Minicurso – Colóquio de Matemática da Região Norte 2014

Comitê Científico

Esta é mais uma publicação da Sociedade Brasileira de Matemática para os minicursos ministrados nos Colóquios.

Os autores que submeterem propostas de minicursos devem estar cientes de que o texto deve ser preparado em **Latex (compatível com o Miktex versão 2.7), as figuras em eps**.

O texto deve ser redigido de forma clara e recomendamos a inclusão de **exercícios** para a verificação de aprendizagem, ao final de cada capítulo.

SOCIEDADE BRASILEIRA DE MATEMÁTICA

Sociedade Brasileira de Matemática

2014

Teoria dos Números e a Lei de Reciprocidade Quadrática

Djair Paulino dos Santos
djair.santos@arapiraca.ufal.br

Fernando Vieira Costa Júnior
fernando.junior@arapiraca.ufal.br

Lindinês Coleta da Silva
lindines.silva@arapiraca.ufal.br

Ornan Filipe de Araújo Oliveira
ornan.filipe@gmail.com

Universidade Federal de Alagoas
Campus de Arapiraca

Sociedade Brasileira de Matemática

Rio de Janeiro - RJ, Brasil
2014

Coordenação Editorial:

Flávia Morgana de O. Jacinto

Editora: SBM

Impresso na Gráfica:

Capa: ? ? ?

Patrocínio: Superitendência da Zona Franca de Manaus (SUFRAMA)

Catalogação elaborada pela Biblioteca ???
Bibliotecária: ????

Santos, Djair Paulino dos
Costa Júnior, Fernando Vieira
Silva, Lindinês Coleta da
Oliveira, Ornan Filipe de Araújo
Teoria dos Números e a Lei de Reciprocidade Quadrática – Rio de Janeiro, RJ : SBM, 2014, ?? p., 20.5 cm - (Minicurso Colóquio CO 2014; v. ??)

ISBN ????-????

1. Resíduos Quadráticos 2. Símbolo de Legendre 3. Símbolo de Jacobi
I. Santos, Djair Paulino dos. II. Costa Júnior, Fernando Vieira. III. Silva, Lindinês Coleta da. IV. Oliveira, Ornan Filipe de Araújo. V. Título. VI. Série

CDD - 51

Este livro é dedicado aos jovens estudantes que buscam percorrer os fascinantes caminhos da Matemática.

"A Matemática é a única linguagem que temos em comum com a natureza."

Stephen Hawking

"Uma gota de amor é mais que um oceano de intelecto."

Blaise Pascal

"Podes chegar a qualquer lugar, desde que andes o suficiente."

Lewis Caroll

Conteúdo

Prefácio

Este texto constitui-se das notas de aula de um minicurso ministrado no III Colóquio de Matemática da Região Norte. Já estávamos a trabalhar no tema quando surgiu a oportunidade de elaborá-lo. Este livro está direcionado a um leitor iniciante na área, que busca realizar estudos sobre a teoria elementar dos números e conhecer importantes resultados de resíduos quadráticos.

Nós, Fernando, Lindinês e Djair, estávamos em busca de ampliar nossos conhecimentos, participar de eventos matemáticos e produzir alguma bibliografia quando pensamos em estudar esta área tão bela da Matemática, a Teoria dos Números. Propomos, então, que o professor Ornan Filipe nos orientasse nesta jornada. Dentre os resultados que a Teoria dos Númeors possui, o professor propôs trabalhar com Lei de Reciprocidade Quadrática, importante teorema que não esteve presente na ementa da disciplina "Introdução à Teoria dos Números" ofertada em nosso curso e ministrada pelo próprio Ornan, na Universidade Federal de Alagoas (UFAL), campus de Arapiraca.

O livro está dividido em três capítulos, os quais estão subdivididos em seções e subseções. Exemplos ilustrativos são apresentados ao fim de cada resultado, possibilitando uma melhor compreensão do seu significado e aplicação. Ao fim de cada capítulo, o leitor encontrará uma lista de exercícios. A fim de que haja um melhor aproveitamento da aprendizagem, recomendamos que todos sejam resolvidos. A organização destes não segue um grau crescente de dificuldade, mas sim, a ordem com a qual o conteúdo está disposto no capítulo. Os exercícios mencionados no conteúdo são de especial importância, pois serão utilizados em algumas demonstrações.

No primeiro capítulo, trataremos do conceito de divisibilidade, do qual decorrem várias definições e resultados que são tidos como base para estudo da Teoria dos Números. A forma como um número inteiro pode ser escrito é um tópico de grande relevância nesta área, e a análise deste caso será possível através de um famoso teorema: o Algoritmo da Divisão. Posteri-

ormente, apresentaremos os números primos, algumas de suas propriedades e o importante teorema Fundamental da Aritmética. Também trataremos das equações diofantinas, que serão de grande importância para o capítulo subseguinte.

No segundo capítulo, trataremos da importante relação de equivalência introduzida por Gauss: a congruência modular. Com este conceito, será possível derivar as mais diversas verdades aritméticas com elevada facilidade e elegância. Três clássicos teoremas serão decorrentes da relação de congruência. Estes, além de servirem de ferramental prático para tratarmos de variados problemas, nos fornecerão resultados intermediários ao principal resultado do presente trabalho.

No último capítulo, trataremos dos principais teoremas relacionados ao estudo dos resíduos quadráticos. O lema de Gauss e o critério de Euler serão discutidos. Feito isso, o imprescindível símbolo de Legendre será definido, o qual nos permitirá formular a Lei de Reciprocidade Quadrática e seus suplementos. Por fim, apresentaremos o símbolo de Jacobi, que estende o de Legendre e possui sua própria versão da Lei.

Os livros e demais formas de trabalhos referenciados poderão servir de direcionamento para os leitores que tenham a intenção de aprofundar seus estudos nos temas aqui abordados. Desejamos uma ótima leitura!

Arapiraca, 7 de Setembro de 2014.

Os autores

Capítulo 1

Divisibilidade

Neste primeiro capítulo introduziremos o conceito de divisibilidade, trazendo os principais resultados referentes ao assunto, falaremos do máximo divisor comum de dois números e ampliaremos a ideia para um número finito de inteiros. Apresentaremos o algoritmo de Euclides e o da divisão, daremos uma breve introdução sobre equações diofantinas e finalizaremos falando de números primos, onde será demonstrado o famoso Teorema Fundamental da Aritmética. Ao fim do capítulo, tem-se uma lista de exercícios para o divertimento do leitor.

1.1 Divisibilidade

Não nos ateremos a abordar as propriedades que os números naturais e inteiros possuem, no entanto, usaremos essas propriedades sem mencioná-las. O leitor deve ficar atento às passagens que as utilizarmos e, se tiver interesse, pode consultar uma explanação mais detalhada em (Silva).

Neste livro, não consideraremos o zero como um número natural, isto é, $\mathbb{N} = \{1, 2, 3, ...\}$, e I_n denotará o conjunto

$$I_n = \{1, 2, ..., n\}.$$

Antes de começarmos a falar de divisibilidade, introduziremos duas importantes proposições, as quais serão usadas, posteriormente, em demonstrações.

Proposição 1.1. *(Princípio da Boa Ordem (PBO)) Seja $X \subset \mathbb{N}$. Se $X \neq \emptyset$ então X possui um elemento mínimo.*

Exemplo 1.1. Mostre que não existe inteiro m tal que $0 < m < 1$.
Solução: Suponhamos que exista $m \in \mathbb{Z}$ e $0 < m < 1$. Então o conjunto

$$X = \{m \in \mathbb{Z} : 0 < m < 1\}$$

é um subconjunto não vazio dos números naturais. Assim, Pelo Princípio da Boa Ordem, existe um menor elemento $d \in X$, isto é, $\forall\ m \in X$, tem-se

$$0 < d \leq m < 1.$$

Multiplicando a desigualdade acima por d, obtém-se

$$0 < d^2 \leq dm < d < 1.$$

Contradição, pois $d^2 \in X$ e $d^2 < d$. Portanto, não existe inteiro m entre zero e um.

Proposição 1.2. *(Princípio da Indução Finita - Primeira forma) Seja P uma propriedade. Se P é válida para 1 e vale para $k+1$ sempre que vale para k, então P é válida para todo $n \in \mathbb{N}$.*

A proposição acima mencionada corresponde à primeira forma do Princípio de Indução. No entanto, às vezes, é necessário recorrer à segunda forma. Um enunciado para esta seria:

Proposição 1.3. *(Princípio da Indução Finita - Segunda forma) Seja P uma propriedade. Se P é válida para 1 e vale para $k+1$ sempre que vale para todo $i \in I_k$, então P é válida para todo $n \in \mathbb{N}$.*

Perceba a sutileza que diferencia os dois princípios de indução. Na primeira forma, exige-se apenas que a validez da propriedade para k implique na veracidade da propriedade para $k+1$. Já na segunda, exige-se que a propriedade valha para $k+1$ desde que valha para todos os números entre 1 e k.

Estes princípios são equivalentes. A seguir, demonstraremos uma das equivalências (convidamos o leitor a fazer as outras demais no exercício 1).

Exemplo 1.2. Mostre o Princípio de Indução Finita, segunda forma, considerando válido o PBO.
Solução: Seja $\alpha(n)$ uma sentença com as seguintes propriedades:

i) $\alpha(1)$ é verdadeira;

ii) $\alpha(k+1)$ é verdadeira se $\alpha(i)$ é verdadeira, $\forall\ i \in I_k$.

Mostraremos que $\alpha(n)$ é verdadeira $\forall\ n \in \mathbb{N}$. Para isso, consideremos os conjuntos

$$X = \{n \in \mathbb{N} \mid \alpha(n) \text{ é verdadeira}\} \text{ e } B = \{n \in \mathbb{N} \text{ e } n \notin X\}.$$

Suponhamos $B \neq \emptyset$. Então, como $B \subset \mathbb{N}$, o PBO garante a existência de um menor elemento $d \in B$. Assim, α é válida para todos os naturais menores do que d, ou seja, $\alpha(n)$ é válida para i, com $i \in I_{d-1}$. Agora, pela segunda propriedade de α, segue que $\alpha(d)$ é válida, isto é, $d \in X$. Contradição, pois $d \in B$ e $B \cap X = \emptyset$. Logo $B = \emptyset$ e $X = \mathbb{N}$.

Muitos resultados envolvendo números naturais são provados usando o Princípio de Indução Finita (PIF). Em geral, utiliza-se o PIF seguindo o seguinte roteiro:

i) verifica-se que o resultado é válido para $n = 1$ ou para o menor valor natural suposto que a afirmação é válida;

ii) supõe-se que o resultado vale para $n = k$. Esta é a *Hipótese de Indução* (HI) e, obrigatoriamente, será usada no próximo passo;

iii) mostra-se que a afirmação também se verifica para $n = k + 1$. Se valer, o PIF garante que a afirmação é verdadeira para todo n natural.

Exemplo 1.3. Mostre que, para todo n natural, tem-se

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

Solução: Usaremos indução finita (primeira forma) para demonstrar. Note que vale para $n = 1$, pois

$$(2 \cdot 1 - 1) = 1 = (1)^2.$$

Supondo que vale para $n = k$, isto é,

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2,$$

mostremos que também vale para $n = k + 1$.

$$\begin{array}{rcll} 1 + 3 + \cdots + (2k - 1) + [2(k + 1) - 1] & = & k^2 + 2(k + 1) - 1 & HI \\ & = & k^2 + 2k + 2 - 1 & \\ & = & k^2 + 2k + 1 & \\ & = & (k + 1)^2. & \end{array}$$

Logo, o resultado é válido para $n = k + 1$ e, pelo princípio de indução, vale para todo n natural.

Definição 1.1. Sejam $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}$. Diz-se que a *divide* b se existir $c \in \mathbb{Z}$ tal que $b = ac$. Neste caso, denota-se por $a|b$. Quando não existe $c \in \mathbb{Z}$ tal que $b = ac$, diz-se que a *não divide* b e escreve-se $a \nmid b$.

Observe que dizer a *divide* b é o mesmo que falar b *é divisível por* a ou b *é um múltiplo de* a.

Na maioria das definições que fizermos a partir de agora, faremos uso do conceito de divisibilidade. E, embora tenhamos usado $b = ac$ na definição, de agora em diante, não nos preocuparemos em seguir essa ordem (podemos usar $b = ca$).

Exemplo 1.4. Note que $5|30$, $2|14$ e $3|18$, pois $30 = 5 \cdot 6$, $14 = 2 \cdot 7$ e $18 = 6 \cdot 3$. Mas $4 \nmid 10$, $3 \nmid 16$ e $10 \nmid 32$, pois não existem inteiros a, b, c tais que $10 = 4a$, $16 = 3b$ ou $32 = 10c$.

O próximo teorema resume as principais propriedades operatórias do conceito de divisibilidade. Portanto, por várias vezes, o evocaremos para justificar algumas passagens nos teoremas e nos exemplos que se sucederão.

Teorema 1.1. *Da definição, decorre que, para quaisquer* $a, b, c, d \in \mathbb{Z}$*:*

i) $a|a$, $1|a$ *e* $a|0$*;*

ii) se $a|b$ *e* $b|c$*, então* $a|c$*;*

iii) se $a|b$ *e* $c|d$*, então* $ac|bd$*;*

iv) se $ab|ac$ *e* $a \neq 0$*, então* $b|c$*;*

v) se $a|b$ *e* $b \neq 0$*, então* $|a| \leq |b|$*;*

vi) $a|1 \Leftrightarrow a = \pm 1$*;*

vii) $a|b$ *e* $b|a \Rightarrow |a| = |b|$*;*

viii) se $c|a$ *e* $c|b$*, então* $c|(ma + nb)$*, para quaisquer* $m, n \in \mathbb{Z}$*;*

ix) se $a|(b \pm c)$*, então* $a|b \Leftrightarrow a|c$*.*

Demonstração:

i) Note que $a = 1 \cdot a$ e $0 = a \cdot 0$.

ii) Da hipótese, tem-se $b = ar$ e $c = bs$, isto é, $c = ars$. Logo, $a|c$.

iii) Como $a|b$ e $c|d$, $b = ar$ e $d = sc$, com $r, s \in \mathbb{Z}$, daí, $bd = arsc = acrs$, ou seja, $ac|bd$, pois $rs \in \mathbb{Z}$.

iv) Como $ab|ac$, existe r inteiro tal que $ac = abr$, dividindo por a, já que $a \neq 0$, tem-se $c = br$, isto é, $b|c$.

v) Da hipótese, $b = ar$. Assim, $|b| = |ar| = |a| \cdot |r|$. Mas $b \neq 0$, então $r \neq 0$, e isto significa que $|r| \geq 1$. Por isso, $|b| = |a| \cdot |r| \geq |a| \cdot 1 = |a|$. Logo, $|a| \leq |b|$.

vi) Do item anterior, tem-se $|a| \leq |1| = 1$. Como $a \neq 0$, decorre que $a = \pm 1$.

vii) Basta usar o item (v).

viii) Da hipótese, $a = cr$ e $b = cs$. Então

$$ma = mcr \quad \text{e} \quad nb = ncs.$$

Somando membro a membro, obtém-se $ma + nb = mcr + ncs = c(mr + ns)$. Como $(mr + ns) \in \mathbb{Z}$, tem-se que $c|(ma + nb)$.

ix) Se $a|(b \pm c)$ e $a|b$ então, pelo item anterior, $a|[1(b \pm c) - b]$, isto é, $a| \pm c$, ou ainda, $a|c$. A recíproca é análoga.

■

Exemplo 1.5. Atenção para erros comuns:

a) $a|(b + c)$ não implica $a|b$ ou $a|c$. Contraexemplo: $6|(4 + 2)$, mas $6 \nmid 2$ e $6 \nmid 4$. Veja o teorema 1.1.ix;

b) $a|b$ não implica $|a| \leq |b|$. Contraexemplo: $2|0$, pois $0 = 2 \cdot 0$, e $|2| > |0|$. Isso mostra que a condição $b \neq 0$ não deve ser esquecida ao usar o item v do teorema 1.1;

c) $a|bc$ não implica $a|b$ ou $a|c$. Contraexemplo: $8|24 = 6 \cdot 4$, mas $8 \nmid 6$ e $8 \nmid 4$. Mais adiante mostraremos condições para que isso seja válido.

Exemplo 1.6. Mostre que $13|(2x + 5y) \Leftrightarrow 13|(x + 9y)$, com $x, y \in \mathbb{Z}$. *Solução:* Da hipótese, $13|(2x + 5y)$. Então $13|7(2x + 5y)$. Mas

$$7(2x + 5y) = (14x + 35y) = (13x + x + 26y + 9y) = [(13x + 26y) + (x + 9y)].$$

Como $13|(13x + 26y)$, pelo teorema 1.1.ix, $13|(x + 9y)$. Reciprocamente, $13|(x + 9y)$ e

$$2(x + 9y) = (2x + 18y) = [(2x + 5y) + 13y].$$

Assim, como $13|13y$ e $13|2(x + 9y)$, segue-se que $13|(2x + 5y)$.

1.2 Algoritmo da Divisão

Desde o ensino fundamental, estamos habituados a realizar divisão de números inteiros, digamos, a por b, onde a é o dividendo e b é o divisor. Se a conta for exata, devemos encontrar um número inteiro q tal que $a = bq$. Se a divisão não for exata, então deve sobrar um resto r e, para sabermos se o nosso cálculo está correto, tiramos a prova real da seguinte forma: o resultado da multiplicação do quociente pelo divisor somado com o resto deve ser igual ao dividendo. Em outras palavras, $a = bq + r$. Mas será que os números q e r sempre existem? E, em caso afirmativo, são únicos? As respostas estão no próximo teorema.

Teorema 1.2. *(Algoritmo da Divisão) Dados $a \in \mathbb{Z}$ e $b \in \mathbb{N}$, existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r, \quad \textit{com} \;\; 0 \leq r < b.$$

Demonstração: Seja

$$X = \{a - bx : x \in \mathbb{Z} \;\text{ e }\; a - bx \geq 0\}.$$

Note que $X \neq \emptyset$, pois, tomando $x = -|a| \in \mathbb{Z}$, tem-se:

$$a - bx = a - b(-|a|) = a + b|a| \geq a + |a| \geq 0,$$

pois $b \geq 1$ e $|a| \geq \pm a$. Como $X \subset \mathbb{N}$ e $X \neq \emptyset$, o Princípio da Boa Ordenação garante a existência de um menor elemento r. Assim, $\exists\ q \in \mathbb{Z}$ tal que

$$r = a - bq.$$

Ou seja,

$$a = qb + r, \;\; \text{com} \;\; r \geq 0.$$

Afirmamos que $r < b$. De fato, suponhamos que não fosse, isto é, $r \geq b$. Então $r - b \geq 0$. Mas $r = a - bq$, daí

$$r - b = a - bq - b = a - b(q + 1) \geq 0,$$

ou seja, $r - b \in X$. Contradição, pois $r - b < r$ e r é o menor elemento de X. Logo,

$$a = qb + r, \;\; \text{com} \;\; 0 \leq r < b.$$

Mostraremos agora a unicidade. Para tanto, suponhamos que existam duas formas, isto é,

$$a = q_1 b + r_1, \;\; \text{com} \;\; 0 \leq r_1 < b \quad \text{e}$$
$$a = q_2 b + r_2, \;\; \text{com} \;\; 0 \leq r_2 < b.$$

Então

$$q_1 b + r_1 = q_2 b + r_2, \tag{1.2.1}$$

ou melhor,

$$b(q_1 - q_2) = r_2 - r_1,$$

o que significa que $b|(r_2 - r_1)$. Mas

$$\begin{cases} 0 \leq r_1 < b; \\ 0 \leq r_2 < b. \end{cases}$$

Multiplicando a segunda inequação por -1, obtém-se

$$\begin{cases} 0 \leq r_1 < b; \\ 0 \geq -r_2 > -b. \end{cases}$$

Ou ainda

$$\begin{cases} 0 \leq r_1 < b; \\ -b < -r_2 \leq 0. \end{cases}$$

Somando as duas inequações membro a membro, obtém-se $-b < r_1 - r_2 < b$ o que implica $|r_1 - r_2| < b$. Então, pelo teorema 1.1.v, decorre que $r_1 = r_2$. Substituindo em 1.2.1, concluímos que $q_1 = q_2$, provando, assim, a unicidade.

Corolário 1.1. *Dados $a, b \in \mathbb{Z}$ e $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r, \quad \textit{com} \;\; 0 \leq r < |b|.$$

Demonstração: Se $b > 0$ o resultado segue imediatamente do teorema 1.2. Se $b < 0$ então $-b > 0$ e pelo teorema 1.2 existem únicos $q_1, r \in \mathbb{Z}$, com $0 \leq r < -b$, tais que

$$a = (-b)q_1 + r = b(-q_1) + r, \quad \text{com} \;\; 0 \leq r < -b.$$

Tomando, $q = -q_1$ temos o resultado. Logo, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = qb + r, \quad \text{com} \;\; 0 \leq r < |b|.$$

Neste livro, usaremos o importante Algoritmo da Divisão para resolver algumas questões, especialmente aquelas que envolvem a forma com a qual um número inteiro é escrito. Agora, demonstraremos resultados interessantes que fazem uso do mesmo.

Exemplo 1.7. Numa divisão por -6, os possíveis restos são os números pertences ao conjunto $X = \{r \in \mathbb{Z} : 0 \leq r < |-6|\}$. Ou seja, ao conjunto $X = \{0, 1, 2, 3, 4, 5\}$.

Exemplo 1.8. Mostre que:

a) a soma de um número ímpar com um número par é um número ímpar;

b) a soma de dois números ímpares é um número par;

c) a soma de dois números pares é um número par.

Solução:

a) Seja a um número par e b um número ímpar. Então a é divisível por 2, ou seja, deixa resto zero na divisão por 2, ou ainda, $a = 2k$, para algum k inteiro. Por outro lado, b não é divisível por 2, isto é, $b = 2r+1$. Assim

$$a + b = 2k + 2r + 1 = 2(k + r) + 1.$$

Portanto $a + b$ deixa resto 1 quando dividido por 2 e, por isso, $a + b$ é ímpar.

b) Sejam a, b números pares. Então $a = 2k$ e $b = 2r$, com $k, r \in \mathbb{Z}$. Daí

$$a + b = 2k + 2r = 2(k + r).$$

Logo, $a + b$ é par.

c) Sejam a, b números ímpares. Então $a = 2r + 1$ e $a = 2s + 1$. Assim

$$a + b = 2r + 1 + 2s + 1 = 2(r + s + 1).$$

Portanto, a soma de números ímpares é um número par.

