UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

RESÍDUOS QUADRÁTICOS

RENAN JACKSON SOARES ISNERI

CAMPINA GRANDE
2017

RENAN JACKSON SOARES ISNERI

RESÍDUOS QUADRÁTICOS

Trabalho Acadêmico Orientado apresentado ao curso de Licenciatura em Matemática do Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba em cumprimento às exigências legais para obtenção do título de licenciado em Matemática.

Área de concentração: Matemática

Orientador: Dr. Vandenberg Lopes Vieira

CAMPINA GRANDE
2017

I84r Isneri, Renan Jackson Soares.
Resíduos quadráticos [manuscrito] / Renan Jackson Soares Isneri. - 2017.
81 p. : il.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2017.
"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática".

1. Congruências quadráticas. 2. Resíduos quadráticos. 3. Lei da Reciprocidade Quadrática. I. Título.

21. ed. CDD 512.72

RENAN JACKSON SOARES ISNERI

RESÍDUOS QUADRÁTICOS

Trabalho Acadêmico Orientado apresentado ao curso de Licenciatura em Matemática do Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba em cumprimento às exigências legais para obtenção do título de licenciado em Matemática.

COMISSÃO EXAMINADORA

Aprovado em 28/07/2017

Prof. Dr. Vandenberg Lopes Vieira
Dpto. Matemática - CCT/UEPB
ORIENTADOR

Prof. Mr. José Ginaldo de Souza Farias
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Prof. Mr. Weiller Felipe Chaves Barboza
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Dedicatória

À minha família dedico este ilustre trabalho pelo companheirismo e incentivo de cada um. Em especial, à minha mãe, Rilvânia Soares da Silva, e ao meu pai, Jardel Jakson Gomes Isneri, que são responsáveis pelo meu desenvolvimento intelectual.

Agradecimentos

Primeiramente, agradeço a Deus por minha vida, família, amigos e por tudo que me tem proporcionado ao longo da minha vida, pois estou aonde estou por conta dEle.

Agradeço à minha família, pelo amor, incentivo, confiança e apoio incondicional. Em especial, aos meus pais Rilvânia e Jardel que me deram apoio em todas as minhas situações, ao meu tio Jordean pelo carinho e incentivo nas horas difíceis, à minha avó, Desterro, por ser sempre uma segunda mãe para mim, aos meus irmãos Larissa, Jaqueline e Ryan e, também, a minha sobrinha Lais que amo tanto.

Agradeço ao meu orientador Dr. Vandenberg Lopes Vieira pela dedicação, atenção, apoio moral, compreensão, paciência e dedicação. Ao doutor agradeço pelas oportunidades que foram dadas durante a gradução, pois essas mesmas oportunidades foram necessárias para o término deste trabalho.

Aos professores Weiller Felipe Chaves Barboza e José Ginaldo de Souza Farias agradeço por estarem presente na minha banca e, principalmente, pelas contribuições de ambos em meu trabalho e, também, durante a graduação visando sempre o meu crescimento e aprendizado.

Agradeço ao Mestre José Elias da Silva e aos meus amigos Jonnas Henrique, Pedro Fellyoe e Ketllyn Mayara por contribuírem para a apresentação final do trabalho.

Aos professores do Departamento de Matemática da UEPB agradeço por me proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional, por não somente por terem me ensinado, mas por terem me feito aprender. Em especial, aos professores Aldo Trajano, Fernando Luiz, Luciana Roze, Thiciany Matsudo e, também, aos professores aposentados, bem como Francisco de Sá, Juarez Dantas e Ernesto Trajano. E, também, a todos os professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta monografia.

Agradeço aos meus amigos Elifal Gomes, Edvan Oliveira, Dimas Vicente, Leonardo Pereira, Anderson Wendel, Cicero Silva e muitos e outros que não foram citados são irmãos na amizade que fizeram parte direta ou indiretamente da minha formação, que sempre me encorajaram para seguir em frente e que vão continuar presentes em toda minha vida.

É difícil agradecer todas as pessoas que de algum modo, nos momentos serenos e ou apreensivos, fizeram ou fazem parte da minha vida, por isso agradeço à todos de coração.

"Há uma palavra que pode servir como regra para a vida de qualquer um - reciprocidade."

(Confúcio)

Resumo

Neste trabalho, estudamos as resoluções em $\mathbb{Z}$ das congruências quadráticas da forma $x^2 \equiv a\,(mod\,p)$, sendo p um número primo positivo e a um inteiro que não é divisível por p, no sentido de verificar a existência ou não de um inteiro x_0 tal que $x_0^2 \equiv a\,(mod\,p)$. Nosso estudo é realizado atráves do Critério de Euler e de algumas prorpiedades do Símbolo de Legendre. Em seguida, estudamos um resutado indispensável, conhecido na literatura como Lema de Gauss, uma vez que, o mesmo é um ponto de partida para provar a Lei da Reciprocidade Quadrática. Essa lei conecta a solubilidade das congruências $x^2 \equiv q\,(mod\,p)$ e $x^2 \equiv p\,(mod\,q)$, em que p e q são primos ímpares distintos. Em especial, caracterizamos os primos p para os quais alguns inteiros são ou não resíduos quadráticos módulo q. Por fim, encerramos o trabalho com algumas aplicações da teoria estuda, bem como o teste de Pépin, que por sua vez, é um teste de primalidade e, também, a irracionalidade de alguns números usando a Lei da Reciprocidade Quadrática.

Palavras-chave: Congruências Quadráticas. Resíduos Quadráticos. Lei da Reciprocidade Quadrática.

Abstract

In this work, we study how $\mathbb{Z}$-resolutions of the quadratic congruences of the form $x^2 \equiv a\,(mod\,p)$, where p is a positive prime number and a whole is not divisible by p, no sense of the existence or not of an integer x_0 such that $x_0^2 \equiv a\,(mod\,p)$. Our study was elaborated through the Euler Criterion and some extensions of the Legendre Symbol. Next, we study an indispensable result, known in the literature as Gauss's Lemma, since it is the starting point for proving the Law of Quadratic Reciprocity. This law connects the solubility of the congruences $x^2 \equiv q\,(mod\,p)$ and $x^2 \equiv p\,(mod\,q)$, where p and q are distinctly different primes. In particular, we characterize the primes p for which some integers are or not quadratic residues module q. Finally, we close the work with some applications of the theory studied, as well as the test of Pépin, in turn, and a test of primality and also an irrationality of some numbers using a Law of Quadratic Reciprocity.

Keywords: Quadratic Congruences. Quadratic Residue. Law of Quadratic Reciprocity.

Sumário

Introdução

"A matemática é a rainha das ciências e a teoria dos números é a rainha da matemática."

C. Gauss (1777-1855).

Johann Carl Friedrich Gauss (1777-1855) foi um grande matemático, chamado por alguns o príncipe da matemática. O mesmo contribuiu em diversas áreas da ciência, dentre elas a Teoria dos Números que por sua vez é o ramo da Matemática Pura que se dedica ao estudo dos números inteiros e suas generalizações. A notável citação acima refere-se do quão importante é a Teoria dos Números dentro da matemática e, consequentemente, da ciência.

Não só apenas Gauss se preocupou com a Teoria dos Números, mas também grandes matemáticos como Pitágoras, Euclides, Diofanto, M. Mersenne, P. Fermat, C. Goldbach, L. Euler, L. Kronecker, G. H. Hardy, S. Ramanujan e A. Wiles. Todos esses e muitos outros que não foram citados desenvolveram resultados importantíssimos na área da Teoria dos Números que hoje são aplicadas em diversas áreas do conhecimento como, por exemplo, Física, Biologia, Acústica, Computação, Criptografia.

A Teoria dos Números é dividida em vários ramos de acordo com os métodos usados ao longo de seus estudos. Por exemplo, Teoria Elementar dos Números, Teoria Analítica dos Números e Teoria Algébrica dos Números são os três principais ramos. Outro fato, a Teoria dos Números também é famosa por seus problemas em aberto. Por exemplo, em 1742, Christian Goldbach conjecturou que todo número par maior que 2 é soma de dois números primos. Este é um dos problemas mais antigos não resolvidos da matemática. Vejamos a sequência,

$$4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 10 = 5 + 5, 12 = 7 + 5, \ldots, 7760 = 5743 + 2017, \ldots.$$

Através de computadores já confirmaram a conjetura de Goldbach para vários números suficientemente grandes.

Além da conjectura de Goldebach, existem outros problemas em aberto na Teoria dos Números, em geral, todos relacionados a números primos, tais como a conjectura dos primos gêmos e a conjectura dos primos de Mersenne. A primeira afirma que existem infinitos pares de primos gêmeos, ou seja, pares da forma $(p, p + 2)$, em que p e $p + 2$ são números primos. Já a última, diz que existem infinitos números primos de Mersenne, isto é, dado o número

$M_p = 2^p - 1$, com p primo, então existe um conjunto infinito de valores para p tais que M_p é primo. Por exemplo,

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127.$$

A Teoria dos Resíduos Quadráticos é abordada na Teoria Elementar dos Números. No estudo das equações diofânticas quadráticas, desenvolvido por Legendre, Fermat, Euler e, principalmente, por Gauss, era de máxima importância determinar se a era um quadrado módulo um número primo $p > 2$, ou seja, dado p um número primo ímpar e um inteiro a não divisível por p, se existe um inteiro b tal que p divide $b^2 - a$. Neste sentido, o estudo da Teoria dos Resíduos Quadráticos se resume em resolver em $\mathbb{Z}$ uma congruência quadrática da forma $x^2 \equiv a\,(mod\,p)$, com p um número primo ímpar.

Em particular, destaca-se a Lei da Reciprocidade Quadrática que conecta a solução de duas congruências

$$x^2 \equiv q\,(mod\,p) \quad \text{e} \quad x^2 \equiv p\,(mod\,q),$$

onde q e p são primos ímpares distintos. Atualmente, encontra-se mais de 300 provas da mesma. No que lhe diz respeito, Gauss com a idade de 18 anos, no ano de 1795, achava que este resultado era verdadeiro após elaborar uma tabela de 10000 valores de (p/q). Contudo, ele só encontrou a prova depois de mais de um ano e publicou em seu livro *Disquisitones Arithmeticae*, onde apresentou duas demonstrações, sendo uma delas usando indução matemática. Porém, contata-se que Gausss encontrou 8 demonstrações distintas da Lei da Reciprocidade Quadrática. Por isso, tem-se noção de que muitos matemáticos trabalharam na Lei da Reciprocidade Quadrática, mas Fermat, Euler, Legendre e Gauss foram as peças fundamentais para as contribuições desta teoria.

