826277$*. Vamos usar o algoritmo de Fermat com* n *supondo que não conhecemos sua fatoração.*

- *Passo 1:* $x = [\sqrt{n}] = 908$*. Como* $x^2 = 824464 < n$*, continuamos.*
- *Passo 2:* $x := x + 1 = 909$*. Como* $\sqrt{909^2 - 826277} = 2$*, paramos.*

Assim: $x = 909$ *e* $y = 2$*. Portanto:* $n = (x + y)(x - y) = 911 \times 907$

Exemplo 7.8 *Como no exemplo anterior, sejam* $p = 40153$ *e* $q = 40163$*. Então,* $n = pq = 1612664939$*.*

- *Passo 1:* $x = [\sqrt{n}] = 40157$*. Como* $x^2 = 1612584649 < n$*, continuamos.*
- *Passo 2: Como* $x + 1 = 40158$ *e* $\sqrt{40158^2 - 1612664939} = 5$*, paramos.*

Observação 7.4 *Quando* $|p - q|$ *é pequeno, o algoritmo de Fermat para logo!*

7.4 Um exercício resolvido

Exercício 7.1 *A chave pública utilizada pelo Banco de Toulouse para codificar suas mensagens é a seguinte* $n = 10403$ *e* $e = 8743$*. Recentemente, os computadores do banco receberam, de local indeterminado, a seguinte mensagem*

$$4746 - 8214 - 9372 - 4453 - 8198$$

O que diz a mensagem mandada ao banco?

Solução: Temos $n = 10403 = 101 \times 103$, $e = 8743$ e $\varphi(n) = 100 \times 102 = 10200$. Para encontrar d, fazemos o algoritmo de euclides estendido.

restos	quocientes	x	y
10200	-	1	0
8743	-	0	1
1457	1	1	-1
1	6	-6	7
0	1457	-	-

Assim, $10200 \times (-6) + 8743 \times 7 = 1$, donde $8743 \times 7 \equiv 1 \pmod{10200}$ e $d = 7$. Agora, podemos passar ao processo de decodificação

$4746^2 = 22524516 \equiv 2021 \pmod{10403}$
$(4746^2)^2 \equiv (2021)^2 \equiv 4084441 \equiv 6465 \pmod{10403}$
$4746^6 \equiv 13065765 \equiv 10000 \pmod{10403}$
$4746^7 \equiv 47460000 \equiv 1514 \pmod{10403}$
$D(4746) = 1514$

$8214 \equiv -2189 \pmod{10403}$
$8214^2 = 4791721 \equiv 6341 \pmod{10403}$
$(8214^2)^2 \equiv 40208281 \equiv 686 \pmod{10403}$
$8214^6 \equiv 4349926 \equiv 1472 \pmod{10403}$
$8214^7 \equiv 12091008 \equiv 2722 \pmod{10403}$
$D(8214) = 2722$

$9372 \equiv -1031 \pmod{10403}$
$9372^2 = 1062961 \equiv 1855 \pmod{10403}$
$(9372^2)^2 \equiv 3441025 \equiv 8035 \pmod{10403}$
$9372^6 \equiv 14904925 \equiv 7829 \pmod{10403}$
$9372^7 \equiv 73373388 \equiv 1029 \pmod{10403}$
$D(9372) = 1029$

$9009 \equiv -1394 \pmod{10403}$
$9009^2 \equiv 1943236 \equiv -2125 \pmod{10403}$
$(9009^2)^2 \equiv 4515625 \equiv 723 \pmod{10403}$
$9009^6 \equiv -1536375 \equiv 3269 \pmod{10403}$
$9009^7 \equiv 29450421 \equiv 9931 \pmod{10403}$
$D(9009) = 9931$

$4453^2 \equiv 19829209 \equiv 1091 \pmod{10403}$
$(4453^2)^2 \equiv 1190281 \equiv 4339 \pmod{10403}$
$4453^6 \equiv 4733849 \equiv 484 \pmod{10403}$
$4453^7 \equiv 2155252 \equiv 1831 \pmod{10403}$
$D(4453) = 1831$

$8198 \equiv -2205 \pmod{10403}$
$8198^2 \equiv 4862025 \equiv 3824 \pmod{10403}$
$(8198^2)^2 \equiv 14622976 \equiv 6761 \pmod{10403}$
$8198^6 \equiv 25854064 \equiv 2609 \pmod{10403}$
$8198^7 \equiv 21388582 \equiv 14 \pmod{10403}$
$D(8198) = 14$

Assim, a mensagem é

15	14	27	22	10	29	99	31	18	31	14
F	E	R	M	A	T		V	I	V	E

7.5 Exercícios

1. O FBI interceptou uma mensagem criptografada enviada por um terrorista do Afeganistão para seus comparsas nos EUA indicando que um agente de alto escalão será morto. McPhee, um experiente policial do FBI, viu a chave

$$(9047, 7085)$$

e disse que não há problema em decifrar o código RSA, já que ele sabe que $83|9047$. Você foi contratado para ajudar. Decifre a mensagem

$$8655 - 1969 - 1563$$

e diga qual o nome do agente que está na mira dos terroristas.

2. Fred e Julia estão brincando de RSA. Ele escolheu os primos 127 e 211, o inteiro $e = 4811$ e recebeu dela a mensagem

$$17523 - 9183$$

como teste. O que diz a mensagem?

3. No fim do seu curso de Teoria dos Números, Gustavo recebeu uma mensagem de um colega de turma. Eram duas frases criptografadas usando chaves diferentes e, com pressa, ele ficou sem saber a primeira frase. Sabendo que $n = 7171$, $e = 4667$ e que $\varphi(n) = 7000$, decodifique a frase

$$2196 - 3791$$

e complete a mensagem

2196-3791! Esse é o último exercício do curso!