Resultados análogos para a multiplicação encontram-se na lista de exercícios no fim do capítulo (ver exercício 8). Recomendamos que o leitor os faça, pois tais resultados serão usados posteriormente.

1.3 O Máximo Divisor Comum

Definição 1.2. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. O *máximo divisor comum (MDC)* de a e b, denotado por $mdc(a, b)$, é um inteiro positivo d que satisfaz as condições:

i) $d|a$ e $d|b$;

ii) se $\exists\ c \in \mathbb{Z}$ tal que $c|a$ e $c|b$, então $c|d$.

O item (i) nos diz que $mdc(a, b)$ é um divisor comum de a e b. Já o item (ii) exige que ele seja o máximo.

Exemplo 1.9. Como podemos verificar, $mdc(3,6) = 2$, $mdc(-5,-30) = 5$, $mdc(6,0) = 6$, $mdc(13,20) = 1$ e $mdc(4,-2) = 2$.

Calcular o MDC desses números foi fácil, pois são números relativamente pequenos e, para estes, não é difícil encontrar os divisores em comum. No entanto, calcular o MDC nem sempre é tarefa simples. Mais adiante, demonstraremos uma maneira prática de fazer isso.

Proposição 1.4. *Da definição de MDC, resulta que:*

i) $mdc(a,b) = mdc(b,a)$;

ii) se a *é não nulo, então* $mdc(a,0) = |a|$;

iii) se $a|b$*, então* $mdc(a,b) = |a|$.

As demonstrações são imediatas, por isso, deixamos a cargo do leitor.

Teorema 1.3. *(Existência e unicidade do MDC) Dados* $a, b \in \mathbb{Z}$*, com* $a \neq 0$*, existe um único* d *tal que* $d = mdc(a,b)$.

Demonstração: Consideremos o conjunto

$$X = \{ar + bs : r, s \in \mathbb{Z} \text{ e } ar + bs > 0\}.$$

Perceba que $X \subset \mathbb{N}$ e $X \neq \emptyset$, pois $|a| \in X$, basta tomar $r = \pm 1$ (a depender de a) e $s = 0$. Então, pelo PBO, X possui um elemento mínimo d. Assim, existem $x, y \in \mathbb{Z}$ tais que

$$d = ax + by. \tag{1.3.2}$$

Mostraremos agora que $d = mdc(a,b)$. Pelo Algoritmo da Divisão, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = dq + r, \quad \text{com} \quad 0 \leq r < d. \tag{1.3.3}$$

Substituindo 1.3.2 em 1.3.3, tem-se

$$a = (ax + by)q + r,$$

ou ainda

$$r = a(1 - xq) + b(-yq), \quad \text{com} \quad 0 \leq r < d.$$

Então $r = 0$, pois, do contrário, teríamos $r \in X$ e $r < d$, o que é absurdo, pois d é o menor elemento de X. Isto significa, substituindo $r = 0$ em 1.3.3, que $a = dq$, ou seja, $d|a$. Analogamente mostra-se que $d|b$. Finalmente, supondo que exista c inteiro tal que $c|a$ e $c|b$ então, pelo teorema 1.1.viii, $c|(ax + by)$, ou melhor, $c|d$. Logo $d = mdc(a,b)$.

Para mostrar a unicidade, suponhamos que $d = mdc(a,b) = d'$. Então $d|d'$ e $d'|d$. Pelo teorema 1.1.vii, $|d| = |d'|$. Mas $d, d' > 0$, portanto $d = d'$. ■

Corolário 1.2. *Se $d = mdc(a, b)$, então existem $m, n \in \mathbb{Z}$ tais que $d = am + nb$.*

Demonstração: Basta tomar $m = x$ e $n = y$ na demonstração do teorema 1.3.

Teorema 1.4. $mdc(ac, bc) = |c| \cdot mdc(a, b)$

Demonstração: Sejam $k = mdc(ac, bc)$ e $r = mdc(a, b)$. Mostraremos que $k = |c| \cdot r$. Como $k = mdc(ac, bc)$, tem-se que $k|ac$ e $k|bc$. Além disso, $r = mdc(a, b)$, isto é, $r|a$ e $r|b$, ou ainda,

$$rc|ac \quad \text{e} \quad rc|bc.$$

Por isso, $rc|mdc(ac, bc) = k$. Ou seja, existe um inteiro x tal que

$$xcr = k. \tag{1.3.4}$$

Assim,

$$xrc|ac \quad \text{e} \quad xrc|bc.$$

Como $c \neq 0$, tem-se $xr|a$ e $xr|b$, por isso, $xr|mdc(a, b) = r$. Logo, $|xr| \leq |r|$. Portanto, obrigatoriamente (por quê?), devemos ter $x = \pm 1$. Substituindo x em 1.3.4, obtém-se $\pm cr = k$, ou ainda, $|c|r = k$, isto é,

$$mdc(ac, bc) = |c| \cdot mdc(a, b).$$

■

Exemplo 1.10. Note que $mdc(12, -18) = mdc(-12, -18) = mdc(-12, 18) = = mdc(12, 18) = mdc(2 \cdot 6, 2 \cdot 9) = |2| \cdot mdc(6, 9) = 2 \cdot 3 = 6$.

Definição 1.3. Quando $mdc(a, b) = 1$, diz-se que *a e b são relativamente primos* ou *primos entre si.*

Exemplo 1.11. Os números 5 e 21 são primos entre si, pois $mdc(5, 21) = 1$. Os números 6 e 7 são relativamente primos, já que $mdc(6, 7) = 1$. Mas $mdc(8, 18) = 2$ e, por isso, 8 e 18 não são primos entre si.

Como comentamos, $a|bc$ não implica $a|b$ ou $a|c$. Mas o próximo teorema nos fornece uma condição para que isso aconteça.

Teorema 1.5. *Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração: Como $mdc(a,b) = 1$, existem $r, s \in \mathbb{Z}$ tais que

$$ar + bs = 1.$$

Multiplicando a equação acima por c, obtém-se

$$arc + bcs = c.$$

Como $a|a$ e $a|bc$, tem-se, pelo teorema 1.1.viii, que $a|[(rc)a + s(bc)]$, isto é, $a|c$. ■

Exemplo 1.12. Como $4|24$, $24 = 3 \cdot 8$ e $mdc(4,3) = 1$, segue que $4|8$.

Exemplo 1.13. Sejam $a, b \in \mathbb{Z}^*$ e $mdc(a,b) = 1$. Mostre que

$$mdc(a+b, a-b) = 1 \text{ ou } 2.$$

Solução: Seja $d = mdc(a+b, a-b)$. Então $d|(a+b)$ e $d|(a-b)$. Portanto,

$$d|[(a+b)+(a-b)] = 2a \text{ e } d|[(a+b)-(a-b)] = 2b.$$

Dessa forma, $d|mdc(2a, 2b)$. Mas $mdc(2a, 2b) = |2|mdc(a,b) = 2 \cdot 1 = 2$. Assim, $d|2$ e, como $d > 0$, segue que $d = 1$ ou $d = 2$.

Observe que, no exemplo anterior, utilizamos várias propriedades de divisibilidade e de MDC. Se o leitor não recorda delas, recomendamos que volte e as releia, pois, de agora em diante, ficará mais comum a utilização dessas propriedades, algumas vezes sem mencioná-las.

Teorema 1.6. *Sejam $a, b, c \in \mathbb{Z}$. Se $a|c$, $b|c$ e $mdc(a,b) = 1$ então $ab|c$.*

Demonstração: Como $a|c$ e $b|c$, existem inteiros m e n tais que

$$c = am \quad \text{e} \quad c = bn. \tag{1.3.5}$$

Além disso, $mdc(a,b) = 1$, portanto, pelo corolário 1.2, existem $r, s \in \mathbb{Z}$ tais que

$$ar + bs = 1. \tag{1.3.6}$$

Multiplicando 1.3.6 por c, tem-se

$$arc + bsc = c.$$

Agora, substituindo c obtido em 1.3.5 no membro esquerdo da igualdade acima, obtemos

$$arbn + bsam = c \Leftrightarrow ab(rn + sm) = c,$$

isto é, $ab|c$. ■

Teorema 1.7. *Seja $d = mdc(a, b)$. Então $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.*

Demonstração: Seja $mdc(\frac{a}{d}, \frac{b}{d}) = k$, então

$$k|\frac{a}{d} \text{ e } k|\frac{b}{d}.$$

Ou seja, existem inteiros r e s tais que

$$\frac{a}{d} = kr \text{ e } \frac{b}{d} = ks,$$

ou melhor, $a = dkr$ e $b = dks$. E isto significa que $dk|a$ e $dk|b$, e mais, $dk|mdc(a, b) = d$. Como $d, k > 0$, pelo teorema 1.1.v, tem-se $k = 1$, o que conclui a demonstração. ■

Observe que usamos fração no exemplo anterior, mas isso só foi possível porque tínhamos a garantia que o valor da fração era um número inteiro.

Definição 1.4. (Extensão) Sejam $a, b, c \in \mathbb{Z}$ não todos nulos, então o MDC desses três números é o inteiro positivo d tal que

i) $d|a$, $d|b$ e $d|c$;

ii) se existir $k \in \mathbb{Z}^*$ tal $k|a$, $k|b$ e $k|c$, então $k|d$.

De um modo geral, o MDC pode ser estendido para uma quantidade finita de inteiros não todos nulos. A definição é análoga às anteriores.

Podemos também ter três inteiros (ou mais) relativamente primos sem que eles sejam dois a dois primos. Por exemplo, os números $6, 10, 35$ são relativamente primos, pois $mdc(6, 10, 35) = 1$, mas eles não são primos dois a dois, já que $mdc(6, 10) = 2$, $mdc(10, 35) = 5$ e $mdc(6, 35) = 3$.

Exemplo 1.14. Mostre que

$$mdc(a, b, c) = mdc(mdc(a, b), c).$$

Solução: Seja $d = mdc(a, b, c)$ e $k = mdc(a, b)$. Então $d|a$, $d|b$ e $d|c$. Por isso, $d|k$, ou seja, d é um divisor comum de k e c. Mostremos que d é o máximo. Para isto, suponhamos que exista um inteiro p tal que $p|k$ e $p|c$. Então, como $k|a$ e $k|b$ (por quê?), por transitividade, tem-se que $p|a, p|b$ e $p|c$. Logo $p|d$. Portando, $d = mdc(mdc(a, b), c)$.

Esta é a demonstração da primeira parte da generalização desse conceito. Recomendamos que o leitor demonstre o exercício correspondente na lista de exercício no fim do capítulo (ver exercício 12).

Teorema 1.8. *Sejam $m, n, r \in \mathbb{Z}$ e $mdc(m, n) = 1$. Então*

$$mdc(r, mn) = 1 \quad \Leftrightarrow \quad mdc(r, m) = mdc(r, n) = 1.$$

Demonstração: ($\Rightarrow$) Seja $d = mdc(r, m)$. Então $d|r$ e $d|m$, ou ainda, $d|r$ e $d|mn$. Assim, $d|mdc(mn, r) = 1$. O que mostra que $mdc(r, m) = 1$. Analogamente mostra-se que $mdc(r, n) = 1$.
($\Leftarrow$) Seja $d = mdc(r, mn)$. Então $d|r$ e $d|mn$. Como $mdc(m, n) = 1$, segue que $d|n$ ou $d|m$. Assim, $d|r$ e $d|n$ ou $d|r$ e $d|m$. Em qualquer caso, $d|mdc(n, r) = mdc(m, r) = 1$. Como $d > 0$, segue que $d = 1$. Concluindo, assim, a demonstração. ■

Teorema 1.9. *Sejam $a, b, q, r \in \mathbb{Z}$, com $a = bq + r$ e $0 \leq r < b$. Então $mdc(a, b) = mdc(b, r)$.*

Demonstração: Seja $d = mdc(a, b)$. Então $d|a$ e $d|b$, em particular, $d|(a - qb)$, isto é, $d|r$. Logo, d é um divisor comum de b e r. Mostremos que d é o máximo. Suponhamos que exista $c \in \mathbb{Z}$ tal que $c|b$ e $c|r$. Então $c|(qb + r)$, ou seja, $c|a$. Como $c|b$, tem-se, $c|mdc(a, b) = d$. Logo, $d = mdc(b, r)$. ■

1.4 O Algoritmo de Euclides

Nesta seção, estudaremos o famoso Algoritmo de Euclides, um método eficiente de encontrar o MDC de dois números. Posteriormente, este algoritmo será utilizado na obtenção de soluções para Equações Diofantinas.

Antes de demonstrarmos o teorema, introduziremos o próximo exemplo, a fim de que o leitor possa compreender melhor o que acontecerá na demonstração.

Exemplo 1.15. Calcule $mdc(234, 123)$.
Solução: Dividindo 234 por 123, obtém-se quociente 1 ($q_1 = 1$) e resto 111 ($r_2 = 111$). Assim, pelo teorema 1.9, segue que

$$mdc(234, 123) = mdc(123, 111).$$

Mas nós podemos usar o teorema novamente, agora dividindo 123 por 111, obtendo quociente 1 ($q_2 = 1$) e resto 12 ($r_3 = 12$). Dessa forma,

$$mdc(123, 111) = mdc(111, 12).$$

Utilizando o teorema mais uma vez, agora dividindo 111 por 12, tem-se quociente 9 ($q_3 = 9$) e resto 3 ($r_4 = 3$). Por isso,

$$mdc(111, 12) = mdc(12, 3).$$

Repetindo o processo, dessa vez dividindo 12 por 3, obteremos quociente 4 ($q_4 = 4$) e resto igual a zero ($r_5 = 0$). Logo,

$$mdc(12, 3) = mdc(3, 0).$$

Mas, $mdc(3, 0) = 3$. Portanto,

$$3 = mdc(3, 0) = mdc(12, 3) = mdc(111, 12) = mdc(123, 111) = mdc(234, 123).$$

Observe que, na medida em que o processo foi aplicado, obtivemos restos cada vez menores. Ou seja, por maior que sejam os números envolvidos, o processo é finito.

Processo análogo será feito na demonstração do próximo teorema. Se houver alguma parte que o leitor não entenda, recomendamos que volte a este exemplo e faça a analogia.

Teorema 1.10. *(Algoritmo de Euclides) Aplicando sucessivas vezes o Algoritmo da Divisão, obtém-se* $mdc(a, b) = r_n$, *onde* $a = r_0 \in \mathbb{Z}_+$, $b = r_1 \in \mathbb{Z}_+^*$, $r_{n+1} = 0$ *e*

$$r_j = q_{j+1} r_{j+1} + r_{j+2}, \quad com \;\; 0 \leq r_{j+2} < r_{j+1},$$

para $j \in \{0, 1, 2, \cdots, n-1\}$. *Ou seja,* r_n *é o último resto não nulo.*

Demonstração: Aplicando o Algoritmo da Divisão para dividir r_0 por r_1, obtemos

$$r_0 = r_1 q_1 + r_2, \quad \text{com} \quad 0 \leq r_2 < r_1.$$

Novamente, agora dividindo r_1 por r_2 segue que

$$r_1 = r_2 q_2 + r_3, \quad \text{com} \quad 0 \leq r_3 < r_2.$$

Repetindo esse processo, que é finito, pois $j < i$ implica $r_i < r_j$, chegaremos a $r_{n+1} = 0$. Então, utilizando o teorema 1.9 sucessivas vezes, obteremos

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = ... = mdc(r_0, r_1) = mdc(a, b).$$

■

Exemplo 1.16. Utilize o teorema 1.10 para determinar:

a) $mdc(56, 12)$;

b) $mdc(148, 25)$.

Solução:

a) Dividindo 56 por 12, obtemos quociente 4 e resto 8. Agora dividindo 12 por 8 (o resto da primeira divisão) obtemos quociente 1 e resto 4. Mais uma vez, dividindo 8 por 4 (o segundo resto) obtemos quociente 2 e resto 0 (o terceiro resto da divisão). Logo, o segundo resto, ou seja, 4 é o MDC de 56 e 12.

b) Dividindo 148 por 25, temos quociente igual a 5 e resto igual a 23. Então devemos dividir o divisor inicial pelo primeiro resto, ou seja, dividir 25 por 23, onde obtemos quociente 1 e resto 2. Agora devemos dividir o primeiro resto (ou se preferir: o divisor da conta anterior) pelo segundo resto, isto é, dividir 23 por 2, onde obtemos quociente 11 e resto 1. Por fim, dividindo 2 por 1 (o segundo resto pelo terceiro) obtém-se quociente 2 e resto 0. Portanto, $mdc(148, 25) = 1$. Isto significa que os números 148 e 25 são primos entre si.

1.5 Equações Diofantinas

As Equações Diofantinas são um tipo especial de equações algébricas. O nome é devido ao matemático grego Diofanto de Alexandria (aprox. 300 d.C.). Nesta seção, estudaremos o tipo mais simples destas: as lineares com duas incógnitas. Mais adiante, mostraremos que há uma íntima ligação entre Equações Diofantinas e Congruências Lineares.

Definição 1.5. Diz-se que uma equação algébrica é uma *equação diofantina* se seus coeficientes e suas soluções são números inteiros.

Exemplo 1.17. Encontre uma solução para cada equação diofantina abaixo:

a) $3x + 6y = 12$;

b) $2x + 7y = 4$;

c) $5x + 3y = 8$.

Solução:

a) Veja que $x = 0$ e $y = 2$ é uma solução para a equação, pois

$$3 \cdot 0 + 6 \cdot 2 = 12.$$

b) Perceba que $x = 2$ e $y = 0$ é uma solução para a equação, já que

$$2 \cdot 2 + 7 \cdot 0 = 4.$$

c) Como

$$5 \cdot (-2) + 3 \cdot 6 = 8,$$

segue que $x = -2$ e $y = 8$ é uma solução para a equação diofantina.

Nos exemplos acima, todas as equações tiveram solução, mas será que esse fato é, em geral, verdadeiro? A resposta estará no próximo teorema.

Teorema 1.11. *Sejam $a, b, c, x, y \in \mathbb{Z}$, com $ab \neq 0$, e $d = mdc(a, b)$. A equação diofantina*

$$ax + by = c \tag{1.5.7}$$

tem solução se, e só se, $d|c$.

Demonstração: Seja (x_0, y_0) uma solução da equação, ou seja,

$$ax_0 + by_0 = c.$$

Como $d = mdc(a, b)$, segue que $d|a$ e $d|b$ e, por isso, d divide qualquer combinação de a e b, em particular,

$$d|(ax_0 + by_0) = c.$$

Reciprocamente, se $d|c$, então $c = kd$, com $k \in \mathbb{Z}$. Além disso, existem $r, s \in \mathbb{Z}$ tais que

$$ar + bs = d, \tag{1.5.8}$$

pois $d = mdc(a, b)$. Multiplicando 1.5.8 por k, tem-se

$$ark + bsk = dk = c.$$

Logo, $x = rk$ e $y = sk$ é uma solução de 1.5.7.

Corolário 1.3. *Quando $mdc(a, b) = 1$ a equação diofantina 1.5.7 sempre tem solução.*

Demonstração: De fato, pois para qualquer $c \in \mathbb{Z}$, tem-se que $1|c$. ■

Exemplo 1.18. A equação diofantina $3x + 7y = 43$ tem solução, pois $mdc(3, 7) = 1$ e $1|43$. Mas a equação $5x + 15y = 17$ não tem solução, já que $mdc(5, 15) = 5$ e $5 \nmid 17$.

O teorema anterior nos forneceu uma maneira de julgarmos se uma equação diofantina linear tem ou não solução. Mas, no caso de possuir solução, tem uma forma para determiná-las? Se sim, como? O próximo teorema responde a esses questionamentos.

Teorema 1.12. *Se (x_0, y_0) é uma solução particular da equação diofantina*

$$ax + by = c, \quad com \quad mdc(a, b) = 1,$$

então as demais soluções são da forma $x = x_0 + bt$ e $y = y_0 - at$, com $t \in \mathbb{Z}$.

Demonstração: Seja (x_0, y_0) uma solução particular da equação diofantina. Então

$$ax_0 + by_0 = c. \tag{1.5.9}$$

Seja agora (x, y) uma solução genérica da equação, isto é,

$$ax + by = c. \tag{1.5.10}$$

Subtraindo 1.5.9 de 1.5.10, tem-se

$$a(x - x_0) + b(y - y_0) = 0,$$

ou melhor

$$a(x - x_0) = b(y_0 - y). \tag{1.5.11}$$

De 1.5.11, decorre que

$$b|a(x - x_0) \quad \text{e} \quad a|b(y_0 - y).$$

Como $mdc(a, b) = 1$,

$$b|(x - x_0) \quad \text{e} \quad a|(y_0 - y).$$

Isto é, existem inteiros k e t tais que

$$y_0 - y = at \quad \text{e} \quad x - x_0 = bk. \tag{1.5.12}$$

Substituindo esses valores em 1.5.11, obtém-se $abk = bat$, o que resulta $k = t$, pois $ab \neq 0$. Retornando em 1.5.12, concluímos que

$$x = x_0 + bt \quad \text{e} \quad y = y_0 - at, \ \text{ com } \ t \in \mathbb{Z}$$

são as soluções da equação diofantina 1.5.10. ■

Corolário 1.4. *Se (x_0, y_0) é uma solução particular da equação diofantina*

$$ax + by = c, \quad com \quad mdc(a, b) = d,$$

então as demais soluções são da forma

$$x = x_0 + \frac{b}{d}t \text{ e } y = y_0 - \frac{a}{d}t, \text{ com } t \in \mathbb{Z}.$$

Demonstração: Basta notar que $mdc(\frac{a}{d}, \frac{b}{d}) = 1$ pelo teorema XX e $d|c$. ■

Exemplo 1.19. Resolva a equação diofantina $5x + 3y = 35$.
Solução: Note que $mdc(5, 3) = 1$ e, por isso, a equação tem solução. Além disso, $x = 1$ e $y = 10$ é uma solução particular da equação, daí, a solução geral é

$$x = 1 + 3t \quad \text{e} \quad y = 10 - 5t, \quad t \in \mathbb{Z}.$$

Exemplo 1.20. Resolva a equação diofantina $5x + 10y = 15$.
Solução: Como $mdc(5, 10) = 5$ e $5|15$, a equação diofantina tem solução. Uma solução particular é (1,1). Assim, a solução geral é:

$$x = 1 + \frac{10}{5}t \text{ e } y = 1 - \frac{5}{5}t \quad t \in \mathbb{Z}.$$

O próximo exemplo mostra como obter uma solução particular (e, pelo teorema x, uma solução geral) de uma equação diofantina pelo algoritmo de Euclides.