Pierre de Fermat nasceu em Beaumont-de-Lomagne no ano de 1601 na França. A ele, muitos matemáticos o chamam de o pai da moderna Teoria dos Números. Fermat provou que para um conjunto de números primos, pode-se expressar cada primo desse conjunto como sendo soma de dois quadrados. Especificamente,

$$p = x^2 + y^2 \Leftrightarrow p = 2 \quad \text{ou} \quad p \equiv 1\,(mod\,4).$$

Também, ele considerou resultados similares para primos da forma

$$x^2 + ny^2, \quad \text{onde} \quad n = \pm 2, \pm 3, \pm 5, \ldots.$$

Embora Fermat nunca tenha afirmado a Lei da Reciprocidade Quadrática, os casos particulares $-1, \pm 2$ e ± 3 podem ser fundamentados do seu teorema.

Leonhard Paul Euler, um dos mais prolíficos matemáticos, nasceu na Suíça na cidade de Basileia no ano de 1707. Euler deu continuidade do trabalho de Fermat provando seu primeiro teorema conhecido, hoje, como Critério de Euler. Em 1744 surgiu a primeira afirmação equivalênte à Lei da Reciprocidade Quadrática, que por sua vez, foi declarada por Euler. Ainda

ele prosseguiu com os estudos intensamente, até que, formulou a lei por completo, sem lacunas. Porém, isso só foi publicado em 1783, depois de sua morte com a idade de 76 anos.

Não muito diferente de Fermat e Euler, Adrien Marie Legendre trabalhou ardualmente na Teoria dos Resíduos Quadráticos. Legendre nasceu em Paris no ano de 1752. O mesmo, definiu o símbolo $\left(\frac{a}{p}\right)$, com p primo, que hojé é atribuido ao seu nome o Símbolo de Legendre. Vejamos a definição:

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

Com essa nova notação, Legendre conseguiu demonstrar resultados com facilidade e, também, influenciou a futuras gerações de matemáticos a seguirem sua linha de raciocínio para produzirem pesquisa na lei da reciprocidade cúbicas e superiores, como por exemplo, os símbolos de Jacobi e Hilbert que sugiram através do estudo do símbolo de Legendre. Legendre também é resposável pela palavra "reciprocidade"na conexão das soluções de duas congruências quadráticas.

Alguns chamam o de o príncipe da matemática, muitos lhe conhecem por Carl Gauss, ou apenas Gauss, mas seu nome é Johann Carl Friedrich Gauss. Nascido na Alemanha em 30 de abril de 1777, Gauss na idade de 7 anos já mostrava o seu potencial em matemática. Ele trabalhou em diversas áreas da matemática, assim como na física. Em particular, se dedicou uma boa parte do seu tempo na Teoria dos Números. Em 1801, publicou seu trabalho *"Disquisitiones Arithmeticae"* onde nele contém a primeira prova da Lei da Reciprocidade Quadrática, esta seria, como já dito, por indução matemática. O gênio alemão foi capaz de fornecer 8 provas, cada uma delas com uma abordagem diferente, algumas usando Teoria dos Números Algébricos.

O presente trabalho é uma revisão bibliográfica em que a base de desenvolvimento é a busca das soluções de congruências quadráticas. O objetivo central é destacar, de modo construtível e detalhado, o maior número possível de resultados clássicos da Teoria Elementar dos Números referentes as congruências quadráticas e aplica-lós em outros conceitos.

Neste trabalho, abordamos alguns resultados tais como Símbolo de Legendre, Critério de Euler, Lema de Gauss, Lei da reciprocidade Quadrática e o teste de primalidade denominado Teste de Pepin. O texto foi dividido em 5 capítulos sendo o último reservado a aplicações, bem como a infinidade de alguns números primos nas formas particulares e a irracionalidade de certos números.

No Capítulo 1, apresetamos resultados introdutórios sobre os números inteiros que servirão para o entendimento da teoria seguinte. A primeira seção é dedicada a conceitos de divisibilidade sobre $\mathbb{Z}$ e, em seguida, conceitos de número primo e congruências. Por ser um capítulo de resultados preliminares, não nos vinculemos a uma abordagem detalhada sobre esses assuntos. Para tal, recomendamos a leitura das refências [5], [11] e [14].

No Capítulo 2, iniciamos o conceito de congruências quadráticas e resíduos quadráticos, com uma vasta séries de execícios, visando sempre o bom entendimento da teoria considerada.

No Capítulo 3, definimos o Símbolo de Legendre e consideramos o Critério de Euler. Também, mostramos que Símbolo de Legendre é uma função totalmente multiplicativa e, por fim, caracterizamos os números primos $p > 2$ para os quais -1 e 2 são resíduos quadráticos de p.

A lei da Reciprocidade Quadrática é dada no Capítulo 4, o qual é consequência do Lema de Gauss. Na última seção, abordamos o Teorema da Caracterização dos primos $p > 2$ para os quais 3, 5, 7 e 11 são resíduos quadráticos de p.

Já o Capítulo 5, fizemos as aplicações da teoria apresentada nos capítulos anteriores. Tais aplicações foram divididas em três seções, onde a primeira é destinada à infinidade de primos das formas $3k + 1$, $5k - 1$ e $8k - 1$. Na segunda seção, mostramos a ultilidade do Símbolo de Legendre no Crivo de Eratóstenes e o Teste de Primalidade de Pépin. Na última seção, usamos o Símbolo de Legendre revestido da Lei da Reciprocidade Quadrática para provar a irracionalidade de alguns números.

O texto é finalizado com o Anexo A, no qual destacamos uma colêtanea de provas da Lei da Reciprocidade Quadrática contendo 314 provas enumerada de 1 a 314 desde a primeira prova incompleta de Legendre, embora Gauss foi o primeiro a provar concretamente, até a demonstração feita pelos matemáticos Brunyate e Clark no ano de 2014. Também, na lista encontra-se o nome de cada autor, o ano e o método usado pelo mesmo nas demonstrações.

Portanto, espera-se que este projeto de pesquisa contribua para os estudantes, em especial, para sociedade matemática, uma vez que o mesmo será baseado nas reflexões mais profunda que o autor pode alcançar para a construção de um conhecimento matemático cada vez mais significativo e concreto.

Capítulo 1

Resultados Preliminares

Neste capítulo, consideraremos tópicos relacionados a Teoria Elementar dos Números bem como conceitos de divisibilidade em $\mathbb{Z}$, números primos e congruências. Tais considerações serão necessárias para o estudo dos capítulos subsequentes. No entento, não faremos um estudo geral e aprofundado dos assuntos aqui tratados, apenas abordaremos resultados que servirão para um bom entendimento dos estudos de Congruências Quadrática e suas devidas aplicações. Ao leitor interessado em mais detalhes indicamos as referências [5], [9], [11] e [14].

1.1 Divisibilidade em $\mathbb{Z}$

A Teoria dos Numéros se dedica ao estudos dos números inteiros e suas generalizações. O conjunto

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

é denominado conjunto dos números inteiros. Em particular, aos números $1,\ 2,\ 3, \ldots$ são chamados de números naturais e

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

é denominado o conjunto dos números naturais. Dentre os conceitos relacionado aos números inteiros, destaca-se o conceito de divisibilidade, definido a seguir.

Definição 1.1. *Dados dois inteiros a e b. Dizemos que b **divide** a, em símbolos, $b \mid a$, se existir um inteiro c tal que*

$$a = bc.$$

*Neste contexto, também dizemos que a é um **múltiplo** de b ou que a é **divisível** por b. Caso não exista o inteiro c dizemos que b **não divide** a e denotaremos por $b \nmid a$.*

Por exemplo, $8 \mid 72$, pois $72 = 8 \cdot 9$. Também, tem-se que $2 \nmid 3$. De fato, se 2 divide 3, então por definição, existe um inteiro c tal que $3 = 2c$. Daí, 3 seria um número par, mas isso é um absurdo. Portanto, $2 \nmid 3$.

Teorema 1.1. *Dados a, b, c e d números inteiros, valem as seguintes propriedades:*

(1) *Se $a \mid b$ e $b \mid c$, então $a \mid c$;*

(2) *Se $a \mid b$ e $c \mid d$, então $ac \mid bd$;*

(3) *Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$ $\forall x, y \in \mathbb{Z}$.*

Demonstração: **(1)** Se $a \mid b$ e $b \mid c$, então por definição, existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = bk_2$. Desse modo, concluímos das duas igualdades que $c = a(k_1k_2)$ e, assim, $a \mid c$.

(2) Se $a \mid b$ e $c \mid d$, então existem inteiros k_1 e k_2 de modo que $b = ak_1$ e $d = ck_2$. Logo, $bd = ac(k_1k_2)$. Portanto, $ac \mid bd$.

(3) Por hipótese, $b = ak_1$ e $c = ak_2$, com $k_1, k_2 \in \mathbb{Z}$. Daí, para quaisquer inteiros x e y, tem-se que

$$bx + cy = ak_1x + ak_2y = a(k_1x + k_2y),$$

isto é, $a \mid (bx + cy)$. ■

Um resultado clássico da Teoria dos Números é o Algoritmo da Divisão. O mesmo se encontra no famoso Livro VII dos Elementos de Euclides que viveu aproximadamente por volta do ano 350 antes de Cristo.

Teorema 1.2 (**Algoritmo de Euclides**). *Se a e b são inteiros, com $b \neq 0$, então existem únicos inteiros q e r tais que*

$$a = b \cdot q + r, \quad com \quad 0 \leq r < |b| .$$

Demonstração: Ver [14]. ■

Os inteiros q e r dados acima são chamados de **quociente** e **resto** da divisão, respectivamente.

Exemplo 1.1. *Determinar o quociente e o resto da divisão de a por b, quando:*

a) *$a = 91$ e $b = 11$;*

b) *$a = -107$ e $b = 23$;*

c) *$a = -1009$ e $b = -7$.*

Solução: a) Como $91 = 11 \cdot 8 + 3$ segue que o quociente é 8 e o resto é 3.

b) De início, para este caso, vamos determinar o quociente e o resto de 107 por 23. São eles 15 e 4 o resto e o quociente da divisão de 107 por 23, respectivamente, pois $107 = 23 \cdot 4 + 15$. Em seguida, manipularemos a igualdade $107 = 23 \cdot 4 + 15$ até chegarmos ao resultado. Multiplicando a igualdade $107 = 23 \cdot 4 + 15$ em ambos os membros por -1 temos que

$$-107 = 23 \cdot (-4) - 15 = 23 \cdot (-4) - 15 + 23 - 23 = 23 \cdot (-5) + 8.$$

Portanto, $q = -5$ e $r = 8$.

c) Para efetuar a divisão de $a = -1009$ por $b = -7$ efetuaremos de modo semelhante ao item b). Como $1009 = 7 \cdot 144 + 1$, então

$$-1009 = (-7) \cdot 144 - 1 = (-7) \cdot 144 - 1 + 7 - 7 = (-7) \cdot 145 + 6.$$

Logo, o quociente é 145 e o resto da divisão é 6.

Definição 1.2 (**Máximo Divisor Comum**). *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{N}$ é o **máximo divisor comum** de a e b, em símbolos $(a, b) = d$, quando as seguintes condições são satisfeitas:*

(1) *$d|a$ e $d|b$;*

(2) *Se $c|a$ e $c|b$, então $c|d$.*

Alguns autores denotam o máximo divisor comum d dos inteiros a e b por $mdc(a, b)$. Porém, neste trabalho vamos denotá-lo por $d = (a, b)$.

Um consequência bastante impotante sobre máximo divisor comum é o seguinte:

Teorema 1.3. *Se $d = (a, b)$, então existem inteiros x e y tais que*

$$d = ax + by.$$

Demonstração: Ver [14]. ■

Definição 1.3. *Dois inteiros a e b são ditos **primos entre si** quando $(a, b) = 1$.*

1.2 Números Primos

Pode-se dizer que os números primos são os números mais importantes da aritmética, ou melhor, da Teoria dos Números, uma vez que pelo Teorema Fundamental da Aritmética os números primos geram todos os números naturais, exceto o número 1. Por isso, dizemos que os números primos são os átomos da Teoria dos Números.

Definição 1.4 (**Número Primo**). *Diz-se que um inteiro positivo p é um **número primo** quando 1 e p são seus únicos divisores. Caso contrário, dizemos que p é um **número composto**.*

Pela definição, nota-se que 2 é o único número primo par. Também,

$$3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31 \text{ e } 37.$$

são todos números primos.

Vamos agora enunciar alguns resultados importantes sobre os números primos. O primeiro deles é o Teorema Fundamental da Aritmética, que é o principal resultado da Teoria dos Números.

Teorema 1.4 (**Teorema Fundamental da Aritmética**). *Todo número natural $n > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, como um produto de fatores primos. Isto é,*

$$n = p_1 p_2 ... p_r,$$

em que $p_1, p_2, ..., p_r$ são todos números primos.

Demonstração: Ver [14]. ■

Na fatoração de um número natural $n > 1$, pode ocorre o caso de aparecer repetidas vezes um mesmo fator primo de n. Por exemplo, $252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$. Neste caso, podemos agrupar os fatores primos que se repetem na fatoração de 252 da seguinte forma $252 = 2^2 \cdot 3^2 \cdot 7$. Desta maneira, enunciaremos a seguinte consequência do Teorema Fundamental da Aritmética.

Corolário 1.1. *Todo número natural $n > 1$ admite uma única fatoração, a menos da ordem, da forma*

$$n = p_1^{k_1} {p_2}^{k_2} ... p_r^{k_r},$$

onde $p_1, p_2, ..., p_r$ são números primos distintos e $k_1, k_2, ..., k_r$ são números naturais.

A fatoração acima é dita **fatoração canônica** do inteiro n ou simplesmente fatoração canônica de n.

Teorema 1.5. *Sejam a e b inteiros e p um número primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \mid a$, então a nossa afirmação esta provada. Caso contrário, se $p \nmid a$, então $(a, p) = 1$. Daí, pela Teorema 1.3 existem inteiros x e y tais que

$$ax + yp = 1.$$

Multiplicando ambos os lados dessa última igualdade por b, vem que

$$abx + ypb = b,$$

de modo que $p \mid b$, pois $p \mid ab$, o que prova o resultado. ■

O seguinte resultado é um teste de primalidade estabelecido pelo matemático grego Eratóstenes durante o século III a.c..

Teorema 1.6 (**Crivo de Eratóstenes**). *Se $n > 1$ for composto, então n possui, necessariamente, um divisor primo p tal que $p \leq \sqrt{n}$. Equivalentemente, se n não possuir divisores diferentes de 1, menores ou iguais a $\sqrt{n}$, então n é um número primo.*

Demonstração: Seja n um número composto. Assism, existem a e b tais que $n = ab$, com $1 < a, b < n$. Por outro lado, se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = ab > \sqrt{n}\sqrt{n} = n,$$

o que é uma contradição. Logo, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Sem perda de generalidade, suponhamos que $a \leq \sqrt{n}$. Agora, como $a > 1$ existe um primo p tal que $p \mid a$. Desde que $a \mid n$ segue que p divide, n com $p \leq a \leq \sqrt{n}$. Portanto, p é um divisor de n tal que $p \leq \sqrt{n}$. ■

Por exemplo, para determinar se 101 é primo, ou não, basta verificar sua divisibilidade pelos primos p tais que $p \leq \sqrt{101}$. Como os únicos primos menores ou iguais que $\sqrt{101}$ são 2, 3, 5 e 7 e, nenhum deles divide 101, segue que 101 é primo.

Um fato importante é que o conjunto dos números primos P é infinito. A prova foi dada por Euclides em seu livro Elementos usando o método de redução ao absurdo.

Teorema 1.7 (**Euclides**). *O conjunto dos números primos P é infinito.*

Demonstração: Por contradição, suponhamos que o conjunto dos números primos P seja finito, digamos, $P = \{p_1, p_2, ..., p_n\}$. Agora, consideremos o número natural a tal que

$$a = p_1 p_2 ... p_n + 1.$$

Pelo Teorema Fundamental da Aritmética, a pode ser escrito como produto de fatores primos e, como consequência, existe algum fator primo p de a tal que $a = pk$, com $k \in \mathbb{Z}$. Como por hipótese $p_1, p_2, ..., p_n$ são os únicos números primos, então $p = p_i$ para algum $i = 1, 2, ..., n$. Sem perca de generalidade, suponhamos que $p = p_1$. Assim,

$$pk = pp_2 ... p_n + 1,$$

ou melhor,

$$pk - pp_2 ... p_n = 1.$$

Logo, $p \mid 1$, o que é um absurdo. Portanto, o conjunto P dos números primos é infinito. ■

1.3 Congruências

O conceito e a notação de congruência foram introduzidos por Gauss no seu livro *Disquisitiones Arithmeticae* quando tinha 24 anos de idade no ano de 1801. As propriedades das congruências nos permite estudar resultados sobre divisibilidade com mais eficácia.

Definição 1.5. *Sejam a e b inteiros e m um número natural. Dizemos que a é **congruente** a b **módulo** m quando m divide a diferença $a - b$. Em símbolos,*

$$a \equiv b \, (mod \, m).$$

De acordo com a definição, tem-se que

$$a \equiv b\,(mod\,m) \Leftrightarrow m \mid (a-b).$$

Isto significa que $a = b + mk$ para algum inteiro k. Por exemplo, $7 \equiv 1\,(mod\,3)$, e $-17 \equiv 2\,(mod\,19)$, pois $3 \mid (7-1)$ e $19 \mid (-17-2)$. Por outro lado, se $m \nmid a-b$, então dizemos que a **é incongruente a** b **módulo** m, em símbolos,

$$a \not\equiv b\,(mod\,m).$$

A relação de congruência módulo m é uma relação de equivalência conforme vejamos abaixo.

Teorema 1.8. *Dados a, b e c números inteiros quaisquer, temos que:*

(1) $a \equiv a\,(mod\,m)$*;*

(2) *Se* $a \equiv b\,(mod\,m)$*, então* $b \equiv a\,(mod\,m)$*;*

(3) *Se* $a \equiv b\,(mod\,m)$ *e* $b \equiv c\,(mod\,m)$*, então* $a \equiv c\,(mod\,m)$.

Demonstração: **(1)** Para qualquer inteiro a tem-se que $a - a = 0 = 0 \cdot m$ e, portanto, por definição de congruência $a \equiv a\,(mod\,m)$.

(2) Por definição, $a \equiv b\,(mod\,m)$ implica que $m \mid (a-b)$. Logo, existe um inteiro k tal que $a - b = mk$. Daí, $b - a = m(-k)$, ou seja, $b \equiv a\,(mod\,m)$.

(3) Por hipótese, existem k_1 e k_2 inteiros tais que

$$a - b = mk_1 \quad \text{e} \quad b - c = mk_2.$$

Somando membro a membro as duas igualdades acima, vem que $a - c = m(k_1 + k_2)$. Portanto, $a \equiv c\,(mod\,m)$. ■

Outras propriedades relevantes ao estudo de congruência módulo m é dada pela seguinte:

Teorema 1.9. *Sejam a, b, c e d inteiros quaisquer. Então,*

(1) *Se* $a \equiv b\,(mod\,m)$ *e* $c \equiv d\,(mod\,m)$*, então*

$$a + c \equiv b + d\,(mod\,m) \quad e \quad ac \equiv bd\,(mod\,m);$$

(2) *Se* $a \equiv b\,(mod\,m)$*, então*

$$(a + c) \equiv (b + c)\,(mod\,m) \quad e \quad ac \equiv bc\,(mod\,m);$$

(3) *Se* $a \equiv b\,(mod\,m)$*, então* $a^k \equiv b^k\,(mod\,m)$ $\forall k \in \mathbb{N}$.

Demonstração: Ver [14]. ■

Teorema 1.10. *Sejam a, b e c inteiros quaisquer. Então*

$$ac \equiv bc\,(mod\, m) \Leftrightarrow a \equiv b\,(mod\, m/d),$$

em que $d = (c, m)$.