Exemplo 1.21. Resolva a equação diofantina $105x + 66y = 18$.
Solução: Como $mdc(105, 66) = 3$ e $3|18$, a equação diofantina tem solução. Dividindo-a pelo $mdc(105, 66)$, obtemos a equação

$$35x + 22y = 6, \quad \text{com } mdc(35, 22) = 1.$$

Faremos, então, as seguintes divisões (as mesmas utilizadas para concluir que o $mdc(35, 22) = 1$ pelo algoritmo de euclides):

$$\begin{array}{rcll} 35 & = & 22 \cdot 1 + 13 & \text{(de 35 por 22)} \\ 22 & = & 13 \cdot 1 + 9 & \text{(de 22 por 13)} \\ 13 & = & 9 \cdot 1 + 4 & \text{(de 13 por 9)} \\ 9 & = & 4 \cdot 2 + 1 & \text{(de 35 por 4)} \\ 4 & = & 2 \cdot 2 + 0 & \text{(de 4 por 2)} \end{array}$$

Podemos reescrever as quatro primeiras equações da seguinte forma:

$$\begin{array}{rcl} 35 - 22 \cdot 1 & = & 13 \\ 22 - 13 \cdot 1 & = & 9 \\ 13 - 9 \cdot 1 & = & 4 \\ 9 - 4 \cdot 2 & = & 1 \end{array}$$

Substituindo a primeira igualdade na segunda, o que se obtém, na terceira e, por último, o que se obtém, na quarta, ficamos com:

$$35 \cdot (-5) + 22 \cdot 8 = 1.$$

Multiplicando por 6, segue que

$$35 \cdot (-30) + 22 \cdot 48 = 6,$$

ou seja, $(-30, 48)$ é uma solução particular da equação $105x + 66y = 18$. Pelo teorema 1.12, a solução geral é

$$x = -30 + 22t \quad \text{e} \quad y = 48 - 35t, \quad \text{com} \quad t \in \mathbb{Z}.$$

1.6 Números Primos

Nesta seção, apresentaremos o importante Teorema Fundamental da Aritmética, bem como demonstraremos que o conjunto dos números primos é infinito.

Definição 1.6. Um número $p \in \mathbb{Z}\backslash\{1, -1, 0\}$ diz-se *primo* se $a|p$ implicar $a = \pm 1$ ou $a = \pm p$. Um número $d \in \mathbb{Z}\backslash\{1, -1, 0\}$ diz-se *composto* quando não é primo.

Note que os números $-1, 0, 1$ não são primos e nem são compostos. Da definição, decorre que se d é um número composto, então existem inteiros r e s, com $1 < r \leq s < d$, tais que $d = rs$.

Como p é primo se, e somente se, $-p$ é primo, na maioria dos resultados que faremos, consideraremos $p > 1$. Além disso, definiremos agora o segundo conjunto, que será usado no decorrer do livro para simplificar os enunciados:

$$\mathbb{P} = \{p \in \mathbb{N} : \text{ p é primo }\}.$$

O conjunto $\mathbb{P}^*$ representará o conjunto $\mathbb{P}\backslash\{2\}$.

Teorema 1.13. *Se $p|ab$ e p é primo, então $p|a$ ou $p|b$.*

Demonstração: Supondo que $p \nmid a$, mostremos que $p|b$. Seja $d = mdc(a, p)$, então $d|a$ e $d|p$. Mas $p \nmid a$ e p é primo, então $d \neq p$, isto é, $d = 1$. Assim, pelo teorema 1.5, o resultado segue.

Corolário 1.5. *Se p e p_i são primos, com $i \in \{1, 2, \cdots, n\}$, e $p|p_1p_2 \cdots p_n$ então $p = p_i$ para algum $i \in I_n$.*

Demonstração: Provaremos por indução sobre n. Para $n = 1$, o resultado é imediato. Supondo válido para n mostremos que vale para $n + 1$. Se $p|p_1p_2 \cdots p_np_{n+1}$ temos duas possibilidades:

i) $p|p_{n+1}$. Então $p = p_{n+1}$ e o resultado segue;

ii) $p \nmid p_{n+1}$, isto é, $mdc(p, p_{n+1}) = 1$. Pelo teorema 1.13, segue que $p|p_1p_2 \cdots p_n$ e, da hipótese de indução, decorre que $p = p_i$ para algum $i \in I_n$.

Logo, pelo princípio de indução, vale para todo n natural.

Teorema 1.14. *(Fundamental da Aritmética) Todo* $a \in \mathbb{Z}\backslash\{-1, 0, 1\}$ *pode ser escrito da forma*

$$a = up_1p_2 \cdots p_k, \quad com \quad p_1 \leq p_2 \leq ... \leq p_k,$$

onde $u = \pm 1$ *e* p_i *é primo* $\forall\ i \in I_k$. *Além disso, essa forma é única.*

Demonstração: Faremos por indução sobre a com $a > 1$, pois para $a < -1$ basta trocar $u = 1$ por $u = -1$. O resultado é válido para $a = 2$. Supondo válido para $a \in \{2, 3, ..., n\}$, mostremos que vale para $a = n + 1$. Se $n + 1$ é primo, então o resultado é imediato, senão, a é composto, isto é, $a = rs$, com $1 < r \leq s < n + 1$. Dessa forma, r e s estão nas condições da hipótese de indução e, por isso,

$$r = q_1q_2 \cdots q_m \quad \text{e} \quad s = p_1p_2 \cdots p_l,$$

com $p_i, q_i \in \mathbb{P},\ q_1 \leq ... \leq q_m$ e $p_1 \leq ... \leq p_l$. Assim,

$$n = q_1q_2 \cdots q_mp_1p_2 \cdots p_l.$$

Organizando, se necessário, tem-se $n = t_1t_2 \cdots t_{m+l}$, com $t_1 \leq t_2 \leq ... \leq t_{m+l}$ e $t_i \in \mathbb{P}$ para $i \in I_{m+l}$, ou seja, o resultado é válido para $n + 1$. Portanto, pelo princípio de indução, vale para todo $a \in \mathbb{N}$ maior do que 1.

Mostremos agora a unicidade. Para tanto, suponhamos que $a > 1$ admita duas formas:

$$a = p_1p_2 \cdots p_b \ \text{ e } \ a = q_1q_2 \cdots q_c.$$

Daí,

$$p_1p_2 \cdots p_b = q_1q_2 \cdots q_c. \tag{1.6.13}$$

Isto é, $p_1|q_1q_2 \cdots q_c$. Pelo corolário 1.5, tem-se

$$p_1 = q_i \tag{1.6.14}$$

para algum $i \in I_c$. Analogamente, tem-se que $q_1 | p_1 p_2 \cdots p_b$ e por isso

$$q_1 = p_j \tag{1.6.15}$$

para algum $j \in I_b$. Como, $q_1 \leq \cdots \leq q_c$ e $p_1 \leq \cdots \leq p_b$, decorre, por 1.6.14 e 1.6.15, que $q_1 = p_1$. Repetindo esse processo, temos de considerar dois casos:

1º caso: $b > c$.

Então chegaremos a

$$p_{c+1} p_{c+2} \cdots p_b = 1,$$

o que é absurdo, pois $p_i > 1$.

2º caso: $b < c$.

Então teremos

$$1 = q_{b+1} q_{b+2} \cdots q_c,$$

o que absurdo, pois $q_i > 1$.

Logo, por exclusão, $c = b$ e $q_i = p_i$ para todo $i \in I_b$, concluindo, assim, a demonstração. ■

Corolário 1.6. *Todo $a \in \mathbb{Z} \backslash \{-1, 0, 1\}$ pode ser escrito de modo único na forma*

$$a = u p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}, \quad com \quad p_1 < p_2 < \cdots < p_n,$$

onde $u = \pm 1$ e p_i é primo $\forall\ i \in I_n$.

Demonstração: O resultado segue imediatamente do teorema, basta juntar os termos repetidos, escrever na forma de potência e desconsiderar a possibilidade de $p_i = p_j$ para algum $i \neq j \in I_n$, pois são todos distintos. ■

Exemplo 1.22. Decomponha os números 60, 124 e 500 como produtos de fatores primos. *Solução:*

i) $60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5$;

ii) $124 = 2 \cdot 62 = 2 \cdot 2 \cdot 31 = 2^2 \cdot 31$;

iii) $500 = 5 \cdot 100 = 5 \cdot 4 \cdot 25 = 2^2 \cdot 5^3$;

iv) $666 = 2 \cdot 3 \cdot 111 = 2 \cdot 3 \cdot 3 \cdot 37 = 2 \cdot 3^2 \cdot 37$.

A decomposição de números em fatores primos, facilita a obtenção do máximo divisor comum destes números (ver exercício 16).

Teorema 1.15. *O conjunto dos números primos é infinito.*

Demonstração: Suponhamos que não fosse. Então

$$X = \{p_1, p_2, ..., p_n\}$$

conteria todos os primos. Seja $b = (p_1 p_2 \cdots p_n + 1) \in \mathbb{Z}$. Então, como $b \notin \{-1, 0, 1\}$, tem-se que existe um primo $p \in X$ tal que $p|b$. Como $p = p_i$ para algum $i \in I_n$, $p|p_1 p_2 \cdots p_n$. Assim, pelo teorema 1.1.ix, segue que $p|1$, ou seja, $p = \pm 1$. Contradição, pois p é primo. Logo, o conjunto dos números primos é infinito. ■

1.7 Exercícios

1. Mostre que o Princípio da Boa Ordem e o Princípio da Indução Finita (primeira e segunda forma) são equivalentes.
2. Mostre que o conjunto $X = \{x \in \mathbb{Z} : a < x < a + 1,\ a \in \mathbb{Z}\}$ é vazio.
3. Mostre, $\forall\ n \in \mathbb{N}$, que
   a) $1^3 + 3^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1)$;
   b) $n < 2^n$;
   c) $2^n < n$, se $n \geq 4$;
   d) $n(n^2 + 5)$ é múltiplo de 6.
4. Sejam $a, b \in \mathbb{Z}$. Mostre que $2x + 3y$ é divisível por 17 se, e só se, $9x + 5y$ também é.
5. Mostre que o quadrado de qualquer inteiro ímpar é da forma $8p + 1$.
6. Seja $m \in \mathbb{Z}$. Mostre que 3 divide um dos inteiros: m, $m + 2$ e $m + 4$.
7. Mostre que o quadrado de qualquer inteiro é da forma $3k$ ou $3k + 1$.
8. Mostre que
   a) o produto de números pares é par;
   b) o produto de números ímpares é ímpar;
   c) o produto de um número par por um número ímpar é par.
9. Mostre que a soma dos cubos de dois números inteiros consecutivos não é divisível por 2.
10. Seja $n \in \mathbb{Z}$. Mostre que n^2 é par $\Leftrightarrow$ n é par.

11. Sejam a e b números pares consecutivos. Mostre que $4|a$ ou $4|b$.

12. Sejam $a_1, a_2, ...a_n \in \mathbb{Z}$. Mostre que

$$mdc(a_1, a_2, ..., a_n) = d_n,$$

onde $mdc(a_1, a_2) = d_2$ e $mdc(d_{i-1}, a_i) = d_i$, para $i \in \{3, 4, ..., n\}$.

13. Sejam $a, b, c \in \mathbb{Z}$. Mostre que

a) $mdc(a, b) = mdc(a, c) = 1 \Leftrightarrow mdc(a, bc) = 1$;
b) $mdc(a, b) = 1 \Rightarrow mdc(a^n, b^n) = 1$, para todo n natural;
c) se $mdc(a, b) = 1$ e $c|(a + b)$, então $mdc(a, c) = mdc(b, c) = 1$;
d) $mdc(4a + 3, 5a + 4) = 1$.

14. Encontre a solução geral, se existir, das equações diofantinas:

a) $11x - 7y = 12$;
b) $2x = 13 + 8y$;
c) $3a - 13b = 25$;
d) $5x + 2y = 1$.

15. Seja $n \in \mathbb{Z}_+$. Se n não é quadrado perfeito, mostre que $\sqrt{n}$ é um número irracional.
(Um número é dito *quadrado perfeito* quando pode ser escrito como o quadrado de outro inteiro.)

16. Sejam $m = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}$ e $n = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$, onde q_i é primo para todo $i \in I_r$ e $a_1, \cdots, a_r, b_1 \cdots, b_r$ são inteiros maiores ou iguais a zero. Mostre que

$$mdc(m, n) = q_1^{c_1} \cdots q_r^{c_r}, \quad \text{com} \quad c_i = max\{a_i, b_i\}, \forall\ i \in I_r.$$

17. Mostre que, para todo inteiro positivo n, existem n inteiros consecutivos todos compostos.

18. Mostre que o conjunto

$$X = \{p \in \mathbb{P} : p = 4k + 3, \quad \text{para algum} \quad k \in \mathbb{Z}\}$$

é infinito.

19. Sejam $a \in \mathbb{Z}$, $n \in \mathbb{N}$ e p um número primo. Mostre que $p|a^n \Rightarrow p^n|a^n$.

20. Mostre que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida como

$$f((m, n)) = 2^{m-1}(2n - 1)$$

é uma função bijetiva.

Capítulo 2

Aritmética modular e os teoremas clássicos

Neste capítulo, estudaremos o conceito de congruência modular, o qual revolucionou o estudo da Aritmética, permitindo tratar de forma muito mais eficiente resultados de divisibilidade e possibilitando a obtenção de muitos outros. Foi o grande matemático Carl Friederich Gauss ($1777 - 1855$) quem introduziu este conceito, em 1801, no seu livro *Disquisitiones Aritmeticae* (Investigações na Aritmética), publicado quando ele tinha apenas 24 anos. Várias ideias usadas na Teoria dos Números foram introduzidas neste trabalho. Até mesmo o símbolo de congruência, com o qual trabalharemos, já era utilizado por Gauss naquela época. Trazendo simplicidade e elegância para a Álgebra, o trabalho de Gauss é a prova de que uma boa notação é a engrenagem principal de uma teoria matemática bem sucedida.

Neste capítulo, enunciaremos e demonstraremos alguns dos principais resultados de Teoria dos Números, concebidos frequentemente como Os Teoremas Clássicos: os Teoremas de Wilson, Fermat e Euler. O leitor é convidado a resolver todos os exercícios propostos, pois são de grande importância para o domínio dos conceitos.

2.1 Congruências Modulares

Baseando-se em divisibilidade, o conceito de congruência modular equivale à divisão da diferença de dois números. Ou seja, analisar se há a congruência entre dois números módulo n é analisar se n divide a diferença destes números. Como veremos, várias propriedades interessantes decorrem

da congruência de dois números, e alguns problemas, que eram difíceis de ser resolvidos antes do conceito, puderam ser solucionados de forma rápida e elegante. Este conceito nos permitirá, por exemplo, responder rapidamente as seguintes perguntas:

a) Qual o resto da divisão de 6^{1987} por 37?

b) Qual seria um fator primo ímpar de $5^{25} - 1$?

Para começarmos a tratar destes problemas, passemos à

Definição 2.1. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Dizemos que a *é congruente* (ou *côngruo*) a b *módulo* n e escrevemos

$$a \equiv b \ (mod\ n)$$

se, e somente se, n é um múltiplo de $a - b$, ou seja, se existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Se, porém, n não é múltiplo de $a - b$, então dizemos que a *é incongruente* a b *módulo* n, e denotamos por

$$a \not\equiv b \ (mod\ n).$$

Perceba que, ao considerar $n \in \mathbb{N}$, dizer que $a \equiv b \ (mod\ n)$, para $a, b \in \mathbb{Z}$, equivale a dizer que $n|(a - b)$. Se $n = 1$, então a congruência $a \equiv b \ (mod\ 1)$ é trivialmente verdadeira, pois todo número inteiro é múltiplo de 1 (basta tomar $k = a - b$ na definição). Se $n = 0$, então a congruência $a \equiv b \ (mod\ 0)$ equivale à igualdade $a = b$, obviamente. Se, por acaso, $n < 0$, na congruência $a \equiv b \ (mod\ n)$, podemos avaliar o caso equivalente $a \equiv b \ (mod\ -n)$. Por definição, o caso $n \leq 0$ é desconsiderado. Além disso, não consideraremos também o caso em que $n = 1$ nos enunciados e demonstrações dos teoremas que se sucederão.

Exemplo 2.1. $12 \equiv 2 \ (mod\ 5)$, pois $12 - 2 = 10$ e $5|10$. Também é verdade que $13 \equiv -2 \ (mod\ 5)$, pois $5|[13 - (-2)]$. Porém, $42 \not\equiv 13 \ (mod\ 2)$, pois $42 - 13 = 29$ e $2 \nmid 29$, e, como $9 \nmid 11$ e $11 = 13 - 2$, $13 \not\equiv 2 \ (mod\ 9)$.

Uma das principais propriedades da congruência, a de ser uma *relação de equivalência*, é estabelecida pela próxima proposição. Com ela, ganhamos a liberdade de realizar algumas manipulações de modo a obter mais propriedades que nos serão de grande utilidade adiante.

Proposição 2.1. *Sejam $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$. A congruência é uma relação reflexiva, simétrica e transitiva, isto é, as seguintes sentenças são verdadeiras:*

i) $a \equiv a \ (mod\ n)$;

ii) se $a \equiv b \ (mod\ n)$*, então* $b \equiv a \ (mod\ n)$*;*

iii) se $a \equiv b \ (mod\ n)$ *e* $b \equiv c \ (mod\ n)$*, então* $a \equiv c \ (mod\ n)$*.*

Demonstração: (i) Como $n|0$, segue-se que $n|(a-a)$, o que equivale a $a \equiv a \ (mod\ n)$. (ii) Se $a \equiv b \ (mod\ n)$, então $n|(a-b)$. Logo, $n|(b-a)$, ou seja, $b \equiv a \ (mod\ n)$. (iii) Se $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$, então $n|(a-b)$ e $n|(b-c)$. Logo, $n|[(a-b)+(b-c)]$, isto é, $n|(a-c)$, o que equivale a $a \equiv c \ (mod\ n)$. ■

Exemplo 2.2. Como $8 \equiv -2 \ (mod\ 5)$ e $-2 \equiv 3 \ (mod\ 5)$, por transitividade, $8 \equiv 3 \ (mod\ 5)$.

Além de ser uma relação de equivalência, a congruência tem propriedades aritméticas muito interessantes. O próxima teorema justifica a afirmação de que a congruência pode ser concebida como uma igualdade na maioria dos casos.

Teorema 2.1. *Se* $a, b, c, d \in \mathbb{Z}$ *e* $n \in \mathbb{N}$ *são tais que* $a \equiv b \ (mod\ n)$ *e* $c \equiv d \ (mod\ n)$*, então*

i) $a + c \equiv b + d \ (mod\ n)$*, em particular,* $a + k \equiv b + k \ (mod\ n)$*;*

ii) $a - c \equiv b - d \ (mod\ n)$*, em particular,* $a - k \equiv b - k \ (mod\ n)$*;*

iii) $ac \equiv bd \ (mod\ n)$*, em particular,* $ak \equiv bk \ (mod\ n)$*.*

Demonstração: (i) Como, por hipótese, $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, segue que $\exists\ k_1, k_2 \in \mathbb{Z}$ tais que $a - b = k_1 n$ e $c - d = k_2 n$. Somando estas igualdades membro a membro, agrupando e colocando n em evidência, ficamos com

$$a + c - (b + d) = (k_1 + k_2)n,$$

ou seja,

$$a + c \equiv b + d \ (mod\ n).$$

(ii) Analogamente, basta, ao invés de somar, subtrair as desigualdades. Assim, ficamos com

$$a - c - (b - d) = (k_1 - k_2)n,$$

isto é,

$$a - c \equiv b - d \ (mod\ n).$$

(iii) Como $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, ou melhor, $n|(a-b)$ e $n|(c-d)$, tem-se $n|(ac-bc)$ e $n|(bc-bd)$, donde

$$n|[(ac-bc)+(bc-bd)],$$

isto é, $n|(ac-bd)$, o que é equivalente a

$$ac \equiv bd \ (mod\ n).$$

■

Corolário 2.1. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Se $a \equiv b \ (mod\ n)$, então*

$$a^k \equiv b^k \ (mod\ n), \ \forall \ k \in \mathbb{N}.$$

Demonstração: A prova segue por indução sobre k. Se $k = 1$, o resultado é garantido pela hipótese. Suponhamos que o resultado é válido para k, isto é,

$$a^k \equiv b^k \ (mod\ n). \tag{2.1.1}$$

Pelo teorema 2.1.iii, podemos multiplicar 2.1.1 pela congruência $a \equiv b \ (mod\, n)$, que é válida por hipótese, obtendo

$$a^k a \equiv b^k b \ (mod\ n),$$

ou seja,

$$a^{k+1} \equiv b^{k+1} \ (mod\ n).$$

Pelo princípio de indução finita, o resultado segue. ■

Assim, tal qual como a igualdade, podemos somar, subtrair ou multiplicar membro a membro uma congruência, desde que o módulo seja o mesmo. Além disso, podemos "passar" uma parcela para o outro membro da congruência, trocando o sinal ao fazê-la. Basta notar que $(a+c)-b = a-(b-c)$ e, como

$$n|[(a+c)-b] \Leftrightarrow n|[a-(b-c)],$$

segue-se que

$$a+c \equiv b \ (mod\ n) \Leftrightarrow a \equiv b-c \ (mod\ n).$$

Exemplo 2.3. Mostrar que $246^{2015} \equiv 1 \ (mod\ 7)$.
Solução: Note que $246 = 6 \cdot 41$. Como $6 \equiv -1 \ (mod\ 7)$, podemos elevar esta congruência a 2015, donde

$$6^{2015} \equiv (-1)^{2015} \equiv -1 \ (mod\ 7).$$

Analogamente, $41 \equiv -1 \ (mod\ 7)$. Então, elevando esta congruência a 2015, obtemos

$$41^{2015} \equiv (-1)^{2015} \equiv -1 \ (mod\ 7).$$

Multipicando as duas congruências obtidas membro a membro, ficamos com

$$6^{2015} \cdot 41^{2015} \equiv (-1) \cdot (-1) \ (mod\ 7).$$

Como $6^{2015} \cdot 41^{2015} = (6 \cdot 41)^{2015} = 246^{2015}$, segue que

$$246^{2015} \equiv 1 \ (mod\ 7).$$

Um cuidado deve ser tomado. Apesar da recíproca ser verdadeira pelo item (iii) da proposição 2.1, a implicação

$$ac \equiv bc \ (mod\ n) \Rightarrow a \equiv b \ (mod\ n)$$

não é válida. Por exemplo, $6 \equiv 2 \ (mod\ 4)$, isto é, $2 \cdot 3 \equiv 2 \cdot 1 \ (mod\ 4)$, porém não é verdade que $3 \equiv 1 \ (mod\ 4)$. Para tratar disto, temos a

Proposição 2.2. *Se $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$ são tais que $ac \equiv bc \ (mod\ n)$, então $a \equiv b \ (mod\ \frac{n}{d})$, onde $d = mdc(c, n)$.*

Demonstração: Como,

$$ac \equiv bc \ (mod\ n),$$

por definição, existe $k \in \mathbb{Z}$ tal que

$$ac - bc = c(a - b) = kn.$$

Se dividirmos os dois últimos membros por d, o que podemos fazer, pois d divide n e d divide c (já que $d = mdc(c, n)$), teremos:

$$\frac{c}{d}(a - b) = k\frac{n}{d}.$$

Ou seja, $\frac{n}{d}$ divide $\frac{c}{d}(a - b)$. Mas, pelo teorema 1.7, $\frac{c}{d}$ e $\frac{n}{d}$ são primos entre si. Logo, $\frac{n}{d}$ divide $a - b$, isto é,

$$a \equiv b \ (mod\ \frac{n}{d}),$$

o que conclui a demonstração. ■

Exemplo 2.4. Mostrar que, para $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$, se $ac \equiv bc \ (mod\ n)$ e se c e n são primos entre si, então

$$a \equiv b \ (mod\ n).$$

Solução: Como n e c são primos entre si, deve ser $mdc(c, n) = 1$ e o resultado é imediato.