Demonstração: Ver [14]. ■

Corolário 1.2. *Sejam $ac \equiv bc\,(mod\, m)$ e $(c, m) = 1$. Então, $a \equiv b\,(mod\, m)$.*

Demonstração: De fato, se $ac \equiv bc\,(mod\, m)$, com $(c, m) = 1$, então segue direto do Teorema 1.9 que $a \equiv b\,(mod\, m)$. ■

Definição 1.6. *Chama-se* ***sistema completo de resíduos módulo*** *m todo conjunto $S = \{r_1, r_2, \ldots, r_m\}$ de m inteiros tais que para qualquer inteiro a é congruente módulo m a um único elemente de S e r_i é incongruente a r_j sempre que $i \neq j$.*

Por exemplo, cada um dos conjuntos

$$\{0, 1, 2\}, \quad \{1, 2, 3\} \quad \text{e} \quad \{-1, 6, 7\}$$

é um sistema completo de resíduos módulo 3.

Teorema 1.11. *O conjunto $S = \{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.*

Demonstração: Primeiramente, notemos que os elementos deste conjunto são dois a dois incongruentes módulo m. Com efeito, dados os inteiros r_i e r_j tais que $1 \leq r_i, r_j \leq m-1$, com $r_i \neq r_j$, então $-m < r_i - r_j < m$. Logo, m não divide $r_i - r_j$ e, consequentemente, r_i e r_j são incongruentes entre si módulo m. Por outro lado, pelo algoritmo da divisão com a e m, existem inteiros q e r tais que

$$a = mq + r, \quad \text{onde} \quad 0 \leq r < m.$$

Em termos de congruência,

$$a \equiv r\,(mod\, m).$$

Agora, como r assume valores de 0 a $m-1$ segue que o inteiro a é congruente módulo m a um único elemento de S. Portanto, $S = \{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m. ■

Definição 1.7. *Chama-se* ***congruência linear*** *toda congruência da forma*

$$ax \equiv b\,(mod\, m),$$

em que a e b são números inteiros, com $a \neq 0$, m um inteiro positivo e x é uma incógnita.

O estudo das congruências lineares se resume em determinar todas as soluções inteiras de

$$ax \equiv b\,(mod\, m).$$

Por exemplo, $x_0 = 4$ é solução de

$$7x \equiv 6\,(mod\, 11),$$

uma vez que $11 \mid (7 \cdot 4 - 6)$. Porém, vale observar que nem toda congruência linear tem solução, como por exemplo $2x \equiv 1\,(mod\, 4)$. De fato, por definição de congruência existe um inteiro k tal que $2x - 1 = 4k$, mas isso nos leva a um absurdo, pois o lado esquedo da igualdade é sempre ímpar para todo inteiro x, enquanto que no lado direito $4k$ é sempre par para qualquer inteiro k. Por isso, a congruência linear $2x \equiv 1\,(mod\, 4)$ não possui solução inteira. No sentido da busca de resultado mais geral da verificação da existência da solução inteira de $ax \equiv b\,(mod\, m)$ o resultado que segue é central.

Teorema 1.12. *A congruência linear $ax \equiv b\,(mod\, m)$ tem solução inteira se, e somente se, d divide b, em que $d = (a, m)$.*

Demonstração: De início, suponhamos que a congruência linear $ax \equiv b\,(mod\, m)$ tem solução inteira. Assim, existe um inteiro x_0 tal que $ax_0 \equiv b\,(mod\, m)$, ou melhor, $ax_0 - b = mk$, com $k \in \mathbb{Z}$, ou seja,

$$ax_0 - mk = b. \tag{1.1}$$

Por outro lado, sendo $d = (a, m)$ segue da igualdade (1.1) que d divide b. Reciprocamente, vamos supor que d divide b. Agora, como $d = (a, m)$, pelo Teorema 1.3 existem inteiros r e s tais que

$$d = ar + ms.$$

Por hipótese, existe $k \in \mathbb{Z}$ tal que $b = dk$. Com isso,

$$b = dk = (ar + ms)k = ark + msk.$$

Daí, $a(rk) \equiv b\,(mod\, m)$ e, portanto, $x_0 = rk$ é uma solução da congruência linear $ax \equiv b\,(mod\, m)$. ■

Uma consequência imediata é que a congruência linear $ax \equiv 1\,(mod\, m)$ tem solução se, e somente se, $(a, m) = 1$. Retornando a congruência $2x \equiv 1\,(mod\, 4)$, pode-se concluir que não possui solução inteira, uma vez que $(2, 4) \neq 1$.

O resultado seguinte é bastante importante na Teoria dos Números. O próprio foi demonstrado pelo matemático Fermat em 1640 e é chamado Teorema de Fermat, vejamos.

Teorema 1.13 (Teorema de Fermat). *Sejam p um número primo e a um inteiro tal que $p \nmid a$. Então,*

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

Demonstração: Ver [5]. ■

Vamos agora definir a função de Euler e suas consequências no sentido de nos conduzir a resultados posteriores sobre congruências quadráticas.

Definição 1.8. *Chama-se* ***função*** ϕ ***de Euler*** *a função* ϕ *definida para todo número natural* n *tal que* $\phi(n)$ *é igual ao número de inteiros positivos menores ou iguais a* n *que são primos com* n*.*

Em particular, $\phi(1) = 1$. Também, $\phi(8) = 4$, pois os únicos números naturais menores ou iguais que 8 relativamente primos com 8 são 1, 3, 5 e 7. A seguir apresentaremos resultados que facilitarão o cálculo da função $\phi(n)$ e, por fim, consideremos o Teorema de Euler.

Uma consequência da definição é que

$$\phi(n) = n - 1 \Leftrightarrow n \text{ é primo.}$$

Com efeito, se n é primo, então todos os números 1, 2,..., $n-1$ são primos relativo a n. Logo, $\phi(n) = n - 1$. Reciprocamente, vamos supor que n é um número composto sempre que $\phi(n) = n - 1$. Assim, existe um divisor d de n tal que $1 < d < n$. Consequentemente, $\phi(n) \leq n - 2$, pois entre os inteiros 1, 2,..., n tem-se de imediato que n e d não são relativamente primos com n. Portanto, n é primo.

Teorema 1.14. *Se* p *é primo e* k *é um inteiro tal que* $k \geq 1$*, então*

$$\phi(p^k) = p^k - p^{k-1}.$$

Demonstração: Sendo p um número primo, então os únicos números não primos menores que p^k com p^k são exatamente $1p$, $2p$, $3p$,..., $(p^{k-1})p$. Por isso, entre os inteiros 1, 2, 3,..., p^k existem $p^k - p^{k-1}$ números relativamente primos com p^k, isto é, $\phi(p^k) = p^k - p^{k-1}$. ■

Teorema 1.15. *Se* m *e* n *são números naturais tais que* $(m, n) = 1$*, então*

$$\phi(mn) = \phi(m)\phi(n).$$

Demonstração: Ver [9]. ■

O Teorema de Euler é uma generalização do Teorema de Fermat.

Teorema 1.16 (**Teorema de Euler**)**.** *Sejam* n *um número natural e* a *um inteiro tal que* $(a, n) = 1$*. Então,*

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

Demonstração: Ver [9]. ■

Definição 1.9. *Sejam n e a inteiros, com $n \geq 1$, tais que $(a, n) = 1$. A* ***ordem de*** *a* ***módulo*** *n, denotada por $ord_n(a)$, é o menor inteiro positivo k tal que*

$$a^k \equiv 1 \, (mod \, n).$$

Teorema 1.17. *Seja a um inteiro com $k = ord_n(a)$. Então, $a^t \equiv 1 \, (mod \, n)$ se, e somente se, $k \mid t$. Em particular, $k \mid \phi(n)$.*

Demonstração: Como $a^k \equiv 1 \, (mod \, n)$, tem-se que

$$a^{km} \equiv 1 \, (mod \, n), \quad \forall \; m \in \mathbb{N}.$$

Por outro lado, sendo $a^t \equiv 1 \, (mod \, n)$ segue pelo algoritmo da divisão que existem inteiros q e r tais que

$$t = kq + r, \quad \text{com} \quad 0 \leq r \leq k - 1.$$

Consequentemente,

$$1 \equiv a^t \equiv a^{kq+r} \equiv a^{kq} a^r \equiv a^r \, (mod \, n).$$

Mas, pela minimalidade da ordem de a módulo n, temos que $r = 0$ e, portanto, k divide t. Por fim, o Teorema de Euler assegura que $k \mid \phi(n)$. ■

Sobre o uso da notação de congruência pode-se gerar vários tipo de teste de primalidade. Os matemáticos Brillhart e Selfrifge em 1975 elaboraram o seguinte teste de primalidade baseado em congruência.

Teorema 1.18. *Seja n um número natural. Supõe-se que para todo fator primo q de $n - 1$ exista um inteiro $a > 1$ tal que*

(i) $a^{n-1} \equiv 1 \, (mod \, n)$;

(ii) $a^{\frac{n-1}{q}} \not\equiv 1 \, (mod \, n)$.

Então, n é primo.

Demonstração: É suficiente mostrar que $\phi(n) = n - 1$ e, como, $\phi(n) \leq n - 1$ basta mostrar que $n - 1$ divide $\phi(n)$. Suponhamos por absurdo que $n - 1$ não divide $\phi(n)$. Assim, existe um primo q e um inteiro $r \geq 1$ tais que $q^r \mid n - 1$ e $q^r \nmid \phi(n)$, sendo q^r a maior potência de q que divide $n - 1$. Agora, sejam $a > 1$ um inteiro e $k = ord_n(a)$. Daí, $k \mid n - 1$, pois $a^{n-1} \equiv 1 \, (mod \, n)$ e k não divide $\frac{n-1}{q}$, uma vez que $a^{\frac{n-1}{q}} \not\equiv 1 \, (mod \, n)$, isto é, se retirarmos o fator q de $n - 1$ implica que $k \nmid \frac{n-1}{q}$. Então, q^r divide k. Por outro lado, como $k \mid \phi(n)$ segue que $q^r \mid \phi(n)$ o que é um absurdo. Portanto, n é primo. ■

Capítulo 2

Congruências Quadráticas: Noções Fundamentais

Depois dos estudos levantado no capítulo anterior sobre congruências lineares é natural olhar para as congruências da forma $Ax^2 + Bx + C \equiv 0\,(mod\, n)$. Porém, em particular, apenas focalizaremos na solubilidade das congruências da particularidade $x^2 \equiv a\,(mod\, n)$ visto que a resolução em $\mathbb{Z}$ da primeira congruência se reduz à solução de um sistema de duas congruências cuja uma delas é do tipo da última e a outra linear. Conforme isto, neste capítulo, se faz necessário o estudo das soluções em $\mathbb{Z}$ de tais congruências para explorar resultados futuros como Critério de Euler, Símbolo de Legendre, Lema de Gaus e, especialmente, a Lei da Reciprocidade Quadrática.