O próximo resultado é de grande importância, pois põe em termos simples o que significa dois inteiros a e b serem côngruos módulo n.

Teorema 2.2. *Dados $a, b \in \mathbb{Z}$, temos:*

$$a \equiv b \ (mod\ n) \ \Leftrightarrow \ a \text{ e } b \text{ deixam o mesmo resto na divisão por } n.$$

Demonstração: ($\Rightarrow$) Como $a \equiv b \ (mod\ n)$, existe $k \in \mathbb{Z}$ tal que

$$a - b = kn. \tag{2.1.2}$$

Além disso, o Algoritmo da Divisão nos garante a existência de $q, r \in \mathbb{Z}$, únicos, tais que

$$b = qn + r, \quad 0 \leq r < n. \tag{2.1.3}$$

Assim, de 2.1.2 e 2.1.3,

$$a - b = kn \Rightarrow a = b + kn \Rightarrow a = qn + r + kn \Rightarrow a = (q + k)n + r,$$

onde $0 \leq r < n$, isto é, r também é o resto da divisão de a por n.
($\Leftarrow$) Seja r o resto da divisão de a e b por n, isto é,

$$a = q_1 n + r \quad \text{e} \quad b = q_2 n + r, \quad 0 \leq r < n.$$

Daí,

$$r = a - q_1 n \quad \text{e} \quad r = b - q_2 n.$$

Assim,

$$a - q_1 n = b - q_2 n \Rightarrow a - b = q_1 n - q_2 n \Rightarrow a - b = (q_1 - q_2)n,$$

ou seja, $n|(a - b)$, o que equivale a $a \equiv b \ (mod\ n)$. ■

Exemplo 2.5. Mostrar que todo inteiro é côngruo, módulo n, a seu resto na divisão por n.
Solução: Seja $a \in \mathbb{Z}$. Pelo Algoritmo da Divisão,

$$a = qn + r, \quad 0 \leq r < n,$$

ou seja,

$$a - r = qn \Rightarrow n|(a - r) \Rightarrow a \equiv r \ (mod\ n).$$

Digamos que a e b sejam inteiros, n seja natural e r seja o resto da divisão de a por n. Pelo exemplo 2.5, vemos que, na congruência $a \equiv b \ (mod\ n)$, b será igual a r se cumprir a condição $0 \leq b < n$. Em todo caso, o teorema 2.2 garante que, se $a \equiv b \ (mod\ n)$, então $b = r + qn,\ q \in \mathbb{Z}$. Não é difícil verificar que, na verdade, se r é o resto de a na divisão por n, a congruência $a \equiv r + kn \ (mod\ n)$ é válida para rodo k inteiro. Nossa análise justifica as seguintes definições:

Definição 2.2. Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}$. Um inteiro b tal que $a \equiv b \ (mod\ n)$ é dito *resíduo de a módulo n.*

Definição 2.3. Dizemos que o conjunto $S = \{r_1, r_2, r_3, ..., r_n\}$ é um *Sistema Completo de Resíduos* (SCR) *módulo n* se são satisfeitas as condições:

i) $r_i \not\equiv r_j \ (mod\ n)$ sempre que $i \neq j, \quad i, j \in I_n$;

ii) para todo inteiro a, existe $i \in I_n$ tal que $a \equiv r_i \ (mod\ n)$.

Um tipo especial de SCR módulo n é quando todos os elementos do conjunto cumprem a condição de resto, isto é, $\forall\ r \in S,\ 0 \leq r < n$. Podemos indicar este caso chamando o conjunto de *Sistema Completo de Restos módulo n.*

Exemplo 2.6. Mostrar que o conjunto $S = \{0, 1, 2\}$ é um Sistema Completo de Restos módulo 3.
Solução: É claro que quaisquer dois elementos de S são incongruentes módulo 3. Devemos, portanto, mostrar que todo e qualquer número é congruente módulo 3 a um destes elementos. De fato, pelo Algoritmo da Divisão, segue-se que, para algum $k \in \mathbb{Z}$, n é de uma das seguintes formas:

i) $n = 3k$;

ii) $n = 3k + 1$;

iii) $n = 3k + 2$.

Em cada um dos casos, n será congruente a 0, 1 ou 2, respectivamente, como queríamos mostrar.

Com o seguinte lema, seremos capazes de demonstrar um fato interessante (o teorema 2.3) sobre os SCR's módulo n.

Lema 2.1. *Seja $n \in \mathbb{N}$. O conjunto $S = \{0, 1, 2, 3, ..., n-1\}$ é um Sistema Completo de Restos módulo n.*

Demonstração: Precisamos verificar as duas condições da definição 2.3 e, além disso, verificar que todos os elementos de S satisfazem a condição de resto. Tomando i e j em S, como $i, j < n$, temos:

$$0 \leq i < n \text{ e } 0 \leq j < n.$$

Assim,

$$0 \leq j < n \Rightarrow -n < -j \leq 0.$$

Somando à desigualdade anterior que envolve i, ficamos com

$$-n < i - j < n \Leftrightarrow |i - j| < n.$$

Daí, a menos que $i = j$, não existe $k \in \mathbb{Z}$ tal que $i - j = kn$, isto é, $i \not\equiv j \ (mod\ n)$, se $i \neq j$. Agora, pelo Algoritmo da Divisão, seja qual for $a \in \mathbb{Z}$ existem únicos q e r tais que

$$a = qn + r, \quad 0 \leq r < n.$$

Como $0 \leq r < n$, as possibilidades para r são os elementos de S. Pelo exercício 2.5, $a \equiv i \ (mod\ n)$ para algum $i \in S$. Por fim, como se vê facilmente, todos os elementos de S cumprem a condição de resto. Logo, S é um Sistema Completo de Restos módulo n. ■

Teorema 2.3. *Dado n natural, se o conjunto $R = \{r_1, r_2, r_3, ..., r_k\}$ é um SCR módulo n, então $k = n$.*

Demonstração: Como o conjunto S do lema 2.1 é um SCR módulo n, todo elemento de R é côngruo a algum dos elementos de S módulo n. Como são todos incongruentes módulo n, R tem, no máximo, n elementos, isto é, $k \leq n$. Analogamente, como, por hipótese, R é um SCR módulo n, todo elemento de S é côngruo a algum elemento de R. Como são todos incongruentes módulo n, S tem, no máximo, k elementos, isto é, $n \leq k$. Portanto, $n = k$. ■

O que este importante teorema nos diz é: fixado n, todo SCR módulo n tem exatamente n elementos, nem mais, nem menos. Fica fácil verificar então que qualquer conjunto com n elementos, dois a dois incongruentes módulo n, formam um SCR módulo n. Deixaremos esta tarefa como exercícios para o leitor (ver exercício 7).

Exemplo 2.7. O conjunto $S = \{3, 5, 9, 12, 16\}$ é um SCR módulo 5, pois todos os elementos são dois a dois incongruentes módulo 5 e S tem 5 elementos. No entanto, o conjunto $S \cup \{a\}$, com $a \in \mathbb{N} \backslash S$, não pode ser um SCR módulo 5, pois tem 6 elementos.

2.2 Congruências Lineares

Similarmente às equações diofantinas, as congruências que analisaremos agora admitem um *conjunto de soluções*.

Definição 2.4. Sejam $a, b, x \in \mathbb{Z}$ e $n \in \mathbb{N}$. Chamamos de *congruência linear* toda congruência da forma

$$ax \equiv b \ (mod\ n).$$

O conjunto dos x para os quais esta congruência é verdadeira é chamado de *conjunto solução* da congruência linear.

Como veremos mais adiante (proposição 2.3), uma congruência linear $ax \equiv b \ (mod\ n)$ tem solução se, e somente se, $mdc(a, n)$ divide b. Usaremos previamente este fato para dar os próximos exemplos.

Exemplo 2.8. $6x \equiv 2 \ (mod\ 3)$ é um exemplo de congruência linear. O conjunto solução desta congruência é vazio, pois $mdc(6, 3) = 3$ e $3 \nmid 2$, isto é, $6x \equiv 2 \ (mod\ 3)$ não tem solução.

Exemplo 2.9. A congruência linear $8x \equiv 4 \ (mod\ 6)$ tem solução, pois $mdc(8, 6) = 2$ e $2|4$. Uma das soluções é 2, visto que $6|(8 \cdot 2 - 4)$. Além desta, 8, 14, -4, ou qualquer número da forma $2 + 6k,\ k \in \mathbb{Z}$ também é solução da congruência, pois

$$8 \cdot 2 \equiv 4 \ (mod\ 6) \tag{2.2.4}$$

e

$$8 \cdot 6k \equiv 0 \ (mod\ 6). \tag{2.2.5}$$

Somando 2.2.4 com 2.2.5, obtemos

$$8 \cdot 2 + 8 \cdot 6k \equiv 4 + 0 \ (mod\ 6),$$

ou seja,

$$8 \cdot (2 + 6k) \equiv 4 \ (mod\ 6).$$

Note, por fim, que 5 também é solução da congruência $8x \equiv 4 \ (mod\ 6)$, porém, 5 não é da forma $2 + 6k$, que só gera números pares. Portanto, o conjunto

$$S' = \{2 + 6k : k \in \mathbb{Z}\}$$

não contém todas as soluções desta congruência.

Novamente, qualquer número da forma $5 + 6k,\ k \in \mathbb{Z}$, é solução da congruência linear do exemplo anterior. Para diferenciar as soluções das duas formas encontradas, temos a

Definição 2.5. Duas soluções x_1 e x_2 da congruência linear

$$ax \equiv b \ (mod\ n)$$

são ditas distintas se

$$x_1 \not\equiv x_2 \ (mod\ n).$$

Exemplo 2.10. Assim, na congruência $8x \equiv 4 \ (mod\ 6)$, 2 e 5 são duas soluções incongruentes módulo 6, pois $2 \not\equiv 5 \ (mod\ 6)$, e, portanto, são soluções distintas módulo 6. Porém, as soluções do conjunto S' são todas congruentes módulo 6, pois $2 + 6k_1 \equiv 2 + 6k_2 \ (mod\ 6), \ \forall \ k_1, k_2 \in \mathbb{Z}$.

Antes de passarmos aos teoremas, notemos que solucionar uma congruência linear é equivalente a solucionar uma equação diofantina. De fato, $ax \equiv b \ (mod\ n)$ significa que existe $y \in \mathbb{Z}$ tal que

$$ax - b = yn,$$

isto é,

$$ax - ny = b.$$

Sendo assim, o corolário 1.4 do teorema 1.12 nos fornece de imediato o seguinte resultado:

Proposição 2.3. *Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d = mdc(a, n)$. Se $d \nmid b$, então a congruência linear $ax \equiv b \ (mod\ n)$ não tem solução. Se $d|b$, então a congruência linear $ax \equiv b \ (mod\ n)$ possui infinitas soluções, que são dadas por*

$$S = \{..., -2 \cdot \frac{n}{d}, -1 \cdot \frac{n}{d}, x_0, x_0 + 1 \cdot \frac{n}{d}, 2 \cdot \frac{n}{d}, ...\} = \{x_0 + k \cdot \frac{n}{d} : k \in \mathbb{Z}\},$$

onde x_0 é uma solução particular.

Exemplo 2.11. Continuando com a congruência $8x \equiv 4 \ (mod\ 6)$, como $\frac{n}{d} = \frac{6}{2} = 3$, vemos que, ao encontrar a solução 2, a próxima solução seria $2 + 3 = 5$, que é uma solução distinta módulo 6. Continuando, a próxima seria $5 + 3 = 8$, que não é distinta de 2 módulo 6, pois $2 \equiv 8 \ (mod\ 6)$.

Se continuássemos o procedimento do exemplo anterior, obteríamos outras soluções que seriam congruentes módulo 6 a 2 ou a 5, isto é, soluções não distintas. O próximo resultado vem confirmar isto, pois demonstra que a congruência $8x \equiv 4 \ (mod\ 6)$ tem exatamente 2 soluções distintas módulo 6.

Teorema 2.4. *Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d = mdc(a, n)$. Se $d|b$, então a congruência linear*

$$ax \equiv b \ (mod \ n)$$

possui exatamente d soluções incongruentes módulo n.

Demonstração: Pela proposição anterior, $ax \equiv b \ (mod \ n)$ tem infinitas soluções. Precisamos mostrar que apenas d delas são incongruentes módulo d. Sejam $x_1 = x_0 + k_1\frac{n}{d}$ e $x_2 = x_0 + k_2\frac{n}{d}$ duas soluções. Se

$$x_1 \equiv x_2 \ (mod \ n),$$

isto é,

$$x_0 + k_1\frac{n}{d} \equiv x_0 + k_2\frac{n}{d} \ (mod \ n),$$

então, cancelando x_0, obtemos

$$k_1\frac{n}{d} \equiv k_2\frac{n}{d} \ (mod \ n).$$

Como $mdc(\frac{n}{d}, n) = \frac{n}{d}$ e $\frac{n}{d}$ divide n, sendo o resultado da divisão de n por $\frac{n}{d}$ igual a d, pela proposição 2.2, ficamos com

$$k_1 \equiv k_2 \ (mod \ d).$$

Ou seja, acabamos de demonstrar a implicação,

$$x_1 \equiv x_2 \ (mod \ n) \Rightarrow k_1 \equiv k_2 \ (mod \ d).$$

Por contraposição,

$$k_1 \not\equiv k_2 \ (mod \ d) \Rightarrow x_1 \not\equiv x_2 \ (mod \ n). \tag{2.2.6}$$

Em outras palavras, teremos soluções incongruentes, isto é,

$$x_1 \not\equiv x_2 \ (mod \ n),$$

se exigirmos que

$$k_1 \not\equiv k_2 \ (mod \ d).$$

Como só podemos ter d elementos incongruentes módulo d, que é a quantidade de elementos de um sistema completo de resíduos módulo d, teremos o antecedente da implicação 2.2.6 sendo satisfeito para exatamente d elementos dois a dois distintos, ou seja, teremos exatamente d soluções incongruentes módulo d. ■

Corolário 2.2. *Se $mdc(a,n) = 1$, a congruência linear $ax \equiv b \ (mod\ n)$ tem uma única solução módulo n.*

Exemplo 2.12. Resolver a congruência linear $12x \equiv 6 \ (mod\ 9)$ e encontrar soluções distintas módulo 9.
Solução: Como $mdc(12,9) = 3$, a congruência tem exatamente 3 soluções distintas módulo 9. Uma destas soluções é $x_0 = 2$, pois $12 \cdot 2 - 6 = 18 = 2 \cdot 9$. Como

$$\frac{9}{mdc(12,9)} = \frac{9}{3} = 3,$$

obtemos o conjunto de soluções

$$S = \{2 + 3k : k \in \mathbb{Z}\}.$$

Três soluções distintas módulo 9 são, por exemplo, 2, 5 e 8.

Exemplo 2.13. Resolver a congruência linear $3x \equiv 15 \ (mod\ 2)$.
Solução: Primeiramente, note que resolver esta congruência é equivalente a resolver a congruência $3x \equiv 1 \ (mod\ 2)$, pois $15 \equiv 1 \ (mod\ 2)$. Como 3 e 2 são primos entre si, a congruência tem solução única módulo 2. Uma solução particular é $x_0 = 1$. Assim, o conjunto solução desta congruência é

$$S = \{1 + 2k : k \in \mathbb{Z}\}.$$

Tal qual os inversos multiplicativos que o corpo $\mathbb{R}$ dos números reais possui na relação de igualdade, o conjunto $\mathbb{Z}$ dos inteiros possui inversos modulares na relação de congruência. É o que estabelece a próxima definição.

Definição 2.6. Dados inteiros $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, dizemos que $\bar{a}$ é um inverso de a módulo n se $\bar{a}$ é solução da congruência

$$ax \equiv 1 \ (mod\ n),$$

isto é, se

$$a\bar{a} \equiv 1 \ (mod\ n).$$

Assim, 2 é o inverso de 3 e 4 é seu próprio inverso módulo 5.

Exemplo 2.14. Mostrar que, $\forall\ n \in \mathbb{Z}$, 1 e $n-1$ são seus próprios inversos módulo n.
Solução: De fato, pois $1 \cdot 1 \equiv 1 \ (mod\ n)$, já que $n|0$, e $(n-1)^2 \equiv n^2 + 2n + 1 \equiv 1 \ (mod\ n)$, já que $n|[(n^2 + 2n + 1) - 1] = (n^2 + 2n)$.

2.3 Teoremas Clássicos

Nesta seção, demonstraremos três dos principais teoremas da Teoria dos Números, os clássicos teoremas de Wilson, Fermat e Euler, os quais serão de essencial importância para a obtenção do principal resultado deste livro: a Lei de Reciprocidade Quadrática. Não obstante, estes resultados são de praticidade inestimável, pois muito facilitam a obtenção das mais variadas verdades aritméticas, como veremos nos exemplos e como o leitor poderá verificar nos exercícios ao fim do capítulo.

2.3.1 O Teorema de Wilson

O seguinte lema será útil na demonstração do Teorema de Wilson.

Lema 2.2. *Mostre que, se $p \in \mathbb{P}$, então $a \in \mathbb{Z}$ é seu próprio inverso módulo p se, e somente se, $a \equiv 1 \ (mod\ p)$ ou $a \equiv -1 \ (mod\ p)$.*

Demonstração: a ser seu próprio inverso equivale a afirmar a congruência

$$a^2 \equiv 1 \ (mod\ p),$$

ou seja,

$$p|(a^2 - 1) \Leftrightarrow p|(a-1)\cdot(a+1) \Leftrightarrow p|(a-1) \text{ ou } p|(a+1),$$

o que, por sua vez, equivale a

$$a \equiv 1 \ (mod\ p) \text{ ou } a \equiv -1 \ (mod\ p).$$

■

Para que o leitor melhor compreenda a demonstração do Teorema de Wilson, o próximo exemplo aplicará a ideia para o caso específico em que $p = 11$.

Exemplo 2.15. Mostrar que $(11-1)! \equiv -1 \ (mod\ 11)$.
Solução: Primeiramente, vamos organizar os inversos $\bar{a}$ de cada a pertencente ao conjunto $R = \{1, 2, 3, ..., 10\}$ na seguinte tabela:

a	1	2	3	4	5	6	7	8	9	10
$\bar{a}$	1	6	4	3	9	2	8	7	5	10

Como podemos ver, 1 e 10 serem seus próprios inversos módulo 11 decorre do lema 2.2, pois estes são os únicos números do conjunto R côngruos a 1 e -1, respectivamente. Com exceção do 1 e do 10, portanto, vemos que

cada elemento do conjunto R é inverso de um único elemento de R distinto, ou seja, podemos fazer $\frac{11-3}{2}$ congruências entre elementos de $R\backslash\{1, 10\}$ da seguinte forma:

$$2 \cdot 6 \equiv 1 \ (mod\ 11);$$

$$3 \cdot 4 \equiv 1 \ (mod\ 11);$$

$$5 \cdot 9 \equiv 1 \ (mod\ 11);$$

$$7 \cdot 8 \equiv 1 \ (mod\ 11).$$

Multiplicando todas estas congruências membro a membro e reorganizando, obtemos

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv 1 \ (mod\ 11).$$

Por fim, multiplicando ambos os lados por 10 e utilizando transitividade com a congruência $10 \equiv -1 \ (mod\ 11)$, obtemos

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv 10 \equiv -1 \ (mod\ 11).$$

Como o lado esquerdo é igual a $10! = (11-1)!$, segue que

$$(11-1)! \equiv -1 \ (mod\ 11).$$

Teorema 2.5. *(de Wilson) Se $p \in \mathbb{P}$, então $(p-1)! \equiv -1 \ (mod\ p)$.*

Demonstração: A igualdade é verdadeira para $p = 2$ ou $p = 3$. Seja, então, $p \geq 5$. Para cada $a \in S = \{1, 2, 3, ..., p-1\}$, considere a congruência

$$ax \equiv 1 \ (mod\ p). \tag{2.3.7}$$

Como $p \in \mathbb{P}$ e $p \nmid a$, segue-se que $mdc(a, p) = 1$. Pelo corolário 2.2, a congruência 2.3.7 tem uma única solução módulo p, ou seja, para cada $a \in S$, existe um único $\bar{a} \in S$ tal que

$$a \cdot \bar{a} \equiv 1 \ (mod\ p).$$

Como os únicos elementos de S côngruos a 1 ou a -1 módulo p são os números 1 e $p-1$, pelo lema 2.2, 1 e $p-1$ são os únicos elementos de S que são seus próprios inversos módulo p. Assim, para cada $a \in S\backslash\{1, p-1\}$, existe $\bar{a} \in S\backslash\{1, p-1\}$, distinto, que é seu inverso. Podemos, então, formar $\frac{p-3}{2}$ pares $(a, \bar{a})$ tais que

$$a \cdot \bar{a} \equiv 1 \ (mod\ p).$$

Embora não saibamos quais, especificamente, são esses pares, podemos multiplicar todas as congruências e obter

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot ... \cdot p - 2 \equiv 1 \ (mod\ p).$$

Multiplicando ambos os membros da congruência acima por $p-1$, obtemos

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot ... \cdot p - 2 \cdot p - 1 \equiv 1 \cdot (p-1) \ (mod\ p).$$

Como $p - 1 \equiv -1 \ (mod\ p)$, por transitividade, obtemos

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot ... \cdot p - 2 \cdot p - 1 \equiv -1 \ (mod\ p),$$

ou melhor,

$$(p-1)! \equiv -1 \ (mod\ p),$$

como queríamos demonstrar. ■

Exemplo 2.16. Calcule o resto da divisão de 15! por 17.
Solução: Pelo Teorema de Wilson, $16! \equiv -1 \ (mod\ 17)$. Ora, $16! = 15! \cdot 16$ e $16 \equiv -1 \ (mod\ 17)$, ou, por simetria, $-1 \equiv 16 \ (mod\ 17)$. Portanto, usando transitividade,

$$16! \equiv 15! \cdot 16 \equiv -1 \equiv 16 \ (mod\ 17).$$

Como $mdc(16, 17) = 1$, podemos cancelá-lo de modo obter

$$15! \equiv 1 \ (mod\ 17).$$

Como 1 deixa resto 1 na divisão por 17, pelo teorema 2.2, o resto da divisão de 15! por 17 também é 1.