2.1 Congruências Quadráticas

Estudaremos conguências da forma:

$$Ax^2 + Bx + C \equiv 0\,(mod\, n),$$

em que $A, B, C, n \in \mathbb{Z}$, $n > 1$ e $(A, n) = 1$. Essas congruências são denominadas de **congruências quadráticas**.

Ao longo do nosso estudo, vamos restringir o módulo a um número primo para facilitar nossos cálculos. No entanto, todo número maior que 1 é um produto de potências de números primos e, portanto, fica viável começarmos com o módulo sendo um inteiro positivo primo. Assim, vamos considerar a congruência quadrática

$$Ax^2 + Bx + C \equiv 0\,(mod\, p),$$

onde p é um número primo. Por outro lado, observamos que a congruência acima é equivalente a

$$4A^2x^2 + 4ABx + 4AC \equiv 0\,(mod\, p).$$

Mas, por ser

$$4A^2x^2 + 4ABx + 4AC = (2Ax + B)^2 - (B^2 - 4AC),$$

então, podemos escrever a congruência dada como

$$(2Ax + B)^2 \equiv (B^2 - 4AC) \, (mod\, p).$$

Fazendo $y = 2Ax + B$ e $\Delta = B^2 - 4AC$, temos a seguinte congruência

$$y^2 \equiv \Delta \, (mod\, p).$$

Resolver a congruência quadrática $Ax^2 + Bx + C \equiv 0 \, (mod\, p)$ é, portanto, equivalente a resolver o sistema de congruências abaixo:

$$\begin{cases} y^2 \equiv \Delta \, (mod\, p), \\ 2Ax + B \equiv y \, (mod\, p), \end{cases}$$

desde que as congruências tenham soluções.

Agora, como sabemos resolver congruências lineares, então apenas focalizaremos, daqui em diante, na congruência quadrática do tipo:

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

sendo p primo.

Notemos que se $(a, p) = p$, então $\alpha = pk$, com $k \in \mathbb{Z}$, se, e somente se, α é uma solução de

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

Com efeito, sendo $a = pq$, com $q \in \mathbb{Z}$, temos que

$$\alpha^2 - a = p^2k^2 - pq = p(pk^2 - q),$$

ou seja, α é uma solução de $x^2 \equiv a \, (mod\, p)$. A reciproca também é verdadeira, visto que se $\alpha^2 \equiv a \, (mod\, p)$, então $p \,|\, \alpha^2 - a$ e, como $p \,|\, a$, segue que $\alpha^2 = p(k + q)$, com $k \in \mathbb{Z}$. Logo, $p \,|\, \alpha$, pois p é primo e, portanto, a solução geral de $x^2 \equiv a \, (mod\, p)$ é da forma $x = p\beta$, em que $\beta \in \mathbb{Z}$.

Portanto, ao estudarmos congruências quadráticas da forma $x^2 \equiv a \, (mod\, p)$ vamos sempre assumir que $(a, p) = 1$ e em que p é um primo ímpar, pois para $p = 2$ a congruência dada tem sempre solução, conforme o teorema abaixo.

Teorema 2.1. *A congruéncia $x^2 \equiv a \, (mod\, 2)$ tem sempre solução.*

Demonstração: Se a é par, então $a = 2{\cdot}k$, com $k \in \mathbb{Z}$ e, assim, obviamente, $x = 0$ é uma solução de $x^2 \equiv a \, (mod\, 2)$. Se a é ímpar, então a pode ser escrito da forma $a = 2{\cdot}k + 1$. Logo, $x = 1$ é uma solução de $x^2 \equiv a \, (mod\, 2)$. Portanto, concluímos nossa demonstração. ■

Uma observação importante é que nem toda congruência $x^2 \equiv a\,(mod\,p)$ tem solução. Por exemplo, módulo 5,

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 4 \quad e \quad 4^2 \equiv 1.$$

Daí, $x^2 \equiv a\,(mod\,5)$ tem solução para $a = 0, 1$ ou 4 e não tem solução para $a = 2$ ou 3. Notemos que apenas analizamos a solução para os valores do conjunto $\{0,\ 1,\ 2,\ 3,\ 4\}$ que, por sua vez, é um sistema completo de resíduos módulo 5.

Notemos que $x^2 \equiv 0\,(mod\,p)$ tem solução se, e somente se, $x \equiv 0\,(mod\,p)$ tem solução. De fato, se $x^2 \equiv 0\,(mod\,p)$ tem solução, então existe um inteiro α tal que $\alpha^2 \equiv 0\,(mod\,p)$. Assim, $p \mid \alpha^2$ e, por p ser primo, $p \mid \alpha$. Logo, α é uma solção de $x \equiv 0\,(mod\,p)$. Reciprocamente, se $x \equiv 0\,(mod\,p)$ tem solução, digamos β, com $\beta \in \mathbb{Z}$, então $p \mid \beta$ e, por conseguinte, $p \mid \beta^2$, pois p é primo. Portanto, β é uma solução de $x^2 \equiv 0\,(mod\,p)$.

Vamos agora mostrar que se $p \nmid a$, então $x^2 \equiv a\,(mod\,p)$ tem exatamente duas soluções incongruentes entre si módulo p. Isto é o que provaremos no teorema seguinte:

Teorema 2.2. *Sejam p um primo ímpar e $(a, p) = 1$. Se a congruência $x^2 \equiv a\,(mod\,p)$ tem solução, então ela tem exatamente duas soluções incongruentes entre si módulo p, a saber, α e $p - \alpha$.*

Demonstração: Suponhamos que α é uma solução de $x^2 \equiv a\,(mod\,p)$, então $p - \alpha$ também o é, pois, $(p - \alpha)^2 \equiv \alpha^2\,(mod\,p)$. Logo,

$$(p - \alpha)^2 \equiv a\,(mod\,p).$$

Além disso, se $\alpha \equiv p - \alpha\,(mod\,p)$, então $2\alpha \equiv 0\,(mod\,p)$, o que implica que $p \,|\, 2\alpha$, mas como $p \,|\, \alpha^2 - a$ e $(2, p) = 1$, então teríamos que $p \,|\, a$ o que é uma contradição e, portanto, $p - \alpha$ é incongruente a α módulo p.

Por outro lado, seja β uma solução de $x^2 \equiv a\,(mod\,p)$. Assim, $\beta^2 \equiv \alpha^2 \equiv a\,(mod\,p)$ e, portanto, $\beta^2 - \alpha^2 = (\beta + \alpha)\cdot(\beta - \alpha) \equiv 0\,(mod\,p)$. Logo, $p \,|\, \beta + \alpha$ *ou* $p \,|\, \beta - \alpha$, o que implica que

$$\beta \equiv -\alpha\,(mod\,p) \quad ou \quad \beta \equiv \alpha\,(mod\,p).$$

Agora, como $p - \alpha \equiv -\alpha\,(mod\,p)$, obtemos que

$$\beta \equiv p - \alpha\,(mod\,p) \quad ou \quad \beta \equiv \alpha\,(mod\,p).$$

Com isto mostramos que, caso exista solução, existem exatamente duas soluções incongruentes entre si módulo p. ∎

Este teorema não é verdadeiro para o módulo composto. Por exemplo, $x^2 \equiv 1\,(mod\,8)$ tem quatros soluções, 1, 3, 5, e 7.

Em particular, a congruência quadrática $x^2 \equiv 1\,(mod\,p)$ é de muita importância no nosso estudo, com ela simplificaremos alguns resultados. O teorema a baixo nos diz que ele tem sempre solução.

Teorema 2.3. *A congruência quadrática $x^2 \equiv 1\,(mod\,p)$ tem exatamente duas soluções incongruentes módulo p, que são 1 e $p-1$.*

Demonstração: De imediato, $x = 1$ é uma solução e, pelo Teorema 2.2, $p-1$ também o é, de modo que são incongruentes entre si módulo p e são exatamente as duas soluções de $x^2 \equiv 1\,(mod\,p)$. ■

Exemplo 2.1. *Resolver a congruência quadrática*

$$x^2 + 3x - 5 \equiv 0\,(mod\,7).$$

Solução: Para resolver esta congruência, temos $A = 1, B = 3, C = -5$ e $\Delta = 3^2 - 4 \cdot 1 \cdot (-5) = 29$. De modo a resolver o seguinte sistema

$$\begin{cases} y^2 \equiv 29\,(mod\,7), \\ 2x + 3 \equiv y\,(mod\,7). \end{cases}$$

Temos que $y^2 \equiv 29 \equiv 1\,(mod\,7)$, cuja soluções incongruentes módulo 7 são 1 e 6. Agora, temos que resolver a congruência $2x + 3 \equiv y\,(mod\,7)$ para $y = 1$ e $y = 6$. Para $y = 1$, temos a seguinte congruência $2x \equiv 5\,(mod\,7)$, onde $x = 6$ é uma solução. Por outro lado, para $y = 6$, temos que $2x \equiv 3\,(mod\,7)$, em que $x = 5$ é uma solução. Logo, 6 e 5 são as únicas soluções incongrunetes entre si módulo 7. Portanto, a solução geral é

$$x \equiv 6 \; ou \; 5\,(mod\,7).$$

Exemplo 2.2. *Se $p > 3$, derterminar as duas soluções incongruentes módulo p de $x^2 \equiv 4\,(mod\,p)$.*

Solução: Seja y uma solução de $x^2 \equiv 4\,(mod\,p)$. Assim, $y^2 - 4 \equiv 0\,(mod\,p)$ o que implica que $(y-2)\cdot(y+2) \equiv 0\,(mod\,p)$, de modo que $p \mid y-2$ ou $p \mid y+2$. Em termos de congruência, temos que

$$y \equiv 2\,(mod\,p) \quad ou \quad y \equiv -2\,(mod\,p).$$

Como $-2 \equiv p-2\,(mod\,p)$, temos que as duas soluções incongruentes módulo p são 2 e $p-2$.