2.3.2 O Pequeno Teorema de Fermat

Lema 2.3. *Seja $r_i \in \mathbb{Z}$, para cada $i \in I_n$. Se $S = \{r_1, r_2, r_3, ..., r_n\}$ é um SCR módulo n, então $S_a = \{a \cdot r_1, a \cdot r_2, a \cdot r_3, ..., a \cdot r_n\}$ também é, desde que $mdc(a, n) = 1$.*

Demonstração: Como S_a tem n elementos, precisamos apenas mostrar que estes são incongruentes dois a dois. Então, para cada $i, j \in I_n$, considere a congruência

$$ar_i \equiv ar_j \ (mod\ n).$$

Como $mdc(a, n) = 1$, podemos cancelar o termo a e obter

$$r_i \equiv r_j \ (mod\ n).$$

Mas isso só acontece se $i = j$, pois $r_i, r_j \in S$, que é um SCR módulo n. Ou seja, os elementos de S_a são dois a dois incongruentes. Portanto, S_a é um SCR módulo n. ■

Teorema 2.6. *(Pequeno Teorema de Fermat) Se $p \in \mathbb{P}$, $a \in \mathbb{Z}$ e $p \nmid a$, então*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Demonstração: Como $p \in \mathbb{P}$ e $p \nmid a$, segue-se que $mdc(a, p) = 1$. Se considerarmos o SCR módulo n trivial $S = \{0, 1, 2, 3, ..., p-1\}$, o lema 2.3 nos garante que $S_a = \{0, a, 2a, 3a, ..., (p-1)a\}$ também é um SCR módulo n. Daí, cada elemento de S é congruente a um único elemento de S_a (estão numa correspondência biunívoca). É óbvio que $0 \equiv 0 \ (mod\ p)$. Por tanto, ainda temos uma correspondência biunívoca do conjunto $S\backslash\{0\}$ com o conjunto $S_a\backslash\{0\}$. Não sabemos quais são os pares de números congruentes gerados por esta correspondência, mas podemos multiplicar as congruências membro a membro. Fazendo isso, e reorganizando se necessário, obtemos

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \ (mod\ p),$$

ou seja,

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \cdot a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \ (mod\ p).$$

Como p não divide nenhum número da lista $1, 2, 3, ..., p-1$, deve ser primo com todos eles. Cancelando estes termos, ficamos com

$$a^{p-1} \equiv 1 \ (mod\ p),$$

como queríamos demonstrar. ■

Corolário 2.3. *Se $p \in \mathbb{P}$, então, para todo $a \in \mathbb{Z}$,*

$$a^p \equiv a \ (mod\ p).$$

Demonstração: Se $p|a$, então $a \equiv 0 \ (mod\ p)$, donde $a^p \equiv 0 \ (mod\ p)$. Usando transitividade nestas congruências, obtemos o resultado. Se, porém, $p \nmid a$, pelo Pequeno Teorema de Fermat,

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Multiplicando ambos os membros por a, obtemos

$$a^p \equiv a \ (mod\ p).$$

■

Exemplo 2.17. Calcule o resto da divisão de $97^{88} + 89^{96}$ por 8633.
Solução: observe que $8633 = 97 \cdot 89$. Por Fermat,

$$89^{96} \equiv 1 \ (mod\ 97) \tag{2.3.8}$$

e

$$97^{88} \equiv 1 \ (mod\ 89). \tag{2.3.9}$$

Ora, $97 \equiv 0 \ (mod\ 97)$. Logo, $97^{88} \equiv 0 \ (mod\ 97)$. Somando isto a 2.3.8, obtemos

$$89^{96} + 97^{88} \equiv 1 + 0 \equiv 1 \ (mod\ 97).$$

Analogamente, $89^{96} \equiv 0 \ (mod\ 89)$. Somando a 2.3.9, obtemos

$$89^{96} + 97^{88} \equiv 1 + 0 \equiv 1 \ (mod\ 89).$$

Ou seja,

$$89|(89^{96} + 97^{88} - 1) \text{ e } 97|(89^{96} + 97^{88} - 1).$$

Como $mdc(89, 97) = 1$, pelo teorema 1.6, segue-se que

$$89 \cdot 97|(89^{96} + 97^{88} - 1),$$

isto é,

$$97^{88} + 89^{96} \equiv 1 \ (mod\ 8633).$$

Portanto, $97^{88} + 89^{96}$ deixa resto 1 na divisão por 8633.

2.3.3 O Teorema de Euler

Antes de passarmos ao principal resultado desta seção, algumas definições terão de ser feitas, começando pela

Definição 2.7. Dizemos que um conjunto $R = \{r_1, r_2, r_3, ..., r_k\}$, onde $r_i \in \mathbb{Z}, \forall\ i \in I_k$, é um *Sistema Reduzido de Resíduos* (SRR) *módulo n* se as seguintes condições são satisfeitas:

i) $mdc(r_i, n) = 1, \forall\ i \in I_k$;

ii) $r_i \not\equiv r_j \ (mod\ n)$, se $i, j \in I_k$ e $i \neq j$; e

iii) para cada $m \in \mathbb{N}$ com $mdc(m, n) = 1$, $\exists\ i \in I_k$ tal que $m \equiv r_i \ (mod\ n)$.

Observe que podemos facilmente obter um SRR módulo n retirando os elementos r de um SCR módulo n que não satisfazem $mdc(r, n) = 1$. Os elementos restantes formarão, então, um SRR módulo n.

Exemplo 2.18. Como bem sabemos, o conjunto $S = \{0, 1, 2, 3, 4, 5\}$ é um SCR módulo 6. Dentre os elementos de S, os únicos não primos com 6 são os números: 0, pois $mdc(0, 6) = 6$; 2, pois $mdc(2, 6) = 2$; 3, pois $mdc(3, 6) = 3$; e 4, pois $mdc(4, 6) = 2$. "Retirando" estes elementos de S, ficamos com o conjunto $R = \{1, 5\}$, que é um sistema reduzido de resíduos módulo 6 (verifique!).

Passaremos a analisar um tipo especial de função, do qual definiremos a função que alicerça o importante Teorema de Euler (e que leva seu nome).

Definição 2.8. Denomina-se *função aritmética* toda função

$$f : \mathbb{N} \longrightarrow \mathbb{Z},$$

isto é, toda função definida em $\mathbb{N}$ com valores em $\mathbb{Z}$.

Duas funções aritméticas muito comuns em textos de Teoria dos Números são as apresentadas nos próximos exemplos.

Exemplo 2.19. A função $\mathcal{D} : \mathbb{N} \longrightarrow \mathbb{N}$, que associa cada número natural à quantidade de seus divisores positivos, isto é,

$$\begin{array}{rccc} \mathcal{D}: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \sharp\{d \in \mathbb{N} : d|n\}, \end{array}$$

é uma função aritmética.

Exemplo 2.20. A função $\mathcal{S} : \mathbb{N} \longrightarrow \mathbb{N}$, que associa cada número natural à soma de seus divisores, isto é,

$$\begin{array}{rccc} \mathcal{S}: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \displaystyle\sum_{\substack{d|n \\ d\in\mathbb{N}}} d, \end{array}$$

é uma função aritmética.

Definição 2.9. Uma função aritmética f é dita uma *função aritmética multiplicativa* quando satisfizer a igualdade

$$f(a \cdot b) = f(a) \cdot f(b),$$

desde que $a, b \in \mathbb{N}$ sejam primos entre si, e será uma *função aritmética completamente multiplicativa* quando satisfizer esta mesma igualdade para quaisquer $a, b \in \mathbb{N}$.

Exemplo 2.21. As funções $\mathcal{D}$ e $\mathcal{S}$ definidas nos exemplos 2.19 e 2.20 são funções aritméticas multiplicativas. A demonstração destes fatos será deixada como exercício (ver exercício 12).

A função aritmética multiplicativa mais importante com a qual trabalharemos é a denominada Função Phi de Euler, a qual definiremos a seguir.

Definição 2.10. Denotaremos por $\varphi(n)$ a quantidade de elementos de um SRR módulo n, isto é, $\varphi : \mathbb{N} \longrightarrow \mathbb{Z}$ é a função que relaciona um número natural com a quantidade de elementos do conjunto

$$R = \{r \in \mathbb{N} : 1 \leq r \leq n,\ mdc(r, n) = 1\}.$$

Esta função é denominada *Função Phi de Euler*.

Sendo assim, também podemos denotar um SRR módulo n arbitrário por $R = \{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$.

Exemplo 2.22. Calcular $\varphi(5)$, $\varphi(6)$, $\varphi(7)$ e $\varphi(8)$.
Solução: Como o conjunto $\{1, 2, 3, 4\}$ dos naturais menores do que 5 e primos com 5 tem 4 elementos, $\varphi(5) = 4$. Já o conjunto $\{1, 5\}$ dos divisores positivos não maiores do que 6 tem 2 elementos, donde $\varphi(6) = 2$. Analogamente, conclui-se que $\varphi(7) = 6$ e $\varphi(8) = 4$.

Exemplo 2.23. Note que, para todo $p \in \mathbb{P}$, todos os números da lista $1, 2, 3, 4, ..., p - 1$ são primos com p e menores do que ele. Assim,

$$p \in \mathbb{P} \Rightarrow \varphi(p) = p - 1.$$

Lema 2.4. *Se $R = \{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$ é um SRR módulo n, então $R_a = \{a \cdot r_1, a \cdot r_2, a \cdot r_3, ..., a \cdot r_{\varphi(n)}\}$ também é um SRR módulo n, desde que se tenha $mdc(a, n) = 1$.*

Demonstração: A demonstração é análoga ao lema 2.3 e será deixada como exercício (ver exercício 13). ■

Estamos prontos para demonstrar o Teorema de Euler. Note que a demonstração é muito semelhante com a do Pequeno Teorema de Fermat. O interessante é que este último pode ser facilmente obtido a partir do Teorema de Euler, como veremos no corolário 2.4.

Teorema 2.7. *(de Euler) Seja $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ tal que $mdc(a, n) = 1$. Então*

$$a^{\varphi(n)} \equiv 1\ (mod\ n).$$

Demonstração: Seja $R = \{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$ um SRR módulo n. Pelo lema 2.4, $R_a = \{a \cdot r_1, a \cdot r_2, a \cdot r_3, ..., a \cdot r_{\varphi(n)}\}$ também é um SRR módulo n. Assim, cada elemento de R é côngruo a um único elemento de R_a. Não sabemos quais são cada um dos pares de elementos congruentes, mas podemos multiplicar todas as congruências membro a membro, obtendo

$$ar_1 \cdot ar_2 \cdot ar_3 \cdot ... \cdot ar_{\varphi(n)} \equiv r_1 \cdot r_2 \cdot r_3 \cdot ... \cdot r_{\varphi(n)} \ (mod\ n),$$

isto é,

$$r_1 \cdot r_2 \cdot r_3 \cdot ... \cdot r_{\varphi(n)} \cdot a^{\varphi(n)} \equiv r_1 \cdot r_2 \cdot r_3 \cdot ... \cdot r_{\varphi(n)} \ (mod\ n). \qquad (2.3.10)$$

Como todos os números da lista $r_1, r_2, r_3, ..., r_{\varphi(n)}$ são primos com n, podemos cancelá-los na congruência 2.3.10, obtendo

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

■

Corolário 2.4. *(Pequeno Teorema de Fermat) Se $p \in \mathbb{P}$, $a \in \mathbb{Z}$ e $p \nmid a$, então*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Demonstração: Como $p \in \mathbb{P}$ e $p \nmid a$, $mdc(a, p) = 1$ e, além disso, $\varphi(p) = p - 1$. Portanto, pelo Teorema de Euler,

$$a^{p-1} \equiv 1 \ (mod\ p).$$

■

Exemplo 2.24. Calcular o resto da divisão de 7^{666} por 4.
Solução: Como $mdc(7, 4) = 1$ e $\varphi(4) = 2$, o Teorema de Euler garante que

$$7^2 \equiv 1 \ (mod\ 4).$$

Elevando ambos os membros à 333-potência, obtemos

$$(7^2)^{333} \equiv 7^{666} \equiv 1^{333} \equiv 1 \ (mod\ 4).$$

Portanto, o resto é igual a 1.

2.4 Exercícios

1. Verifique que, se $a \equiv b \ (mod\ n)$, então $mdc(a, n) = mdc(b, n)$.

2. Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}$. Em cada caso, determinar o resto da divisão de a por n.

   a) $a = 6^{1987},\ n = 37$;

   b) $a = 7^{10},\ n = 51$;

   c) $a = 13^{3k} + 17^{3k},\ n = 45$, com k ímpar.

3. Prove que, se a é um inteiro ímpar, então $a^2 \equiv 1 \ (mod\ 8)$.

4. Determine o resto na divisão por 7 do inteiro $x = 1! + 2! + 3! + ... + 100!$.

5. Prove que, para qualquer $a \in \mathbb{Z}$ é válido que $a^3 \equiv a \ (mod\ 6)$.

6. Determine um fator primo ímpar de $5^{25} - 1$.

7. Mostre que qualquer conjunto com n elementos dois a dois incongruentes módulo n formam um SCR módulo n.

8. Calcular o resto da divisão por 31 dos inteiros

   a) $2^{11^{28733}}$;

   b) $2^{13^{28733}}$.
   (Sugestão: faça por partes, em duas congruências.)

9. Mostre que, se $mdc(a, 35) = 1$, então $a^{12} \equiv 1 \ (mod\ 35)$.

10. Mostre que $18! + 1$ é divisível por 437.

11. Seja $a \in \mathbb{Z}$. Se $p, q \in \mathbb{P}$, distintos, são tais que

$$a^p \equiv a \ (mod\ q) \ \text{ e } \ a^q \equiv a \ (mod\ p),$$

    prove que

$$a^{pq} \equiv a \ (mod\ pq).$$

12. Mostre que as funções $\mathcal{D}$ e $\mathcal{S}$ definidas nos exemplos 2.19 e 2.20, respectivamente, são funções aritméticas multiplicativas.

13. Demonstre o lema 2.4.

14. Sejam $p \in \mathbb{P}$ e $\alpha \geq 1$ inteiros positivos. Mostre que $\varphi(p^\alpha) = p^\alpha + p^{\alpha-1}$.

15. Com três contraexemplos, refute a frase:

    A função phi de euler é uma função aritmética completamente multiplicativa.

16. Use o Teorema de Euler para determinar o resto da divisão de 3^{100} por 34.

Capítulo 3

Resíduos Quadráticos

Neste capítulo apresentaremos alguns resultados fundamentais para a realização das demonstrações do principal teorema deste livro: a Lei de Reciprocidade Quadrática. Iniciaremos com uma breve introdução sobre congruências quadráticas e alguns importantes teoremas relacionados a estas. Posteriormente, serão enunciados e demonstrados, o critério de Euler, o Lema de Gauss e outros resultados para a demonstração da Lei e, além destes, teoremas suplementares a esta.

3.1 Símbolo de Legendre, Critério de Euler e Lema de Gauss

Definição 3.1. Sejam $a, n \in \mathbb{Z}$ e primos entre si. Se $x^2 \equiv a \ (mod\ n)$ tiver solução, dizemos que a é um *resíduo quadrático módulo n*. Em caso contrário, isto é, $x^2 \not\equiv a \ (mod\ n)$ para todo inteiro x, dizemos que *a não é um resíduo quadrático módulo n*, ou ainda, a é um *resíduo não-quadrático*.

Exemplo 3.1. Na congruência $x^2 \equiv 2 \ (mod\ 7)$, tem-se que 2 é resíduo quadrático módulo 7, pois $mdc(2, 7) = 1$ e $7|(3^2 - 2)$, isto é, $x = 3$ é solução da congruência.

Exemplo 3.2. Determine se 13 é resíduo quadrático módulo 17.
Solução: Para resolvermos a questão, basta determinarmos se a congruência $x^2 \equiv 13 \ (mod\ 17)$ tem ou não solução. Como, para $x = 9$ temos que $9^2 \equiv 13 \ (mod\ 17)$, concluímos que 13 é resíduo quadrático módulo 17.

Teorema 3.1. *Se a congruência $x^2 \equiv a\ (mod\ p)$ tiver solução, ela tem exatamente duas soluções incongruentes módulo p, onde $p \in \mathbb{P}^*$, $mdc(p, a) = 1$ e $a \in \mathbb{Z}$.*

Demonstração: Seja x_1 uma solução de $x^2 \equiv a\ (mod\ p)$. Note que, $-x_1$ também é solução, pois $(-x_1)^2 = x_1^2 \equiv a\ (mod\ p)$. Mostremos que estas soluções são incongruentes módulo p, isto é, $x_1 \not\equiv -x_1\ (mod\ p)$.

Suponhamos que $x_1 \equiv -x_1\ (mod\ p)$, então $p|[x_1 - (-x_1)]$, o que implica que $p|2x_1$. Mas, $mdc(p, 2) = 1$, então $p|x_1$. Contudo, por hipótese x_1 é solução, então $x_1^2 \equiv a\ (mod\ p)$, ou seja, $p|(x_1^2 - a)$ e $p|x_1$, então $p|a$, o que é absurdo. Logo, $x_1 \not\equiv -x_1\ (mod\ p)$.

Agora demonstraremos que só existem duas soluções incongruentes módulo p. Para isso, suponhamos que y_1 seja outra solução da congruência, isto é, $y_1^2 \equiv a\ (mod\ p)$. Como x_1 também é solução, decorre que $x_1^2 \equiv a\ (mod\ p)$. Das propriedades de congruência, tem-se que

$$y_1^2 \equiv x_1^2\ (mod\ p) \Rightarrow p|(y_1^2 - x_1^2) \Rightarrow p|(y_1 + x_1)(y_1 - x_1),$$

ou seja,

$$y_1 \equiv -x_1\ (mod\ p)\ \text{ ou }\ y_1 \equiv x_1\ (mod\ p),$$

o que conclui a demonstração. ■

Deste modo, podemos afirmar que, ao determinarmos uma solução para uma congruência quadrática, estaremos obtendo, consequentemente, duas soluções.

Exemplo 3.3. Verifique se a congruência $3x^2 \equiv 12(mod\ 13)$ possui ou não solução.
Solução: Note que a congruência tem solução, pois para $x = 2$ tem-se que $3 \cdot 2^2 \equiv 12\ (mod\ 13)$. E, como $13 \in \mathbb{P}^*$ e $13|(12 - 12)$, pelo teorema 3.1, -2 também é solução.

Teorema 3.2. *(de Lagrange) Se $mdc(c_n, p) = 1$, com $p \in \mathbb{P}$, então a congruência $f(x) \equiv 0\ (mod\ p)$ tem, no máximo, n soluções, onde*

$$f(x) = c_n x^n + c_{n-1}x^{n-1} + ... + c_2 x^2 + c_1 x + c_0\ \ e\ c_i \in \mathbb{Z},\ i \in I_n.$$

Demonstração: Utilizemos o Princípio de Indução Finita sobre o grau do polinômio. Note que para $n = 1$ o resultado é válido, pois temos a congruência $c_1 x + c_0 \equiv 0\ (mod\ p)$, ou ainda,

$$c_1 x \equiv -c_0\ (mod\ p),$$

que possui uma única solução, pelo corolário 2.2 do teorema 2.4. Suponhamos válido para $n-1$, isto é, se $g(x)$ é um polinômio de grau $n-1$, então a congruência $g(x) \equiv 0 \ (mod\ p)$ tem, no máximo, $n-1$ soluções. Mostremos que é válido para n. Para tanto, suponhamos que não valha, isto é, que a congruência

$$c_n x^n + c_{n-1}x^{n-1} + ... + c_2 x^2 + c_1 x + c_0 \equiv 0 \ (mod\ p)$$

tenha (pelo menos) $n+1$ soluções incongruentes módulo p. Digamos que estas soluções sejam: $x_0, x_1, x_2, ..., x_n$. Fixando x_0, temos que

$$f(x) - f(x_0) \equiv 0 \ (mod\ p)$$

tem n soluções, pois $f(x_0) \equiv 0 \ (mod\ p)$. Mas,

$$\begin{aligned} f(x) - f(x_0) &= c_n x^n + ... + c_1 x + c_0 - (c_n x_0^n + ... + c_1 x_0 + c_0) \\ &= c_n(x^n - x_0^n) + c_{n-1}(x^{n-1} - x_0^{n-1}) + ... + c_1(x - x_0). \end{aligned}$$

Note que $(x - x_0)$ é um fator comum de cada parcela $c_i(x^i - x_0^i),\ i \in I_n$. Assim, para todo $i \in I_n$, tem-se

$c_i(x^i - x_0^i) = (x - x_0) \cdot p_{i-1}(x)$, onde $p_{i-1}(x)$ é um polinômio de grau $i-1$.

Seja

$$h(x) = \sum_{i=0}^{n-1} p_i(x).$$

Então $h(x)$ é um polinômio de grau $n-1$, com c_n sendo o coeficiente de x^{n-1}. Daí,

$$f(x) - f(x_0) = (x - x_0) \cdot h(x) \equiv 0 \ (mod\ p),$$

e isto significa que $p|(x - x_0) \cdot h(x)$. Como $p|(x - x_0) \Leftrightarrow x = x_0$, segue que $p|h(x)$ para todo $x_i,\ \ i \in I_n$. Ou seja, a congruência

$$h(x) \equiv 0 \ (mod\ p)$$

possui n soluções, contrariando a hipótese de indução. Logo, o resultado é válido para n e, pelo PIF, vale para todo polinômio satisfazendo as condições do teorema. ■

Antes de adentrarmos no próximo teorema, vejamos o

Exemplo 3.4. Seja $p = 11$. Averiguando quantos são os resíduos quadráticos módulo 11, obteremos:

$$\begin{array}{ll} 1^2 \equiv 1 \ (mod\ 11); & 6^2 \equiv 3 \ (mod\ 11); \\ 2^2 \equiv 4 \ (mod\ 11); & 7^2 \equiv 5 \ (mod\ 11); \\ 3^2 \equiv 9 \ (mod\ 11); & 8^2 \equiv 9 \ (mod\ 11); \\ 4^2 \equiv 5 \ (mod\ 11); & 9^2 \equiv 4 \ (mod\ 11); \\ 5^2 \equiv 3 \ (mod\ 11); & 10^2 \equiv 1 \ (mod\ 11). \end{array}$$

Assim, $1, 3, 4, 5$ e 9 são todos resíduos quadráticos módulo 11 e $2, 6, 7, 8$ e 10 não são.

Assim, pelo exemplo anterior, para $p = 11$, temos que $\frac{p-1}{2}$ números são resíduos quadráticos e $\frac{p-1}{2}$ não são. O próximo teorema será uma generalização deste resultado, isto é, para todo $p \in \mathbb{P}^*$.

Lema 3.1. *Seja $p \in \mathbb{P}^*$. Se $x, y \in \left\{1, 2, ..., \frac{p-1}{2}\right\}$, com $x \neq y$, então $x^2 \not\equiv y^2 \ (mod\ p)$.*

Demonstração: Suponhamos que $x^2 \equiv y^2 \ (mod\ p)$, então $p|(x^2 - y^2)$, ou ainda, $p|(x-y)(x+y)$. Logo, $p|(x-y)$ ou $p|(x+y)$. Mas $p \nmid (x+y)$, uma vez que $x + y < p$. Portanto, $p|(x-y)$, isto é, $x - y = 0$ ou $|x - y| \geq |p|$. Como a segunda não pode ocorrer, segue que $x = y$. ■

Definição 3.2. A função

$$\begin{array}{rccl} f: & \mathbb{R} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & \lfloor x \rfloor \ = \text{máx}\{m \in \mathbb{Z} : m \leq x\} \end{array}$$

é denominada *função maior inteiro.*

Teorema 3.3. *Seja $p \in \mathbb{P}^*$. Dentre os números $1, 2, 3, ..., p-1$, temos exatamente $\lfloor \frac{p}{2} \rfloor$ resíduos quadráticos módulo p.*

Demonstração: Pelo lema 3.1, sabemos que $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ são todos incongruentes módulo p. Note que, se $k = \frac{p-1}{2}$, então $p - k = \frac{p+1}{2}$. Assim,

$$k \in B = \left\{1, 2, ..., \frac{p-1}{2}\right\} \Rightarrow (p-k) \in X = \left\{\frac{p+1}{2}, \frac{p+3}{2}, ..., p-1\right\}.$$

Como $(p-k) \equiv -k \ (mod\ p)$, segue que $(p-k)^2 \equiv k^2 \ (mod\ p)$. Logo, para cada $x \in X$, existe um único $y \in B$ tal que $x^2 \equiv y^2 \ (mod\ p)$. Mas, para cada $k \in B$, temos que $x^2 \equiv j \ (mod\ p)$, com $j \in \{0, 1, 2, ..., p-1\}$. Logo, existem $\lfloor \frac{p}{2} \rfloor$ j's que são soluções da congruência $x^2 \equiv j \ (mod\ p)$, e isto mostra que existem exatamente $\lfloor \frac{p}{2} \rfloor$ resíduos quadráticos módulo p. ■

Exemplo 3.5. Do teorema anterior, decorre que 6 é a quantidade de resíduos quadráticos que o primo ímpar 13 possui, assim como 15 é a quantidade de resíduos quadráticos módulo 31 e 18 é a quantidade de resíduos quadráticos módulo 37. Deixamos a cargo do leitor a verificação destes fatos usando congruência.

Definição 3.3. (Símbolo de Legendre) Sejam $p, a \in \mathbb{Z}$ e $p \in \mathbb{P}^*$. O *Símbolo de Legendre de a módulo p*, denotado por $(\frac{a}{p})$ (lê-se: a legendre p), e definido como:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p; \\ 0, & \text{se } p|a; \\ -1, & \text{se } p \nmid a \text{ e } a \text{ não é um resíduo quadrático módulo } p. \end{cases}$$

Exemplo 3.6. Determine:

a) $\left(\frac{1}{7}\right)$;

b) $\left(\frac{2}{3}\right)$;

c) $\left(\frac{110}{11}\right)$.

Solução: Note que resolver os problemas acima consiste em analisar se $p|a$ ou se $p \nmid a$ e, neste caso, se a congruência $x^2 \equiv a \ (mod\ p)$ tem solução. Deste modo,

a) $x^2 \equiv 1 \ (mod\ 7)$, $7 \nmid 1$ e $x = 1$ é solução, então $\left(\frac{1}{7}\right) = 1$;

b) $x^2 \equiv 2 \ (mod\ 3)$, $3 \nmid 2$, mas 2 não é resíduo quadrático módulo 3, uma vez que a congruência não tem solução, então $\left(\frac{2}{3}\right) = -1$;

c) $x^2 \equiv 110 \ (mod\ 11)$, então $\left(\frac{110}{11}\right) = 0$, pois $11|110$.

Teorema 3.4. *(Critério de Euler) Se $p \in \mathbb{P}^*$ e $mdc(p, a) = 1$, então*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p).$$

Demonstração: Vamos considerar os casos em que a é ou não resíduo quadrático módulo p.

1º caso: a é resíduo quadrático módulo p.

Então a congruência

$$a \equiv x^2 \ (mod\ p)$$

tem solução. Seja x_0 uma solução. Então $p \nmid x_0$, pois $p|(a - x_0^2)$ e, se $p|x_0$, teríamos $p|x_0^2$, o que implica que $p|a$, contrariando a hipótese. Assim, por Fermat,

$$x_0^{p-1} \equiv 1 \ (mod\ p),$$

ou seja,

$$(x_0^2)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p). \tag{3.1.1}$$

Por outro lado, como $a \equiv x_0^2 \ (mod\ p)$, segue que

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \ (mod\ p). \tag{3.1.2}$$

Por transitividade em 3.1.2 e 3.1.1, temos que, se a é resíduo quadrático módulo p,

$$a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \ (mod\ p).$$

2º caso: a não é resíduo quadrático módulo p.

Como $p \in \mathbb{P}^*$ e $mdc(p, a) = 1$, por Fermat, temos que

$$(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \ (mod\ p),$$

isto é,

$$p|[a^{(\frac{p-1}{2})^2} - 1] = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1).$$

Como p é primo, segue que $p|(a^{\frac{p-1}{2}} - 1)$ ou $p|(a^{\frac{p-1}{2}} + 1)$, o que significa

$$a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p) \ \text{ ou } \ a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p). \tag{3.1.3}$$

Seja

$$X = \left\{ i^2 : 1 \leq i \leq \frac{p-1}{2} \right\}.$$

Note que $a \notin X$, pois todo elemento de X é resíduo quadrático. Mostremos que todo elemento de X satisfaz $x^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$. Para isso, seja $k \in X$. Então $k = i^2$ para algum $i \in I_{\frac{p-1}{2}}$. Como $|i| \leq \frac{p-1}{2}$, tem-se $p \nmid i$, donde, por Fermat, $i^{p-1} \equiv 1 \ (mod\ p)$, o que equivale a $(i^2)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$, ou seja, $k^{\frac{p-1}{2}} \equiv 1 \ (mod\ p), \forall\ k \in X$. Pelo Teorema de Lagrange, o polinômio $f(x) = x^{\frac{p-1}{2}} - 1 \equiv 0 \ (mod\ p)$ tem, no máximo, $\frac{p-1}{2}$ raízes. Mas X tem $\frac{p-1}{2}$ elementos que satisfazem $f(x) \equiv 0 \ (mod\ p)$. Portanto, vale a implicação

$$k \text{ satisfaz } x^{\frac{p-1}{2}} \equiv 1 \ (mod\ p) \ \Rightarrow \ k \in X. \tag{3.1.4}$$

Como $a \notin X$, por 3.1.4, segue que a não satisfaz $x^{\frac{p-1}{2}}$. Assim, por 3.1.3, segue que, se a não é resíduo quadrático módulo p,

$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \ (mod\ p).$$

■

Exemplo 3.7. Como $2^4 \equiv -1 \ (mod\ 17)$, segue que $2^8 \equiv 1 \ (mod\ 17)$. Assim, pelo Critério de Euler, $\left(\frac{2}{17}\right) \equiv 2^{\frac{17-1}{2}} \equiv 2^8 \equiv 1 \ (mod\ 17)$. E isso só é verdadeiro se

$$\left(\frac{2}{17}\right) = 1.$$

Da definição do símbolo de Legendre também chegamos a esse resultado, pois 6 é solução da congruência $x^2 \equiv 2 \ (mod\ 17)$.

Note que o critério de Euler nos fornece um meio de resolver o símbolo de Legendre sem usar congruência quadrática, apenas congruências de grau 1 que, em geral, são muito mais fáceis de serem resolvidas.

Teorema 3.5. *O Símbolo de Legendre é uma função completamente multiplicativa, isto é,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demonstração: Se $p|a$ ou $p|b$, então o resultado é imediato (por quê?). Consideremos que $p \nmid a$ e $p \nmid b$, ou seja, $p \nmid ab$. Assim, pelo Critério de Euler,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \ (mod\ p).$$

Mas,

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ (mod\ p),$$

então, por transitividade,

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ (mod\ p).$$

Porém, a congruência é verdadeira se, e somente se,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

■

Exemplo 3.8. Como o símbolo de Legendre é completamente multiplicativo, temos que

$$\left(\frac{8}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{4}{7}\right) = 1.$$

De fato, pois 3 é solução da congruência $x^2 \equiv 2 \ (mod\ 7)$ e 2 é solução da congruência $x^2 \equiv 4 \ (mod\ 7)$.

Teorema 3.6. *(Lema de Gauss) Sejam $a \in \mathbb{Z}$, $mdc(p,a) = 1$ e $p \in \mathbb{P}^*$. Consideremos os restos positivos da divisão por p dos números*

$$a, 2a, 3a, ..., \left(\frac{p-1}{2}\right)a.$$

Então,

$$\left(\frac{a}{p}\right) = (-1)^r,$$

onde r é o número dos restos positivos que são maiores do que $\frac{p}{2}$.

Demonstração: Digamos que $a_1, a_2, ..., a_s$ sejam os restos menores que $\frac{p}{2}$ e $b_1, b_2, ..., b_r$ são os maiores que $\frac{p}{2}$. Pelo exemplo 2.5, cada elemento da lista $1a, 2a, ..., \frac{p-1}{2}a$ é congruente a seu resto, isto é, a um a_i ou um b_j, com $i \in I_s$ e $j \in I_r$. Não sabemos quais são os pares de números congruentes gerados por esta correspondência, mas podemos multiplicar todas as congruências membro a membro, obtendo

$$1a \cdot 2a \cdot 3a \cdot ... \cdot \frac{p-1}{2}a \equiv a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r \ (mod\ p).$$

Reescrevendo a congruência e multiplicando por $(-1)^r$, obtemos

$$(-1)^r \cdot a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^r a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r \ (mod\ p). \qquad (3.1.5)$$

Nossa demonstração consistirá agora em mostrar que

$$a_1, a_2, ..., a_s, p-b_1, p-b_2, ..., p-b_r \qquad (3.1.6)$$

são, a menos da ordem, os números $1, 2, ..., \frac{p-1}{2}$. Uma vez que $\frac{p}{2} \leq b_j < p$, multiplicando por -1 e somando p a todos os membros da desigualdade, obtemos:

$$p - p < p - b_j < p - \frac{p}{2} = \frac{p}{2},$$

isto é, $1 \leq p - b_j \leq \frac{p-1}{2}$. Assim, basta mostrar que os números da lista 3.1.6 são todos incongruentes módulo p.

Para $i \in I_s$ e $j \in I_r$, suponha que $a_i \equiv b_j \ (mod\, p)$. Então $p|(a_i - b_j)$, o que é absurdo, pois $|a_i - b_j| \leq p$ e $a_i \neq b_j$. Logo, $a_i \not\equiv b_j \ (mod\ p)$. Além disso, $a_i \not\equiv p - b_j \ (mod\, p)$, $\forall\ i \in I_s$ e $j \in I_r$. A prova disso é que, se existissem $i \in I_s$ e $j \in I_r$ tais que $a_i \equiv p - b_j \ (mod\ p)$, então, como $p \equiv 0 \ (mod\ p)$, teríamos $a_i \equiv -b_j \ (mod\ p)$. Mas isto também é absurdo, pois a_i e b_j são côngruos a um dos elementos do conjunto $\{1a, 2a, ..., \frac{p-1}{2}a\}$ e $mdc(a,p) = 1$, o que nos fornece, após manipulações utilizando as propriedades de congruência,

$k \equiv -t \ (mod\ p)$ com $k, t \in \{1, 2, ..., \frac{p-1}{2}\}$. Portanto, os números da lista 3.1.6 são os mesmos elementos da lista $1, 2, ..., \frac{p-1}{2}$. Logo, por reflexividade,

$$a_1 a_2 \cdots a_s (p - b_1)(p - b_2) \cdots (p - b_r) \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot \left(\frac{p-1}{2}\right) \ (mod\ p),$$

o que, eliminando as parcelas côngruas a 0 após o desenvolvimento do produto do membro esquerdo, equivale a

$$(-1)^r a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r \equiv \left(\frac{p-1}{2}\right)! \ (mod\ p).$$

Por transitividade com a congruência 3.1.5,

$$(-1)^r a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \ (mod\ p).$$

Eliminando $(\frac{p-1}{2})!$ em ambos os membros (por que podemos fazer isso?), obtemos

$$(-1)^r a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p).$$

Multiplicano ambos os membros por $(-1)^r$, teremos

$$a^{\frac{p-1}{2}} \equiv (-1)^r \ (mod\ p).$$

Mas, pelo Critério de Euler,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p).$$

Assim,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^r \ (mod\ p),$$

cuja validade implica

$$\left(\frac{a}{p}\right) = (-1)^r,$$

como queríamos demonstrar. ■

Exemplo 3.9. Tomemos $a = 3$ e $p = 11$ no Lema de Gauss. Calculando os restos módulo 11 dos múltiplos de 3

$$1 \cdot 3, \ 2 \cdot 3, \ 3 \cdot 3, \ 4 \cdot 3 \text{ e } 5 \cdot 3,$$

temos:

$$1 \cdot 3 \equiv 3 \ (mod\ 11); \quad 4 \cdot 3 \equiv 1 \ (mod\ 11);$$
$$2 \cdot 3 \equiv 6 \ (mod\ 11); \quad 5 \cdot 3 \equiv 4 \ (mod\ 11).$$
$$3 \cdot 3 \equiv 9 \ (mod\ 11);$$

Dentre estes restos, apenas 6 e 9 são maiores do que $\frac{11}{2}$, ou seja, $r = 2$. Assim, pelo Lema de Gauss,

$$\left(\frac{3}{11}\right) = (-1)^2 = 1.$$

3.2 Suplementos à Lei de Reciprocidade Quadrática

Os dois próximos teoremas que serão apresentados são conhecidos como teoremas suplementares da Lei de Reciprocidade Quadrática. Pelo teorema 3.5, para analisar o caráter quadrático de um inteiro a, basta o fazer para cada um de seus fatores. Com a Lei em mãos, ficará bem mais fácil determinar o valor do Símbolo de Legendre. Porém, esta não enquadra todos os casos, pois, nada podemos afirmar sobre o caráter quadrático dos números -1 e 2 a partir da Lei, nem possuímos ferramentas que tornem esta análise simplificada. Portanto, os próximos teoremas são fundamentais para a determinação de resíduos quadráticos, de modo que conheçamos o caráter quadrado de qualquer inteiro a em relação a um p primo ímpar qualquer.

Teorema 3.7. *Se $p \in \mathbb{P}^*$, então*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & se \quad p \equiv \ \ 1 \ (mod\ 4); \\ -1, & se \quad p \equiv -1 \ (mod\ 4). \end{cases}$$

Demonstração: Pelo Algoritmo da Divisão, na divisão por 4, todos os inteiros são da forma $4k, 4k+1, 4k+2$ ou $4k+3$. Como p é ímpar, as possibilidades se reduzem a $4k+1$ ou $4k+3$. É fácil ver que $p = 4k+1$ equivale a $p \equiv 1 \ (mod\ 4)$ e que $p = 4k+3$ equivale a $p \equiv 3 \equiv -1 \ (mod\ 4)$. Vamos analisar o valor de $(-1)^{\frac{p-1}{2}}$ em cada um destes casos.

1º caso: $p = 4k+1$.

Então $p - 1 = 4k$, isto é, $\frac{p-1}{2} = 2k$ é par. Daí, $(-1)^{\frac{p-1}{2}} = 1$. Pelo Critério de Euler,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p),$$

ou seja,

$$\left(\frac{-1}{p}\right) = 1, \text{ se } p \equiv 1 \ (mod\ 4).$$

2º caso: $p = 4k + 3$.

Então $p - 1 = 4k + 2 = 2(2k + 1)$, isto é, $\frac{p-1}{2} = 2k + 1$ é ímpar. Daí, $(-1)^{\frac{p-1}{2}} = -1$. Pelo Critério de Euler,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \ (mod\ p),$$

ou seja,

$$\left(\frac{-1}{p}\right) = -1, \text{ se } p \equiv -1 \ (mod\ 4).$$

■

Exemplo 3.10. O teorema 3.7 nos fornece $\left(\frac{-1}{13}\right) = 1$, pois $13 \equiv 1 \ (mod\ 4)$. De fato, -1 é um resíduo quadrático módulo 13, pois 5 é solução da congruência $x^2 \equiv -1 \ (mod\ 13)$. E, pelo mesmo teorema, $\left(\frac{-1}{7}\right) = -1$, já que $7 \equiv 3 \ (mod\ 4)$. Com efeito, a congruência $x^2 \equiv -1 \ (mod\ 7)$ não tem solução, pois, pelo Algoritmo da Divisão, x é da forma

$$7k, 7k + 1, ..., 7k + 5 \text{ ou } 7k + 6.$$

Assim, $x^2 + 1$ é da forma

$$7r + 1, 7r + 2, 7r + 3 \text{ ou } 7r + 5,$$

e, em nenhum destes casos, $7|(x^2 + 1)$. Por isso, pela definição do símbolo de Legendre, $\left(\frac{-1}{7}\right) = -1$.

A próxima proposição será útil em dois dos teoremas que se sucederão.

Proposição 3.1. *Seja n um natural ímpar maior do que 2. Então vale a igualdade*

$$1 + 2 + 3 + ... + \frac{n-1}{2} = \frac{n^2 - 1}{8}.$$

Demonstração: Será deixada como exercício (ver exercício 9). ■

Teorema 3.8. *Se* $p \in \mathbb{P}^*$*, então*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & se \quad p \equiv \pm 1 \ (mod\ 8); \\ -1, & se \quad p \equiv \pm 3 \ (mod\ 8). \end{cases}$$

Demonstração: Pelo Critério de Euler, $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}$. Mostraremos que a validade da congruência

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \ (mod\ p) \tag{3.2.7}$$

será suficiente para, por transitividade, concluirmos o teorema. Para isto, consideraremos todos os possíveis restos de p na divisão por 8. Mas antes, vamos demonstrar que a congruência 3.2.7 é verdadeira.

Seja $i \in \{1, 2, 3, ..., \frac{p-1}{2}\}$. Então, se i é par, segue que

$$i \equiv 2k \equiv 2k \cdot (-1)^{2k} \equiv i \cdot (-1)^i \ (mod\ p).$$

Se, porém, i é ímpar, segue que

$$p - i \equiv p - (2k+1) \equiv -(2k+1) \equiv (-1)^{2k+1} \cdot (2k+1) \equiv (-1)^i \cdot i \ (mod\ p).$$

Ou seja, para números pares, podemos afirmar congruências do tipo

$$i \equiv i \cdot (-1)^i \ (mod\ p), \tag{3.2.8}$$

e, para números ímpares, podemos formar congruências do tipo

$$p - i \equiv (-1)^i \cdot i \ (mod\ p). \tag{3.2.9}$$

Perceba que, em ambos os tipos, 3.2.8 ou 3.2.9, os números dos membros esquerdos das congruências são sempre números pares. Mais ainda, estes números são $2, 4, 6, ..., p-1$. Assim, multiplicando todas essas $\frac{p-1}{2}$ congruências membro a membro, obtemos

$$2 \cdot 4 \cdot 6 \cdot ... \cdot (p-1) \equiv 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2} \cdot (-1)^1 \cdot (-1)^2 \cdot ... \cdot (-1)^{\frac{p-1}{2}} \ (mod\ p),$$

ou seja,

$$2 \cdot 4 \cdot 6 \cdot ... \cdot (p-1) \equiv \left(\frac{p-1}{2}\right)! (-1)^{(1+2+...+\frac{p-1}{2})} \ (mod\ p).$$

Mas $2 \cdot 4 \cdot 6 \cdot ... \cdot (p-1) = 2^{\frac{p-1}{2}} (\frac{p-1}{2})!$ e, pela proposição 3.1, $1+2+...+\frac{p-1}{2} = \frac{p^2-1}{8}$. Assim,

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)! \ (mod\ p).$$

Cancelando o fator $(\frac{p-1}{2})!$ em ambos os membros, obtemos o resultado.