2.2 Resíduos Quadráticos

A ideia de resíduos quadráticos nos permite construir resultados mais sofisticados para o desenvolvimento dos tópicos subsequentes.

Definição 2.1. *Sejam $a, n \in \mathbb{Z}$, com $n > 1$, tais que $(a, n) = 1$. Dizemos que a é um* ***resíduo quadrático módulo*** *n (ou de n) quando a congruência quadrática $x^2 \equiv a\,(mod\,p)$ tem solução. Caso contrário, dizemos que a é um* ***residuo não-quadrático módulo*** *n (ou de n).*

Por exemplo, $3^2 \equiv 1\,(mod\,8)$, então 1 é um resíduo quadrático módulo 8. Por outo lado, 2 é um resíduo não-quadrático de 3. Com efeito, se α é uma solução de $x^2 \equiv 2\,(mod\,3)$, então $\alpha^2 \equiv 2\,(mod\,3)$, isto é, $3 \mid \alpha^2 - 2$ e, consequentemente, $3 \nmid \alpha$. Agora, pelo algoritmo da divisão

$$\alpha = 3k + 1 \quad ou \quad \alpha = 3k + 2,$$

com $k \in \mathbb{Z}$. Desse modo, para $\alpha = 3k + 1$ temos que

$$(3k + 1)^2 = 9k^2 + 6k + 1 \equiv 2\,(mod\,3),$$

o que implica que $3 \mid 1$, mas isto é um absurdo. Assim, se $\alpha = 3k + 2$ tem-se

$$(3k + 2)^2 = 9k^2 + 12k + 4 \equiv 2\,(mod\,3),$$

o que acarreta que $3 \mid 2$, o que é uma contradição. Portanto, 2 é um resíduo não-quadrático módulo 3.

A seguir apresentaremos dois resultados básicos, porém considéraveis.

Proposição 2.1. *Todo inteiro a é um resíduo quadrático módulo 2.*

Demonstração: Pelo Teorema 2.1 a congruência quadrática

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

tem sempre solução. Portanto, para todo inteiro a, a é um resíduo quadrático módulo 2. ■

Observamos que para todo p primo, 1 é um resíduo quadrático módulo p. Com efeito, conforme o Teorema 2.3 a congruência quadrática

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

tem sempre solução. Portanto, 1 é um resíduo quadrático módulo p, para todo p primo.

Notemos que se $a, b \in \mathbb{Z}$ e $a \equiv b\,(mod\,p)$, então a é um resíduo quadrático módulo p se, e somente se, b é um resíduo quadrático módulo p. De fato, basta mostrar que se $a \equiv b\,(mod\,p)$, então $x^2 \equiv a\,(mod\,p)$ tem solução se, e só se, $x^2 \equiv b\,(mod\,p)$ tem solução. Desse modo, se $x^2 \equiv a\,(mod\,p)$ tem solução, então existe $x_0 \in \mathbb{Z}$ tal que

$$x_0^2 \equiv a\,(mod\,p).$$

Ora, $a \equiv b\,(mod\,p)$ implica que $x_0^2 \equiv b\,(mod\,p)$. Com isto, x_0 é uma solução de $x^2 \equiv b\,(mod\,p)$. A recíproca é de modo análogo e, assim, fica provada nossa afirmação. Além disso, sabemos

que $A = \{0, 1, 2, ..., p-1\}$ é um sisema completo de resíduo módulo p, isto é, qualquer inteiro a é congruente módulo p a um único elemento de A. Assim, consideremos as seguintes classes residuais

$$\overline{0} = \{a \in \mathbb{Z} : a \equiv 0 \,(mod\, p)\},$$

$$\overline{1} = \{a \in \mathbb{Z} : a \equiv 1 \,(mod\, p)\},$$

$$\vdots$$

$$\overline{p-1} = \{a \in \mathbb{Z} : a \equiv p-1 \,(mod\, p)\}.$$

Por outro lado, como estamos estudando congruências da forma $x^2 \equiv a \,(mod\, p)$ sempre que $(a, p) = 1$, então pelo algoritmo da divisão segue que $a \equiv k \,(mod\, p)$ para algum $k = 1, 2, ..., p-1$. Por isso, tomemos o conjunto R_p de todas as classes residuais $\overline{a}$ tais que a é um resíduo quadrático de p. Simbolicamente,

$$\overline{a} \in R_p \Leftrightarrow x^2 \equiv a \,(mod\, p) \text{ tem solução.}$$

De forma ánaloga definimos o conjunto N_p das classes residuais $\overline{a}$ de modo que a é um resíduo não quadrático de p. Simbolicamente,

$$\overline{a} \in N_p \Leftrightarrow x^2 \equiv a \,(mod\, p) \text{ não tem solução.}$$

Vale ressaltar que

$$\overline{a_i} = \overline{a_j} \Leftrightarrow a_i \equiv a_j \,(mod\, p).$$

Dessa maneira, podemos denotar

$$R_p = \{\overline{a_1}, \overline{a_2}, ..., \overline{a_r}\},$$

com $1 \leq a_r < p$. O mesmo acontece para o conjunto N_p. Por isso,

$$R_p, N_p \subset \{\overline{0}, \overline{1}, ..., \overline{p-1}\} = \mathbb{Z}_p.$$

Obeservamos que $\overline{1} \in R_p$ para todo p primo.

Observação 2.1. *Ressaltamos que o conceito e as demais propriedade de classe residuais se encontram no Apêndice A.*

Proposição 2.2. *Sejam $a \in \mathbb{Z}$ e $p > 2$ primo. Então, a é um resíduo quadrático de p se, e só se, a classe residual $\overline{a} \in \mathbb{Z}_p$ é um quadrado perfeito em $\mathbb{Z}_p$.*

Demonstração: Sendo a um resíduo quadrático de p, então $\overline{a} \in R_p$. Logo, por definição,

$$\overline{a} \in R_p \Leftrightarrow x^2 \equiv a \,(mod\, p) \text{ tem solução} \Leftrightarrow \exists b \in Z \text{ tal que } b^2 \equiv a \,(mod\, p) \Leftrightarrow \overline{b}^2 = \overline{a},$$

o que prova o resultado. ■

Vamos considerar o número primo 7 e determinar os conjuntos R_7 e N_7. Para isto, devemos apenas considerar os quadrados dos elementos de $\{1, 2, ..., 6\}$. Com isto, temos que

$$1^2 \equiv 1\,(mod\,7) \quad 2^2 \equiv 4\,(mod\,7) \quad 3^2 \equiv 2\,(mod\,7),$$

$$4^2 \equiv 2\,(mod\,7) \quad 5^2 \equiv 4\,(mod\,7) \quad 6^2 \equiv 1\,(mod\,7).$$

Portanto,

$$R_7 = \{\overline{1}, \overline{2}, \overline{4}\} \;\; e \;\; N_7 = \{\overline{3}, \overline{5}, \overline{6}\}.$$

De modo analogo, para $p = 11$, obtemos que

$$R_{11} = \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\} \;\; e \;\; N_{11} = \{\overline{2}, \overline{6}, \overline{7}, \overline{8}, \overline{10}\}.$$

Observamos que o número das classes residuais dos resíduos quadráticos é igual ao número das classes residuais dos resíduos não quadráticos, isto para $p = 7$ e $p = 11$. Essa observação pode ser generalizada para todo primo p ímpar como consequência do teorema abaixo.

Teorema 2.4. *Se p é primo ímpar, então entre os inteiros $1, 2, ..., p-1$ existem $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ resíduos não-quadráticos módulo p.*

Demonstração: Consideremos os quadrados de $1, 2, ..., \frac{p-1}{2}$, ou seja,

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

A princípio, mostraremos que estes inteiros são incongruentes entre si módulo p. Sejam α e β interos, com $1 \leq \beta, \alpha \leq (p-1)/2$, e suponhamos que $\alpha^2 \equiv \beta^2\,(mod\,p)$. Consequentemente, da definição de congruência, diz que p divide $\alpha^2 - \beta^2$, ou melhor,

$$p \mid (\alpha + \beta)(\alpha - \beta).$$

Assim, sendo p primo, então $p \mid \alpha + \beta$ ou $p \mid \alpha - \beta$. Como $\alpha + \beta < p$, então p não divide $\alpha + \beta$. Por consequência, p divide $\alpha - \beta$. Por outro lado, $-p < \alpha - \beta < p$, o que implica que $\alpha - \beta = 0$, isto é, $\alpha = \beta$. Portanto, os quadrados são dois a dois incongruentes módulo p. Agora, notemos que se $k \in \{1, 2, ..., \frac{p-1}{2}\}$, então $p - k$ pecorre os inteiros

$$p-1, p-2, ..., \frac{p+1}{2}$$

e, ainda, que $(p-k)^2 \equiv k^2\,(mod\,p)$. Desse modo, pelo Proposição 2.3 os resíduos quadráticos módulo p pertencem as classes de congruências que contém os quadrados

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

Portanto, existem $\frac{p-1}{2}$ resíduos quadráticos entre os inteiros $1, 2, ..., p-1$. Depois disso, como os demais inteiros são resíduos não quadráticos e

$$(p-1) - \left(\frac{p-1}{2}\right) = \frac{p-1}{2},$$

segue que também existem $\frac{p-1}{2}$ resíduos não quadráticos entre os inteiros $1, 2, ..., p-1$. ■

Nosso objetivo é recolher o máximo de resultados possíveis desta teoria para que se tenha um conhemento amplo da Teoria dos Resíduos Quadráticos. Em particular, uma parte desse objetivo se resume em determinar quando um inteiro a é um resíduo quadrático módulo p ou não quadrático de p, ou seja, quando $\overline{a}$ pertence a R_p ou N_p. Desse modo, para determinar se $8p$, com $p > 5$ primo, é um resíduo quadrático módulo $p-2$, com $p-2$ primo, não é uma tarefa fácil. Para isto, devemos encontrar um inteiro quadrado b tal que p divida a diferença entre b^2 e $8p$. Isto é, queremos designar um inteiro b, se é que existe, tal que $b^2 \equiv 8p\,(mod\, p-2)$. De fato, esse inteiro b existe, a saber, $b = p^3 - 2p$. Com efeito,

$$(p^3 - 2p)^2 - 8p = p^6 - 4p^4 + 4p^2 - 8p = (p-2)(p^5 + 2p^4 + 4p).$$

Logo, $p-2$ divide $(p^3 - 2p)^2 - 8p$ e, portanto, $8p$ é um resíduo quadrático módulo $p-2$. Determinar o inteiro b em função de p não é um trabalho simples. Por isso, no capítulo seguinte vamos definir um símbolo de Legendre que facilitará a resoluções destes tipos de problemas.