Agora, precisamos mostrar que

$$(-1)^{\frac{p^2-1}{8}} = 1, \text{ se } p \equiv \pm 1 \ (mod\ 8)$$

e

$$(-1)^{\frac{p^2-1}{8}} = -1, \text{ se } p \equiv \pm 3 \ (mod\ 8).$$

Como p é ímpar, pelo Algoritmo da Divisão, p é de uma das seguintes formas: $8k+1, 8k+3, 8k+5$ ou $8k+7$. Vamos analisar cada um destes quatro casos e, em cada um deles, utilizaremos a igualdade

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8}. \tag{3.2.10}$$

1º caso: $p = 8k+1$.

Então $p-1 = 8k+1-1 = 8k$ e $p+1 = 8k+1+1 = 8k+2$. Substituindo em 3.2.10, obtemos

$$\frac{8k(8k+2)}{8} = \frac{8 \cdot 2k(4k+1)}{8} = 2(4k^2+k).$$

Assim, se $p = 8k+1$, então $\frac{p^2-1}{8}$ é par. Portanto,

$$(-1)^{\frac{p^2-1}{8}} = 1, \text{ se } p \equiv 1 \ (mod\ 8).$$

2º caso: $p = 8k+3$.

Então $p-1 = 8k+3-1 = 8k+2$ e $p+1 = 8k+3+1 = 8k+4$. Substituindo em 3.2.10, obtemos

$$\frac{(8k+2)(8k+4)}{8} = \frac{8 \cdot (4k+1)(2k+1)}{8} = (4k+1)(2k+1).$$

Assim, se $p = 8k+3$, então $\frac{p^2-1}{8}$ é ímpar (ver exercício 8 do capítulo 1). Portanto,

$$(-1)^{\frac{p^2-1}{8}} = -1, \text{ se } p \equiv 3 \ (mod\ 8).$$

3º caso: $p = 8k+5$.

Então $p-1 = 8k+5-1 = 8k+4$ e $p+1 = 8k+5+1 = 8k+6$. Substituindo em 3.2.10, obtemos

$$\frac{(8k+4)(8k+6)}{8} = \frac{8 \cdot (2k+1)(4k+3)}{8} = (2k+1)(4k+3).$$

Assim, se $p = 8k+5$, então $\frac{p^2-1}{8}$ é ímpar. Portanto,

$$(-1)^{\frac{p^2-1}{8}} = 1, \text{ se } p \equiv 5 \equiv -3 \ (mod\ 8).$$

4^o caso: $p = 8k + 7$.

Então $p - 1 = 8k + 7 - 1 = 8k + 6$ e $p + 1 = 8k + 7 + 1 = 8k + 8$. Substituindo em 3.2.10, obtemos

$$\frac{(8k+6)(8k+8)}{8} = \frac{8 \cdot 2(4k+3)(k+1)}{8} = 2(4k+3)(k+1).$$

Assim, se $p = 8k + 7$, então $\frac{p^2-1}{8}$ é par. Portanto,

$$(-1)^{\frac{p^2-1}{8}} = 1, \text{ se } p \equiv 7 \equiv -1 \ (mod\ 8),$$

o que conclui o teorema.

Exemplo 3.11. Do teorema 3.8, segue que $\left(\frac{2}{5}\right) = -1$ e $\left(\frac{2}{7}\right) = 1$, pois $5 \equiv -3 \ (mod\ 8)$ e $7 \equiv -1 \ (mod\ 8)$. Esse é o mesmo resultado obtido através da definição do símbolo. Com efeito, a congruência $x^2 \equiv 2 \ (mod\ 5)$ não tem solução, pois o Algoritmo da Divisão garante que x é da forma

$$5t, 5t + 1, 5t + 2, 5t + 3 \text{ ou } 5t + 4.$$

Daí, $x^2 - 2$ é da forma

$$5m + 2, 5m + 3 \text{ ou } 5m + 4$$

e nenhum destes números é múltiplo de 5, isto é, $\left(\frac{2}{5}\right) = -1$. Por outro lado, 3 é solução da $x^2 \equiv 2 \ (mod\ 7)$ e, por isso, $\left(\frac{2}{7}\right) = 1$.

3.3 A Lei de Reciprocidade Quadrática

Nesta seção apresentaremos um importante teorema que nos ajudará a determinar a solução para o símbolo de Legendre. Conhecendo o valor para $\left(\frac{p}{q}\right)$, será que temos condições de determinarmos $\left(\frac{q}{p}\right)$? A Lei mostrará em qual caso isso é possível.

O próximo resultado é fundamental para a demonstração da Lei. Para demonstrá-lo, utilizaremos alguns resultados, tais como o Algoritmo da Divisão e o Lema de Gauss. Pedimos ao leitor, caso não recorde, que reveja estes teoremas.

Teorema 3.9. *Sendo* $M = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \left\lfloor \frac{3a}{p} \right\rfloor + ... + \left\lfloor \frac{p-1}{2} \cdot \frac{a}{p} \right\rfloor$, *a um inteiro ímpar e* $p \in \mathbb{P}^*$, *tal que* $mdc(p, a) = 1$, *temos*

$$\left(\frac{a}{p}\right) = (-1)^M.$$

Demonstração: Nossa demonstração consiste, inicialmente, em determinar os restos módulo p de $Y_a = \{a, 2a, ..., \frac{p-1}{2}a\}$. Para isso, apliquemos o Algoritmo da Divisão para cada elemento do conjunto Y_a:

$$\begin{aligned} a &= p\left\lfloor \frac{a}{p} \right\rfloor + r_1 \\ 2a &= p\left\lfloor \frac{2a}{p} \right\rfloor + r_2 \\ 3a &= p\left\lfloor \frac{3a}{p} \right\rfloor + r_3 \\ &\vdots \\ \frac{p-1}{2}a &= p\left\lfloor \frac{p-1}{2}\cdot\frac{a}{p} \right\rfloor + r_{\frac{p-1}{2}} \end{aligned}$$

Perceba que cada $r_1, r_2, ..., r_{\frac{p-1}{2}}$ são os a_i e b_j definidos na demonstração do Lema de Gauss (com a característica de serem menores do que $\frac{p}{2}$ e maiores do que $\frac{p}{2}$, respectivamente). Agora, somando membro a membro cada uma das igualdades acima, obtemos

$$a\left(1 + ... + \frac{p-1}{2}\right) = p\left(\left\lfloor \frac{a}{p} \right\rfloor + ... + \left\lfloor \frac{p-1}{2}\cdot\frac{a}{p} \right\rfloor\right) + r_1 + ... + r_{\frac{p-1}{2}},$$

o que, pela proposição 3.1, equivale a

$$\frac{p^2-1}{8}\cdot a = p\left(\left\lfloor \frac{a}{p} \right\rfloor + ... + \left\lfloor \frac{p-1}{2}\cdot\frac{a}{p} \right\rfloor\right) + r_1 + ... + r_{\frac{p-1}{2}}.$$

Agora, seja $I = a_1 + a_2 + ... + a_s$ e $S = b_1 + b_2 + ... + b_r$, então

$$\frac{p^2-1}{8}\cdot a = pM + I + S. \tag{3.3.11}$$

Mas, como verificamos na demonstração do Lema de Gauss, os números $a_1, a_2, ..., a_s, p-b_1, p-b_2, p-b_3, ..., p-b_r$ são, a menos da ordem, os números $1, 2, 3, ..., \frac{p-1}{2}$. Portanto,

$$1 + 2 + ... + \frac{p-1}{2} = a_1 + a_2 + ... + a_s + rp - (b_1 + b_2 + ... + b_r).$$

Daí,

$$\frac{p^2-1}{8} = I + rp - S. \tag{3.3.12}$$

Logo, subtraindo 3.3.12 de 3.3.11, temos que

$$\frac{p^2-1}{8}(a-1) = p(M-r) + 2S.$$

Como a é ímpar por hipótese, segue que $\frac{(p^2-1)}{8} \cdot (a-1)$ é par, ou seja, $p(M-r)+2S$ é par. Como $2S$ é par, segue que $M-r$ também é par. Portanto M e r possuem a mesma paridade (são ambos pares ou ambos ímpares) e, pelo Lema de Gauss, sabemos que $\left(\frac{a}{p}\right) = (-1)^r$. Logo,

$$\left(\frac{a}{p}\right) = (-1)^M.$$

■

A Lei de Reciprocidade Quadrática é um importante resultado da Teoria dos Números que permite determinar soluções para congruências quadráticas. Foi conjecturada por Leonhard P. Euler (1707−1783) em 1783 e demonstrada pela primeira vez por Adrien-Marie Legendre (1752−1833) em 1785 para um caso particular e utilizando regras de inferências informais (não demonstradas). A Lei é um dos resultados favoritos de Gauss, que o demonstrou formalmente pela primeira vez em seu livro *Disquisitiones Arithmeticae* de 1801 (o mesmo no qual introduziu o conceito e a notação de congruência, como já comentado no capítulo 2). Neste, Gauss realizou 8 demonstrações diferentes para o teorema. Hoje, a Lei é o resultado de Teoria dos Números que mais possui demonstrações, sendo, ao todo, 221 demonstrações distintas.

A seguir, exporemos uma demonstração da Lei fazendo uso de argumentação geométrica. Esta demonstração foi apresentada, originalmente, por Eisenstein (1823−1852).

Teorema 3.10. *(Lei de Reciprocidade Quadrática) Sejam $p, q \in \mathbb{P}^*$ distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Demonstração: Como já mencionamos, a demonstração deste belo teorema será realizada através de argumentos geométricos, na qual faremos uso de um retângulo com dimensões representadas a partir dos números p e q, como vemos na figura 3.3. Utilizaremos esta ilustração para facilitar o desenvolvimento e o entendimento da demonstração.

Note que, no retângulo ABCD, com vértices $(0,0), (\frac{p}{2},0), (\frac{p}{2},\frac{q}{2})$ e $(0,\frac{q}{2})$, temos $\frac{q-1}{2} \cdot \frac{p-1}{2}$ pares ordenados, nos quais ambos os números das coordenadas x e y são inteiros. Durante a demonstração, consideraremos que *pares ordenados* são *pares ordenados com coordenadas inteiras.*

A reta r, que contém os pontos A e C e tem equação $y = \frac{qx}{p}$, não contém qualquer par ordenado. Para demonstrarmos esta afirmação, suponhamos

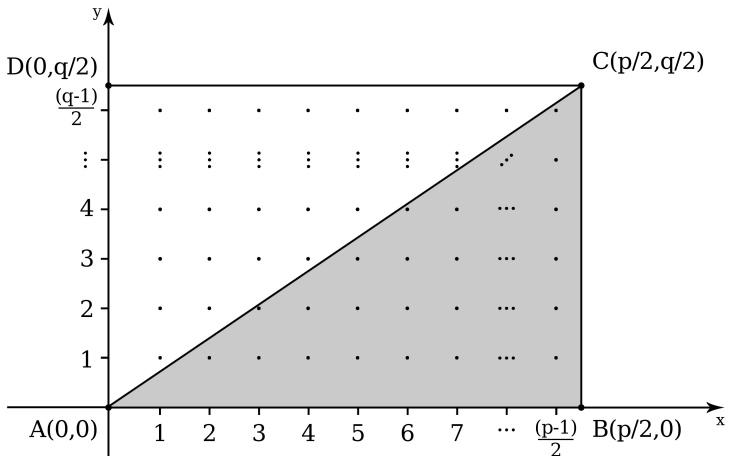

Figura 3.1: Representação geométrica dos pares ordenados

que exista algum ponto (x_0, y_0) nesta reta. Então, temos que $y_0 = \frac{qx_0}{p}$ é um número inteiro com $x_0 \in \{1, ..., \frac{p-1}{2}\}$. Mas $p \nmid qx_0$, pois $p \nmid q$ e $p \nmid x_0$, uma vez que $|x_0| < p$. Logo, o ponto (x_0, y_0) não pertence à reta r, seja qual for x_0.

Agora, percebamos que a reta r intercepta as retas $x = k$ nos pontos $(k, kq/p)$, com $k \in \{1, 2, ..., \frac{p-1}{2}\}$. Já sabemos que $(k, kq/p)$ não é um par inteiro, assim, temos que $\left\lfloor \frac{kq}{p} \right\rfloor$ é o número de pontos da reta $x = k$ com coordenadas inteiras que estão acima do eixo x e abaixo da reta r (região cinza). Logo, podemos representar a quantidade desses pontos do triângulo ABC, como

$$M = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{3q}{p} \right\rfloor + ... + \left\lfloor \frac{p-1}{2} \cdot \frac{q}{p} \right\rfloor.$$

Considerando as interseções das retas $y = k$ com a reta r (agora com $k \in \{1, 2, 3, ..., \frac{q-1}{2}\}$), de modo análogo, obtemos que $\left\lfloor \frac{kp}{q} \right\rfloor$ é o número de pontos da reta $y = k$ que estão acima da reta r e a direita do eixo y (região branca). Representaremos a quantidade de pontos no interior do triângulo ACD por

$$N = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \left\lfloor \frac{3p}{q} \right\rfloor + ... + \left\lfloor \frac{q-1}{2} . \frac{p}{q} \right\rfloor.$$

Note que

$$M + N = \frac{q-1}{2} \cdot \frac{p-1}{2}.$$

Mas, pelo teorema anterior,

$$\left(\frac{q}{p}\right) = (-1)^M \text{ e } \left(\frac{p}{q}\right) = (-1)^N.$$

Multiplicando, membro a membro, as igualdades acima, tem-se

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N}.$$

E, portanto,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

■

Antes de terminar esta seção, observemos alguns fatos acerca da Lei de Reciprocidade Quadrática. Como vimos na demonstração do teorema 3.7, $\frac{p-1}{2}$ é par se, e somente se, $p \equiv 1 \ (mod\ 4)$. Desta forma, $\frac{p-1}{2} \cdot \frac{q-1}{2}$ é ímpar se, e só se, $p \equiv q \equiv 3 \ (mod\ 4)$. Assim, a depender do resto de p e q na divisão por 4, $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$ ou -1. Ou seja, se pelo menos um, entre p e q, tiver resto 1 na divisão po 4, a Lei nos diz que

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Se, porém, ambos p e q deixam resto 3 na divisão por 4, a Lei nos diz que

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Portanto, podemos optar por calcular o mais simples entre os dois símbolos e, dessa forma, julgar se, no primeiro caso, ambos são ou não resíduos quadráticos e, no segundo caso, se um deles é e outro não. Para exemplificar cada um destes casos, vejamos os seguintes exemplos:

Exemplo 3.12. Verifique se 6481 é resíduo quadrático módulo 6661, onde 6481 e 6661 $\in \mathbb{P}^*$.
Solução: Note que isto equivale a calcular $(\frac{6481}{6661})$. Como 6481 e 6661 $\in \mathbb{P}^*$, pela Lei de Reciprocidade Quadrática,

$$\left(\frac{6481}{6661}\right)\left(\frac{6661}{6481}\right) = (-1)^{\frac{6661-1}{2}\cdot\frac{6481-1}{2}} = 1,$$

ou seja, ou 6661 e 6481 são resíduos quadráticos ou ambos não são. Assim, precisamos verificar apenas um deles. Primeiramente, note que

$$6661 \equiv 180 \ (mod\ 6481),$$

ou seja (veja exercício 15),

$$\left(\frac{6661}{6481}\right) = \left(\frac{180}{6481}\right).$$

Mas $180 = 2^2 \cdot 3^2 \cdot 5$, isto é,

$$\left(\frac{180}{6481}\right) = \left(\frac{2^2 \cdot 3^2 \cdot 5}{6481}\right) = \left(\frac{2^2}{6481}\right)\left(\frac{3^2}{6481}\right)\left(\frac{5}{6481}\right).$$

Deste modo (veja exercício 1),

$$\left(\frac{180}{6481}\right) = \left(\frac{2^2}{6481}\right)\left(\frac{3^2}{6481}\right)\left(\frac{5}{6481}\right) = 1 \cdot 1 \cdot \left(\frac{5}{6481}\right) = \left(\frac{5}{6481}\right).$$

Como $5 \equiv 1 \ (mod\ 4)$, aplicando a Lei novamente, temos que

$$\left(\frac{5}{6481}\right) = \left(\frac{6481}{5}\right).$$

Finalmente, pelo fato de $6481 \equiv 1 \ (mod\ 5)$, segue que

$$\left(\frac{6481}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Portanto, 6481 é resíduo quadrático módulo 6661.

Exemplo 3.13. Verifique se $x^2 \equiv 2865 \ (mod\ 991)$ tem solução.
Solução: Vamos calcular $\left(\frac{2865}{991}\right)$. Note que 991 é primo ímpar e, além disso, $2865 \equiv 883 \ (mod\ 991)$, onde 883 também é primo ímpar. Assim,

$$\left(\frac{2865}{991}\right) = \left(\frac{883}{991}\right).$$

Aplicando a Lei, temos que

$$\left(\frac{883}{991}\right)\left(\frac{991}{883}\right) = (-1)^{\frac{883-1}{2}\cdot\frac{991-1}{2}} = -1.$$

Daí,

$$\left(\frac{883}{991}\right) = -\left(\frac{991}{883}\right).$$

Ora, $991 \equiv 108 \ (mod\ 883)$ e $108 = 2^2 \cdot 3^2 \cdot 3$. Portanto,

$$\left(\frac{991}{883}\right) = \left(\frac{108}{883}\right) = \left(\frac{2^2}{883}\right)\left(\frac{3^2}{883}\right)\left(\frac{3}{883}\right) = \left(\frac{3}{883}\right).$$

Como $3 \equiv 883 \equiv 3 \ (mod\ 4)$, deve ser

$$\left(\frac{3}{883}\right) = -\left(\frac{883}{3}\right),$$

ou ainda,

$$\left(\frac{883}{991}\right) = \left(\frac{883}{3}\right).$$

Finalmente, do fato de ser $883 \equiv 1 \ (mod\ 3)$, temos que

$$\left(\frac{2865}{991}\right) = \left(\frac{883}{991}\right) = \left(\frac{883}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Portanto, $x^2 \equiv 2865 \ (mod\ 991)$ tem solução.

No exemplo anterior, vimos que 2865 (e portanto 883) é resíduo quadrático módulo 991. Como tanto 883 quanto 991 são côngruos a 3 módulo 4, apenas um deles é resíduo quadrático módulo o outro. Neste caso, com verificamos, 991 não é resíduo quadrático módulo 883.

Exemplo 3.14. Determine se $x^2 \equiv 3613 \ (mod\ 3011)$ tem, ou não, solução, onde $3613, 3011 \in \mathbb{P}^*$.
Solução: Pela Lei de Reciprocidade Quadrática,

$$\left(\frac{3613}{3011}\right)\left(\frac{3011}{3613}\right) = (-1)^{\frac{3613-1}{2}\cdot\frac{3011-1}{2}} = 1.$$

Assim,

$$\left(\frac{3613}{3011}\right) = \left(\frac{3011}{3613}\right).$$

Ora, $3613 \equiv 602 \ (mod\ 3011)$. Logo,

$$\left(\frac{3613}{3011}\right) = \left(\frac{602}{3011}\right) = \left(\frac{2}{3011}\right)\left(\frac{7}{3011}\right)\left(\frac{43}{3011}\right).$$

Pelo teorema 3.8, $(\frac{2}{3011}) = -1$, pois $3011 \equiv 3 \ (mod\ 8)$. Além disso, temos que $7 \equiv 3011 \equiv 3 \ (mod\ 4)$ e $3011 \equiv 1 \ (mod\ 7)$, donde

$$-\left(\frac{7}{3011}\right) = \left(\frac{3011}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

Analogamente,

$$-\left(\frac{43}{3011}\right) = \left(\frac{3011}{43}\right) = \left(\frac{1}{43}\right) = 1.$$

Logo,

$$\left(\frac{3613}{3011}\right) = \left(\frac{2}{3011}\right)\left(\frac{7}{3011}\right)\left(\frac{43}{3011}\right) = (-1)\cdot(-1)\cdot(-1) = -1.$$

Portanto, a congruência $x^2 \equiv 3613\ (mod\ 3011)$ não tem solução.

3.4 Símbolo de Jacobi: uma extensão do Símbolo de Legendre

Como vimos, o Símbolo de Legendre de a módulo n está definido quando n é, necessariamente, um número primo ímpar. Podemos generalizar definindo o Símbolo de Jacobi que exige, tão somente, que n seja ímpar e $mdc(a,n) = 1$ para estar bem definido.

Definição 3.4. Sejam $a \in \mathbb{Z}$ e $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ a decomposição em fatores primos de um inteiro positivo e ímpar n, com $mdc(a,n) = 1$. *O símbolo de Jacobi*, denotado por $\left[\frac{a}{n}\right]$ (lê-se: a jacobi n), é definido por

$$\left[\frac{a}{n}\right] = \left[\frac{a}{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}}\right] = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_t}\right)^{\alpha_t}.$$

É importante ressaltar que, embora o símbolo de Jacobi seja uma extensão do símbolo de Legendre, ao contrário deste, pode ocorrer que a não seja resíduo quadrático módulo n mesmo que $\left[\frac{a}{n}\right] = 1$. Convidamos o leitor a exemplificar esta afirmação.

Exemplo 3.15. Calcule $\left[\frac{13}{72}\right]$.
Solução: Como $72 = 3^2\cdot 2^2\cdot 2$, pela definição do símbolo de Jacobi,

$$\left[\frac{13}{72}\right] = \left[\frac{13}{3^2\cdot 2^2\cdot 2}\right] = \left(\frac{13}{3}\right)^2\left(\frac{13}{2}\right)^2\left(\frac{13}{2}\right) = 1\cdot 1\cdot\left(\frac{13}{2}\right) = 1,$$

pois 1 é solução da congruência $x^2 \equiv 13\ (mod\ 2)$.