Capítulo 3

Símbolo de Legendre

Notação matemática é uma linguagem cuja grafia se aplica dos símbolos matemáticos e o estudo do significado se apoia na lógica matemática. O ponto central da notação matemática é simplificar cálculos admiravelmente complicados e complexos, como também, evitar a limitação das descobertas matemáticas. Um grande exemplo disso é o símbolo " $\equiv$ " de congruência desenvolvida por Gauss.

Não muito diferente de Gauss, o matemático francês Adrien Marie Legendre (1752-1833) desenvolveu uma notação para abreviar quando a congruência $x^2 \equiv a\,(mod.\,p)$ tem ou não solução. No decorrer do seu trabalho sobre lei da reciprocidade quadrática (onde falaremos mais adiante) identroduziu o símbolo $\left(\frac{a}{p}\right)$ ou (a/p).

3.1 Critério de Euler

Vamos agora desenvolver um método que nos permitirão decidir quando um inteiro a é ou não um resíduo quadrático módulo p.

Definição 3.1. *Sejam p um primo ímpar e a um inteiro tal que $(a,p) = 1$. Definimos o* ***Símbolo de Legendre*** (a/p) *ou* $\left(\frac{a}{p}\right)$ *da seguinte forma:*

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

É também conveniente fazer $\left(\frac{a}{p}\right) = 0$ quando p divide a. Por exemplo, para $p = 7$, segue que

$$R_7 = \{\overline{1}, \overline{2}, \overline{4}\} \;\; e \;\; N_7 = \{\overline{3}, \overline{5}, \overline{6}\}.$$

Logo,

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1 \;\; e \;\; \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

E, além disso, para alguns multiplos de 7,

$$\left(\frac{7}{7}\right) = \left(\frac{14}{7}\right) = \left(\frac{21}{7}\right) = 0.$$

Vamos denominar, daqui em diante, o inteiro a de **numerador** e o primo p de **denominador** do símbolo de Legendre $\left(\frac{a}{p}\right)$.

A fim de avaliar o caráter quadrático para primos maiores que 2, apresentaremos a seguir o critério de Euler.

Teorema 3.1. ***(Critério de Euler)*** *Se p é um primo ímpar e a um inteiro tal que $(a, p) = 1$, então*

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

Demonstração: Inicialmente, notemos que as soluções de $x^2 \equiv 1\,(mod\, p)$ são $x \equiv \pm 1\,(mod\, p)$. Agora, como por hipótese $(a, p) = 1$, então pelo teorema de Fermat segue que

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

Portanto,

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

Suponhamos, agora, que $\left(\frac{a}{p}\right) = 1$. Daí, a congruência quadrática $x^2 \equiv a\,(mod\, p)$ tem solução, digamos $\alpha \in \mathbb{Z}$, isto é, $\alpha^2 \equiv a\,(mod\, p)$. Por outro lado, $(a, p) = 1$ implica que $(\alpha, p) = 1$. Logo, novamente pelo teorema de Fermat, $\alpha^{p-1} \equiv 1\,(mod\, p)$. Portanto,

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

Reciprocamente, consideremos o caso em que $\left(\frac{a}{p}\right) = -1$. Notemos que

$$a^{p-1} - 1 \equiv 0\,(mod\, p),$$

ou melhor,

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0\,(mod\, p).$$

Sendo a um resíduo não quadrático módulo p e usando o fato provado acima devemos ter $a^{\frac{p-1}{2}} \equiv -1\,(mod\, p)$ e, portanto, fica provado o Critério de Euler. ■

Por exemplo, para $a = 2$ e $p = 11$, temos que

$$\left(\frac{2}{11}\right) \equiv 2^{\frac{11-1}{2}} \equiv 2^5 \equiv 32 \equiv -1\,(mod\, 11).$$

Logo, como $\left(\frac{2}{11}\right)$ assume valores 1 ou -1, segue a igualdade $\left(\frac{2}{11}\right) = -1$ e, assim, pelo critério de Euler, 2 é um resíduo não-quadrático módulo $p = 11$.

O critério de Euler pode ser também enunciado da seguinte forma:

Teorema 3.2. *Se p é um primo ímpar e a um inteiro tal que $(a,p)=1$, então $x^2 \equiv a\,(mod\,p)$ tem solução se, e só se,*

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

ou não tem solução se, e só se,

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

Observamos que o critério de Euler nos diz quando $x^2 \equiv a\,(mod\,p)$ tem ou não solução. No caso em que tenha solução, o critério não nos dá nenhuma maneira de encontra-lás. Naturalmente, é possível substituir $x = 1, 2, 3, ...$ até que encontre uma solução, mas esse procedimente é longo e cansativo. Porém, o método a seguir é, por vezes, mais conveniente. Por exemplo, seja $x^2 \equiv 7\,(mod\,31)$. Através do critério de Euler, chegaremos que

$$\left(\frac{7}{31}\right) \equiv 7^{15} \equiv 1\,(mod\,31),$$

isto é, $x^2 \equiv 7\,(mod\,31)$ tem solução. Assim, para encontrar uma solução de $x^2 \equiv 7\,(mod\,31)$ vamos adicionar o módulo 31 ate chegar em um fator quadrado, ou seja,

$$x^2 \equiv 7 \equiv 38 \equiv 69 \equiv 100 \equiv 10^2\,(mod\,31).$$

De imediato, para $x = 10$ a congruência é satisfeita e, por conseginte, pelo Teorema 2.2, a outra solução é 21. Porém, para números primos relativamente grande esse método perde a eficiência, mas com mais trabalho, ou não, sempre teremos uma solução, caso a congruência dada tenha solução. Vejamos por exemplo, a congruência $x^2 \equiv 41\,(mod\,61)$ tem solução conforme o critério de Euler. Assim, temos que

$$x^2 \equiv 41 \equiv 102 \equiv 163 \equiv 224 \equiv 4^2 \cdot 14\,(mod\,61).$$

Agora, como

$$14 \equiv 75 \equiv 5^2 \cdot 3\,(mod\,61),$$

segue que $x^2 \equiv 4^2 \cdot 5^2 \cdot 3\,(mod\,61)$. Mas,

$$3 \equiv 64 \equiv 8^2\,(mod\,61).$$

Logo, $x^2 \equiv 4^2 \cdot 5^2 \cdot 8^2 \equiv 160^2\,(mod\,61)$ e, por ser, $160 \equiv 38\,(mod\,61)$ concluímos que $x^2 \equiv 38^2\,(mod\,61)$. Cosequentemente, as duas soluções são 38 e 23.

Por outro lado, não é conveniente verificar se $x^2 \equiv 1009\,(mod\,20023)$ tem solução pelo critério de Euler. Mas, com alguns resultados adicionais, podemos avaliar o símbolo $\left(\frac{1009}{20023}\right)$ com certa facilidade. Vejamos alguns resultados.

Teorema 3.3. *Sejam $p > 2$ e $(a,p) = 1$. O símbolo de Legendre tem as seguintes propiedades:*

(1) *Se $a \equiv b\,(mod\,p)$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;*

(2) $\left(\frac{a^2}{p}\right) = 1$;

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

Demonstração: **(1)** Sendo $a \equiv b\,(mod\,p)$, então

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

Agora, pelo critério de Euler, vem que

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

Como o símbolo de Legendre assume valores 1 e -1 e $p > 2$, temos a seguinte igualdade

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

(2) Por hipótese, $(a, p) = 1$. Logo, $(a^2, p) = 1$, pois p é um número primo e, assim, $\left(\frac{a^2}{p}\right) \neq 0$. Por outro lado, a congruência quadrática $x^2 \equiv a^2\,(mod\,p)$ tem solução, em particular, a. Portanto, $\left(\frac{a^2}{p}\right) = 1$.

(3) Inicialmente, pelo critério de Euler,

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

Agora, como $\left(\frac{-1}{p}\right)$ e $(-1)^{\frac{p-1}{2}}$ assumem valores 1 e -1 e $p > 2$ é primo, segue a igualdade

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

■

Uma breve observação é que sendo $a = p - 1$, então

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

uma vez que $p - 1 \equiv -1\,(mod\,p)$.

Exemplo 3.1. *Avaliar o símbolo de Legendre* $\left(\frac{3}{29}\right)$.

Solução: Avaliar o símbolo de Legendre $\left(\frac{3}{29}\right)$ é determinar se a congruência $x^2 \equiv 3\,(mod\,29)$ tem ou não solução. Por isso, pelo Critério de Euler,

$$\left(\frac{3}{29}\right) \equiv 3^{\frac{29-1}{2}} \equiv 3^{14}\,(mod\,29).$$

Por outro lado, como $3^3 \equiv -2\,(mod\,29)$, ou ainda, $3^{12} \equiv (-2)^4 \equiv 16\,(mod\,29)$, segue que

$$3^{14} \equiv 16 \cdot 3^2 \equiv 144 \equiv -1\,(mod\,29).$$

Por transitividade, tem-se que $\left(\frac{3}{29}\right) \equiv -1\,(mod\,29)$ e, por conseguinte, $\left(\frac{3}{29}\right) = -1$. Portanto, a congruência quadrática $x^2 \equiv 3\,(mod\,29)$ não tem solução.