Exemplo 3.16. Determine $\left[\frac{4304}{1323}\right]$.
Solução: Note que, como $4304 \equiv 335\ (mod\ 1323)$, temos que

$$\left[\frac{4304}{1323}\right] = \left[\frac{335}{1323}\right].$$

Deste modo, determinemos $\left[\frac{335}{1323}\right]$. Utilizando a definição do símbolo de Jacobi e aplicando as devidas propriedades para o símbolo de Legendre, determinemos o valor para os símbolos acima. Assim, temos que

$$\left[\frac{335}{1323}\right] = \left[\frac{335}{3^3 \cdot 7^2}\right] = \left(\frac{335}{3}\right)^3 \left(\frac{335}{7}\right)^2.$$

Daí,

$$\left(\frac{335}{3}\right)^3 \left(\frac{335}{7}\right)^2 = \left\{\left(\frac{5}{3}\right)\left(\frac{67}{3}\right)\right\}^3 \cdot \left\{\left(\frac{5}{7}\right)\left(\frac{67}{7}\right)\right\}^2.$$

Calculendo cada símbolo de Legendre acima, obtemos que

$$\left\{\left(\frac{5}{3}\right)\left(\frac{67}{3}\right)\right\}^3 = -1,$$

uma vez que 5 não é resíduo quadrático módulo 3 e 67 o é. Como

$$\left\{\left(\frac{5}{7}\right)\left(\frac{67}{7}\right)\right\}^2 = 1,$$

seque que

$$\left\{\left(\frac{5}{3}\right)\left(\frac{67}{3}\right)\right\}^3 \cdot \left\{\left(\frac{5}{7}\right)\left(\frac{67}{7}\right)\right\}^2 = -1.$$

E, portanto

$$\left[\frac{4304}{1323}\right] = \left[\frac{335}{1323}\right] = -1.$$

Teorema 3.11. *Para n inteiro ímpar e positivo, temos*

$$\left[\frac{-1}{n}\right] = (-1)^{\frac{n-1}{2}}.$$

Demonstração: Seja $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_t^{a_t}$, com p_i primo, $i \in I_t$. Da definição, temos:

$$\left[\frac{-1}{n}\right] = \left(\frac{-1}{p_1}\right)^{a_1} \cdots \left(\frac{-1}{p_t}\right)^{a_t}. \tag{3.4.13}$$

Note que

$$\begin{aligned}
(4k+1)(4q+1) &= 4(4kq+k+q)+1, \\
(4k+3)(4q+1) &= 4(4qk+k+3q)+3, \\
(4k+3)(4q+3) &= 4(4qk+3k+3q+2)+1.
\end{aligned}$$

Isto significa que, se um número ímpar é da forma $4m+1$, então sua decomposição prima tem uma quantidade par de fatores primos da forma $4k+3$. Por outro lado, se o número é da forma $4x+3$, então ele tem uma quantidade ímpar de fatores da forma $4k+3$ (esse fato será utilizado para concluir a demonstração). Pelo teorema 3.7, sabemos que $\left(\frac{-1}{p}\right)$, para todo p da forma $4k+1$, não interfere no resultado de 3.4.13. Assim, reagrupando se necessário,

$$\left[\frac{-1}{n}\right] = \left(\frac{-1}{p_1}\right)^{a_1} \cdots \left(\frac{-1}{p_s}\right)^{a_s},$$

com $s \leq t$ e p_i é da forma $4k+3$, com $i \in I_s$.
Temos dois casos a considerar:
1º caso: $n = 4m+1$, para algum $m \in \mathbb{Z}$.

Temos, usando o teorema 3.7 novamente,

$$\left[\frac{-1}{n}\right] = (-1)^{2r} = 1 = (-1)^{\frac{n-1}{2}}. \tag{3.4.14}$$

2º caso: $n = 4m+3$, para algum $m \in \mathbb{Z}$.
Temos, do teorema já mencionado:

$$\left[\frac{-1}{n}\right] = (-1)^{2p+1} = -1 = (-1)^{\frac{n-1}{2}}. \tag{3.4.15}$$

Dos dois casos, concluímos a demonstração. ■

Exemplo 3.17. Determine $\left[\frac{-1}{1317}\right]$.
Solução: Pelo teorema 3.11, sabemos que

$$\left[\frac{-1}{1317}\right] = (-1)^{\frac{1317-1}{2}} = (-1)^{658} = 1.$$

Exemplo 3.18. Determine o valor de $\left[\frac{-4301}{4459}\right]$, onde $mdc(4459, -4301) = 1$.
Solução: Como Jacobi é completamente multiplicativo (veja exercício 18),

$$\left[\frac{-4301}{4459}\right] = \left[\frac{-1}{4459}\right]\left[\frac{4301}{4459}\right].$$

Do teorema anterior,

$$\left[\frac{-1}{4459}\right] = (-1)^{\frac{4459-1}{2}} = -1.$$

Vamos calcular o fator $\left[\frac{4301}{4459}\right]$. Como $4459 = 7^3 \cdot 13$, segue que

$$\left[\frac{4301}{4459}\right] = \left(\frac{4301}{7}\right)^3 \left(\frac{4301}{13}\right).$$

Calculemos primeiro $\left(\frac{4301}{7}\right)$. Sendo $4301 = 23 \cdot 17 \cdot 11$,

$$\left(\frac{4301}{7}\right) = \left(\frac{23}{7}\right)\left(\frac{17}{7}\right)\left(\frac{11}{7}\right).$$

Mas $23 \equiv 2 \ (mod\ 7)$, $17 \equiv 3 \ (mod\ 7)$ e $11 \equiv -3 \ (mod\ 7)$, o que implica

$$\left(\frac{4301}{7}\right) = \left(\frac{23}{7}\right)\left(\frac{17}{7}\right)\left(\frac{11}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{-1}{7}\right)\left(\frac{3}{7}\right).$$

Pelo teorema 3.8, $\left(\frac{2}{7}\right) = 1$ e, pelo teorema 3.7, $\left(\frac{-1}{7}\right) = -1$. Assim,

$$\left(\frac{4301}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{-1}{7}\right)\left(\frac{3}{7}\right) = 1 \cdot (-1) \cdot \left(\frac{3}{7}\right)^2 = -1.$$

Agora, calculemos $\left(\frac{4301}{13}\right)$. Analogamente,

$$\left(\frac{4301}{13}\right) = \left(\frac{23}{13}\right)\left(\frac{17}{13}\right)\left(\frac{11}{13}\right).$$

Mas $23 \equiv -3 \ (mod\ 13), 17 \equiv 4 \equiv 2^2 \ (mod\ 13)$ e $11 \equiv -2 \ (mod\ 13)$, o que implica

$$\left(\frac{4301}{13}\right) = \left(\frac{23}{13}\right)\left(\frac{17}{13}\right)\left(\frac{11}{13}\right) = \left(\frac{-3}{13}\right)\left(\frac{4}{13}\right)\left(\frac{-2}{13}\right) =$$

$$= \left(\frac{-1}{13}\right)^2 \left(\frac{3}{13}\right)\left(\frac{2^2}{13}\right)\left(\frac{2}{13}\right) = \left(\frac{3}{13}\right)\left(\frac{2}{13}\right).$$

Como $13 \equiv -3 \ (mod\ 8)$, pelo teorema 3.8, segue que $\left(\frac{2}{13}\right) = -1$. Além disso, $13 \equiv 1 \ (mod\ 4)$ e $13 \equiv 1 \ (mod\ 3)$, donde, pelo teorema 3.10,

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Finalmente,

$$\left[\frac{4301}{4459}\right] = \left(\frac{4301}{7}\right)^3 \left(\frac{4301}{13}\right) = \left(\frac{4301}{7}\right)\left(\frac{3}{13}\right)\left(\frac{2}{13}\right) = (-1) \cdot 1 \cdot (-1) = 1.$$

A seguir, mostraremos que a Lei de Reciprocidade Quadrática continua válida se substituirmos o símbolo de Legendre pelo símbolo de Jacobi.

Teorema 3.12. *Se $n, m \in \mathbb{Z}_+$, ímpares, são tais que $mdc(m,n) = 1$, então*

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Demonstração: Sejam $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ e $q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}$ as decomposições em fatores primos de n e m, respectivamente. Da definição do símbolo de Jacobi e pelo teorema 3.5, temos:

$$\left[\frac{n}{m}\right] = \prod_{j=1}^{s}\left(\frac{n}{q_j}\right)^{\beta_j} = \prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)^{\beta_j\alpha_i},$$

e, analogamente,

$$\left[\frac{m}{n}\right] = \prod_{i=1}^{t}\left(\frac{m}{p_i}\right)^{\alpha_i} = \prod_{j=1}^{s}\prod_{i=1}^{t}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}.$$

Multiplicando estas igualdades e agrupando os produtórios, obtemos

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] = \prod_{i=1}^{t}\prod_{j=1}^{s}\left\{\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right\}^{\alpha_i\beta_j}.$$

Pela Lei de Reciprocidade Quadrática, tem-se

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}. \tag{3.4.16}$$

Assim,

$$\begin{aligned}
\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] &= \prod_{i=1}^{t}\prod_{j=1}^{s}\left\{\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right\}^{\alpha_i\beta_j} \\
&= \prod_{i=1}^{t}\prod_{j=1}^{s}(-1)^{\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})} \\
&= \prod_{i=1}^{t}[(-1)^{\alpha_i(\frac{p_i-1}{2})\beta_1(\frac{q_1-1}{2})}\cdot\ldots\cdot(-1)^{\alpha_i(\frac{p_i-1}{2})\beta_s(\frac{q_s-1}{2})}] \\
&= \prod_{i=1}^{t}[(-1)^{\sum_{j=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})}] \\
&= [(-1)^{\sum_{j=1}^{s}\alpha_1(\frac{p_1-1}{2})\beta_j(\frac{q_j-1}{2})}]\cdot\ldots\cdot[(-1)^{\sum_{j=1}^{s}\alpha_t(\frac{p_t-1}{2})\beta_j(\frac{q_j-1}{2})}] \\
&= (-1)^{\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})}.
\end{aligned}$$

Afirmação:

$$\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2}) \quad \text{e} \quad \frac{m-1}{2}\cdot\frac{n-1}{2}$$

têm a mesma paridade. Perceba que essa afirmação conclui a demonstração. Para demonstrá-la, temos dois casos a analisar.
1º caso: $\frac{m-1}{2}\cdot\frac{n-1}{2}$ é ímpar.

Então $\frac{m-1}{2}$ e $\frac{n-1}{2}$ são da forma $4k+3$. Assim, do que foi provado no teorema anterior, na fatoração de m e n em fatores primos, há uma quantidade ímpar de fatores da forma $4k+3$ e, portanto,

$$(\sum_{i=1}^{t}\alpha_i(\frac{p_i-1}{2}))(\sum_{j=1}^{s}\beta_j(\frac{q_j-1}{2}))$$

é ímpar, pois

$$(\sum_{i=1}^{t}\alpha_i(\frac{p_i-1}{2})) \text{ e } (\sum_{j=1}^{s}\beta_j(\frac{q_j-1}{2}))$$

são, ambos, ímpares (veja exemplo 1.8).
2º caso: $(\frac{m-1}{2})(\frac{n-1}{2})$ é par.

Então ao menos um dos fatores é par. Sem perda de generalidade, digamos que seja $(\frac{m-1}{2})$. Daí, na fatoração de m, há uma quantidade par de elementos da forma $4z+3$ e, por isso,

$$\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{j_1-1}{2})$$

é par, uma vez que

$$(\sum_{j=1}^{s}\beta_j(\frac{q_j-1}{2}))$$

é par. Concluindo, assim, a demonstração. ■

Exemplo 3.19. Quanto vale $\left[\frac{25725}{17303}\right]$? E $\left[\frac{17303}{25725}\right]$?
Solução: Pelo teorema 3.12,

$$\left[\frac{25725}{17303}\right]\left[\frac{17303}{25725}\right] = (-1)^{\frac{25725-1}{2}\frac{17303-1}{2}} = 1,$$

ou seja, ou 25725 e 17303 estão em reciprocidade quadrática ou ambos não estão. Como $25725 = 7^2 \cdot 7 \cdot 5^2 \cdot 3$ e $17303 = 11^2 \cdot 11 \cdot 13$, segue que

$$\left[\frac{17303}{25725}\right] = \left(\frac{17303}{7}\right)^2 \left(\frac{17303}{7}\right) \left(\frac{17303}{5}\right)^2 \left(\frac{17303}{3}\right) =$$

$$= \left(\frac{11^2}{7}\right) \left(\frac{11}{7}\right) \left(\frac{13}{7}\right) \left(\frac{11^2}{3}\right) \left(\frac{11}{3}\right) \left(\frac{13}{3}\right) = \left(\frac{11}{7}\right) \left(\frac{13}{7}\right) \left(\frac{11}{3}\right) \left(\frac{13}{3}\right).$$

Como $11 \equiv -3$ $(mod\ 7)$, $13 \equiv -1$ $(mod\ 7)$, $11 \equiv -1$ $(mod\ 3)$ e, ainda, $13 \equiv 1$ $(mod\ 3)$, tem-se

$$\left[\frac{17303}{25725}\right] = \left(\frac{11}{7}\right) \left(\frac{13}{7}\right) \left(\frac{11}{3}\right) \left(\frac{13}{3}\right) = \left(\frac{-3}{7}\right) \left(\frac{-1}{7}\right) \left(\frac{-1}{3}\right) \left(\frac{1}{3}\right) =$$

$$= \left(\frac{-1}{7}\right)^2 \left(\frac{3}{7}\right) \left(\frac{-1}{3}\right) = \left(\frac{3}{7}\right) \left(\frac{-1}{3}\right).$$

Do fato de $3 \equiv -1$ $(mod\ 4)$, segue que $\left(\frac{-1}{3}\right) = -1$. Além disso, pelo critério de Euler,

$$\left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}} \equiv 3^3 \equiv 27 \equiv -1\ (mod\ 7),$$

isto é, $\left(\frac{3}{7}\right) = -1$. Portanto,

$$\left[\frac{25725}{17303}\right] = \left[\frac{17303}{25725}\right] = \left(\frac{3}{7}\right) \left(\frac{-1}{3}\right) = (-1) \cdot (-1) = 1.$$

No próximo exemplo, traremos um caso em que ambos os números envolvidos no Jacobi são côngruos a 3 módulo 4.

Exemplo 3.20. Determine $\left[\frac{81675}{75803}\right]$ e $\left[\frac{75803}{81675}\right]$.
Solução: Pelo teorema 3.12,

$$\left[\frac{81675}{75803}\right] \left[\frac{75803}{81675}\right] = (-1)^{\frac{81675-1}{2} \frac{75803-1}{2}} = -1.$$

Portanto,

$$\left[\frac{81675}{75803}\right] = -\left[\frac{75803}{81675}\right].$$

Como $81675 = 11 \cdot 3^2 \cdot 3 \cdot 5^2$ e $75803 = 7^2 \cdot 7 \cdot 13 \cdot 17$, segue que

$$\left[\frac{75803}{81675}\right] = \left(\frac{75803}{11}\right) \left(\frac{75803}{3}\right)^2 \left(\frac{75803}{3}\right) \left(\frac{75803}{5}\right)^2 =$$

$$= \left(\frac{7^2 \cdot 7 \cdot 13 \cdot 17}{11}\right)\left(\frac{7^2 \cdot 7 \cdot 13 \cdot 17}{3}\right) =$$

$$= \left(\frac{7}{11}\right)\left(\frac{13}{11}\right)\left(\frac{17}{11}\right)\left(\frac{7}{3}\right)\left(\frac{13}{3}\right)\left(\frac{17}{3}\right).$$

Mas $7 \equiv -4 \equiv -2^2 \ (mod\ 11)$, $13 \equiv 2 \ (mod\ 11)$, $17 \equiv -5 \ (mod\ 11)$, $7 \equiv 1 \ (mod\ 3), 13 \equiv 1 \ (mod\ 3)$ e $17 \equiv -1 \ (mod\ 3)$. Logo,

$$\left[\frac{75803}{81675}\right] = \left(\frac{7}{11}\right)\left(\frac{13}{11}\right)\left(\frac{17}{11}\right)\left(\frac{7}{3}\right)\left(\frac{13}{3}\right)\left(\frac{17}{3}\right) =$$

$$= \left(\frac{-1}{11}\right)\left(\frac{2^2}{11}\right)\left(\frac{2}{11}\right)\left(\frac{-1}{11}\right)\left(\frac{5}{11}\right)\left(\frac{1}{3}\right)\left(\frac{1}{3}\right)\left(\frac{-1}{3}\right) =$$

$$= \left(\frac{2}{11}\right)\left(\frac{5}{11}\right)\left(\frac{-1}{3}\right).$$

Na primeira parcela, podemos utilizar o teorema 3.8, obtendo $\left(\frac{2}{11}\right) = -1$. Na segunda parcela, note que 4 é solução da congruência $x^2 \equiv 5 \ (mod\ 11)$, donde $\left(\frac{5}{11}\right) = 1$. Na última parcela, podemos utilizar o teorema 3.7, obtendo $\left(\frac{-1}{3}\right) = -1$. Daí,

$$\left[\frac{75803}{81675}\right] = \left(\frac{2}{11}\right)\left(\frac{5}{11}\right)\left(\frac{-1}{3}\right) = (-1) \cdot 1 \cdot (-1) = 1.$$

Portanto,

$$\left[\frac{81675}{75803}\right] = -1 \quad \text{e} \quad \left[\frac{75803}{81675}\right] = 1.$$

3.5 Exercícios

1. Mostre que todos os quadrados perfeitos são resíduos quadráticos módulo n, para qualquer $n \in \mathbb{Z}$.

2. Determine todos os resíduos quadráticos módulo 13 e módulo17.

3. Determine, no conjunto $\{1, 2, ..., 30\}$, os resíduos quadráticos módulo 31.

4. Determine se as congruências quadráticas têm ou não solução. Em caso afirmativo expresse-as.

a) $x^2 \equiv 1 \ (mod\ 5)$;
b) $x^2 \equiv 2 \ (mod\ 17)$;
c) $x^2 \equiv 6 \ (mod\ 47)$;
d) $x^2 \equiv -12 \ (mod\ 71)$;
e) $x^2 \equiv 2 \ (mod\ 7)$;
f) $x^2 \equiv 2 \ (mod\ 13)$.

5. Usando apenas a definição do símbolo de Legendre, determine:

a) $\left(\frac{2}{7}\right)$;
b) $\left(\frac{13}{3}\right)$;
c) $\left(\frac{6}{7}\right)$;
d) $\left(\frac{5}{31}\right)$;
e) $\left(\frac{12}{37}\right)$;
f) $\left(\frac{335}{67}\right)$.

6. Mostre que $p-3$ é resíduo quadrático para todo número primo da forma $6n+1$ e não-resíduo quadrático para todo número primo da forma $6n-1$.

7. Avaliar

a) $\left(\frac{356}{241}\right)$; b) $\left(\frac{44}{103}\right)$; c) $\left(\frac{2014}{1019}\right)$; d) $\left(\frac{-4}{293}\right)$.

8. Determine todos os números a, com $mdc(a, 47) = 1$, tais que

$$47|(a^{\frac{p-1}{2}} - 1) \text{ e } 47|(a^{\frac{p-1}{2}} + 1).$$

9. Demonstre a proposição 3.1.

10. Mostre que a congruência $x^2 \equiv 93 \ (mod\ 137)$ possui solução.

11. Encontre números primos p para os quais $\left(\frac{p}{11}\right) = 1$.

12. Determine, em cada caso, $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$:

a) $p = 311$ e $q = 829$;
b) $p = 2137$ e $q = 3469$;
c) $p = -4591$ e $q = 5281$;
d) $p = 6571$ e $q = 6011$;
e) $p = 17497$ e $q = 19267$;
f) $p = 458$ e $q = 5881$.

13. Utilizando a Lei de Reciprocidade Quadrática, determine $\left(\frac{7417}{4451}\right)$, onde 7417 e 4451 são números primos.

14. Use a Lei de Reciprocidade Quadrática para mostrar que, se $p \in \mathbb{P}^*$, então
$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{se} \quad p \equiv \pm 1 \ (mod\ 12); \\ -1, & \text{se} \quad p \equiv \pm 5 \ (mod\ 12). \end{cases}$$

15. Mostre que, se $p \in \mathbb{P}^*$, $a, a_0 \in \mathbb{Z}$, $a \equiv a_0 \ (mod\ p)$ e $mdc(a,p) = 1$, então $(\frac{a}{p}) = (\frac{a_0}{p})$.

16. Avaliar $\left(\frac{356}{241}\right)$ e $\left[\frac{181}{991}\right]$.

17. Determine

a) $\left[\frac{2}{55}\right]$;

b) $\left[\frac{11}{35}\right]$;

c) $\left[\frac{19}{1575}\right]$;

d) $\left[\frac{-4}{31}\right]$;

e) $\left[\frac{12}{33}\right]$;

f) $\left[\frac{335}{27}\right]$.

18. Mostre que o símbolo de Jacobi é multiplicativo, isto é,
$$\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right] \cdot \left[\frac{b}{n}\right]$$
para $a, b \in \mathbb{Z}$ com $mdc(ab, n) = 1$ e $n \in \mathbb{Z}$ ímpar.

19. Mostrar que, se n for um inteiro ímpar e positivo, então
$$\left[\frac{2}{p}\right] = (-1)^{\frac{n^2-1}{8}}.$$

Bibliografia

[da Rocha] da Rocha, L. V. A Lei de Reciprocidade Quadrática. Seminário Matemático (Disciplina de Licenciatura Matemática), Universidade de Coimbra, Departamento de Matemática: Faculdade de de Ciências e Tecnologia.

[1] Freire, B. T. V. (2009). Notas de aula - Teoria dos Números.

[2] Halmos, P. R. (2001). *Teoria Ingênua dos Conjuntos*. Ed. Ciência Moderna, Rio de Janeiro.

[3] Hefez, A. (2006). *Elementos de Aritmética*. Ed. SBM, Rio de Janeiro.

[4] Landau, E. (2002). *Teoria Elementar dos Números*. Ed. Ciência Moderna, Rio de Janeiro.

[5] Maier, R. R. (2005). Teoria dos Números - Texo de aula. Universidade de Brasília (Departamento de Matemática - IE).

[6] Martinez, F. B., Moreira, C. G., Saldanha, N., e Tengan, E. (2013). *Teoria dos Números - Um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA, Rio de Janeiro.

[7] Milies, F. C. P. e Coelho, S. P. (2006). *Números: Uma introdução à matemática*. EDUSP, S.Paulo.

[8] Santos, J. P. (2012). *Introdução à Teoria dos Números*. IMPA, Rio de Janeiro.

[Silva] Silva, A. A. Números, Relações e Criptografia. Universidade Federal da Paraíba, Centro de Ciências Exatas e da Natureza, Departamento de Matemática.

Índice