3.2 Propriedades Multiplicativas

O Símbolo de Legendre pode ser visto como uma função. Para cada $p \in \mathbb{N}$, com $p > 2$ primo, seja a função $f_p : \mathbb{Z} \longrightarrow \{0, \pm 1\}$ definida como uma regra que permite associar, de modo bem determinado, a cada elemento $a \in \mathbb{Z}$, um único elemento $f_p(a) \in \{0, \pm 1\}$, de modo que $f_p(a) = \left(\frac{a}{p}\right)$. Assim, a função f_p fica definida por

$$f_p(a) = \begin{cases} +1 & \text{se} \quad \overline{a} \in R_P, \\ 0 & \text{se} \quad p \,|\, a, \\ -1 & \text{se} \quad \overline{a} \in N_P. \end{cases}$$

Este fato é de extrema importância na teoria das congruências quadráticas, porque poderemos simplificar cálculos consideravelmente difíceis. Mais adiante, mostraremos mediante a um exemplo a sua importância, mas antes disso consideremos o seguinte:

Definição 3.2. *Uma função $f : A \longrightarrow B$ diz-se uma* ***função totalmente multiplicativa*** *se*

$$f(ab) = f(a)f(b),$$

para todos $a, b \in A$

Teorema 3.4. *O símbolo de Legendre é uma função totalmente multiplicativa.*

Demonstração: Basta mostra que para cada $p > 2$ primo, $f_p(ab) = f_p(a)f_p(b)$ para todos a e b em $\mathbb{Z}$. Isto é,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \ \forall\, a, b \in \mathbb{Z}.$$

Primeiramente, consideremos que $(a, p) = 1$ e $(b, p) = 1$. Assim, pelo critério de Euler,

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

Como o símbolo de Legendre assume somente valores 1 e -1 e como $p > 2$, a congruência acima implica a igualdade

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

Por outro lado, se $p|ab$, então $p|a$ ou $p|b$, pois p é primo. Logo, $\left(\frac{ab}{p}\right) = 0$ e $\left(\frac{a}{p}\right) = 0$ *ou* $\left(\frac{b}{p}\right) = 0$, o que também mostra a igualdade. Portanto, o símbolo de Legendre é uma função totalmente multiplicativa. ■

Generalizando, temos que se $a_1, a_2, ..., a_n$ são inteiros quaisquer e $p > 2$ é primo, então usando indução matemática sobre n temos que

$$\left(\frac{a_1 a_2 ... a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) ... \left(\frac{a_n}{p}\right).$$

De fato, para $n = 1$ a igualdade é imediata. Além disso, para $n = 2$ o Teorema 3.4 garante. Agora suponhamos que para $n = k$, $k \geq 2$, tem-se

$$\left(\frac{a_1 a_2 ... a_k}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) ... \left(\frac{a_k}{p}\right).$$

Desse modo, para $a_{k+1} \in \mathbb{Z}$ qualquer, segue que

$$\left(\frac{(a_1 a_2 ... a_k)a_{k+1}}{p}\right) = \left(\frac{a_1 a_2 ... a_k}{p}\right)\left(\frac{a_{k+1}}{p}\right).$$

Logo, por hipótese,

$$\left(\frac{a_1 a_2 ... a_k a_{k+1}}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) ... \left(\frac{a_k}{p}\right)\left(\frac{a_{k+1}}{p}\right).$$

O que prova nossa afirmação.

Uma decorrência bastante relevante do teorema acima é dada pelo seguinte resultado:

Corolário 3.1. *Dados $a, b \in \mathbb{Z}$ e p um primo ímpar. Então,*

(1) *Se $\overline{a}, \overline{b} \in R_p$, então $\overline{a} \cdot \overline{b} \in R_p$;*

(2) *Se $\overline{a}, \overline{b} \in N_p$, então $\overline{a} \cdot \overline{b} \in R_p$;*

(3) *Se $\overline{a} \in R_p$ e $\overline{b} \in N_p$, então $\overline{a} \cdot \overline{b} \in N_p$.*

Demonstração: (1) Se $\overline{a}, \overline{b} \in R_p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. Desse modo,

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1 \cdot 1 = 1.$$

Ou seja, $a \cdot b$ é um resíduo quadrático módulo p e, por definição, $\overline{a} \cdot \overline{b} \in R_p$

(2) Se $\overline{a}, \overline{b} \in N_p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. Logo,

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1) \cdot (-1) = 1.$$

Portanto, $\overline{a} \cdot \overline{b} \in R_p$.

(3) Por fim, $\overline{a} \in R_p$ e $\overline{b} \in N_p$, então temos que $\left(\frac{a}{p}\right) = 1$ e $\left(\frac{b}{p}\right) = -1$. Daí,

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1 \cdot (-1) = -1,$$

o que implica que $a \cdot b$ é um resíduo não quadrático de p e, por consequência, $\overline{a} \cdot \overline{b} \in N_p$. ■

Uma outra consequência bastante interesante do Teorema 3.4 é que dados $p > 2$ primo e a um inteiro tal que $(a, p) = 1$, então, $\left(\frac{a^k}{p}\right) = \left(\frac{a}{p}\right)^k$ para todo $k \in \mathbb{N}$. Com efeito,

$$\left(\frac{a^k}{p}\right) = \left(\frac{\overbrace{a \cdot a \cdot ... \cdot a}^{n \text{ fatores}}}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) ... \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^k.$$

É claro que para $k = 0$ a igualdade também ocorre.

De modo geral, se considerarmos p um número primo ímpar e a um inteiro tais que $|a| > 1$ e $(a, p) = 1$, a fatoração canônica de a em fatores primos é da forma $a = \pm 2^{k_0} p_1^{k_1} ... p_r^{k_r}$ em que $p_1, ..., p_r$ são primos distintos, $k_1, ..., k_r$ são naturais e $k_0 \in \mathbb{N} \cup \{0\}$. Notemos que p não é nenhum dos primos p_i, com $i = 1, 2, ..., r$, visto que p não divide a. Então,

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{k_0}\left(\frac{p_1}{p}\right)^{k_1} ... \left(\frac{p_r}{p}\right)^{k_r}.$$

Proposição 3.1. *Sejam $k \in \mathbb{N}$ e a um inteiro de maneira que $(a, p) = 1$. Então,*

$$\left(\frac{a}{p}\right)^k = \begin{cases} 1 & \text{se } k \text{ é par,} \\ \left(\frac{a}{p}\right) & \text{se } k \text{ é ímpar.} \end{cases}$$

Demonstração: De fato, pelo algoritmo da divisão $k = 2q$ ou $k = 2q + 1$, com $q \in \mathbb{Z}$. Assim, para $k = 2q$ tem-se que

$$\left(\frac{a}{p}\right)^k = \left(\frac{a}{p}\right)^{2q} = \left(\frac{a^2}{p}\right)^q = 1.$$

Para $k = 2q + 1$,

$$\left(\frac{a}{p}\right)^k = \left(\frac{a}{p}\right)^{2q+1} = \left(\frac{a}{p}\right)^{2q}\left(\frac{a}{p}\right) = \left(\frac{a^2}{p}\right)^q\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right).$$

■

A Proposição 3.1 aplicada na observação feita acima facilita o processo de avaliar o Símbolo de Legendre $\left(\frac{a}{p}\right)$. Por exemplo, como $72 = 2^3 \cdot 3^2$, então para avaliar $\left(\frac{72}{83}\right)$ basta avaliar $\left(\frac{2}{83}\right)$. Porém, notemos que esse processo não é tão simples como parece, pois dado o inteiro $a \in \mathbb{Z}$ suficientemente grande, determinar sua fatoração é uma tarefa árdua, por vezes quase impossível.

Vamos mostrar alguns exemplos de como o Teorema 3.4 é útil.

Exemplo 3.2. *Mostre que 2592 é um resíduo quadrático módulo* 23.

Solução: Devemos mostrar que $x^2 \equiv 2592\,(mod\,23)$ tem solução, isto é, $\left(\frac{2592}{23}\right) = 1$. Já que o símbolo de Legendre é uma função totalmente multiplicativa e por $2^3 \cdot 3^2 \cdot 6^2$ ser a fatoração de potências de primos de 2592, ocorre que

$$\left(\frac{2592}{23}\right) = \left(\frac{2^3 \cdot 3^2 \cdot 6^2}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{2^2}{23}\right)\left(\frac{3^2}{23}\right)\left(\frac{6^2}{23}\right).$$

Por isso, avaliar o Símbolo de Legendre $\left(\frac{2592}{23}\right)$ equivale a avaliar $\left(\frac{2}{23}\right)$, pois $\left(\frac{2^2}{23}\right) = \left(\frac{3^2}{23}\right) = \left(\frac{6^2}{23}\right) = 1$. Logo,

$$\left(\frac{2592}{23}\right) = \left(\frac{2}{23}\right).$$

Sendo assim, pelo famoso critério de Euler,

$$\left(\frac{2}{23}\right) \equiv 2^{\frac{23-1}{2}} \equiv 2^{11} \,(mod\, 23).$$

Por outro lado, $2^5 \equiv 9\,(mod\, 23)$ e, então, elevando ambos os membros ao quadrado desta conngruência quadrática teremos

$$2^{10} \equiv 9^2 = 81 \equiv 12\,(mod\, 23),$$

que é equivalente a

$$2^{11} \equiv 24 \equiv 1\,(mod\, 23).$$

Portanto, $\left(\frac{2592}{23}\right) = 1$ e, por conseguinte, 2592 é um resíduo quadrático módulo 23.

Exemplo 3.3. *Mostre que se a é um resíduo quadrático de p e $a \cdot b \equiv 1\,(mod\, p)$, então b é um resíduo quadrático módulo p.*

Solução: Por hipótese, $\left(\frac{a}{p}\right) = 1$ e $a \cdot b \equiv 1\,(mod\, p)$. Assim, pelo item (1) do Teorema 3.3 devemos ter

$$\left(\frac{ab}{p}\right) = \left(\frac{1}{p}\right).$$

Agora, pelo Teorema 2.3, $\left(\frac{1}{p}\right) = 1$ para todo primo p. Logo,

$$\left(\frac{ab}{p}\right) = 1.$$

Como a é um resíduo quadrático de p e o símbolo de Legendre é uma função totalmente multiplicativa, temos que

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1 \Longrightarrow \left(\frac{b}{p}\right) = 1,$$

isto é, b é um resíduo quadrático módulo p.

Exemplo 3.4. *Sendo p primo ímpar e a o menor resíduo não quadrático positivo módulo p, prove que $a < 1 + \sqrt{p}$.*

Solução: Seja b um inteiro positivo tal que

$$(b-1)a < p < ba.$$

Multiplicando por -1 em ambos os lados da desigualdade, temos que

$$-ab < -p < a - ab.$$

Agora, adicionando ab em ambos os lados da última desigualdade, obtemos $0 < ab - p < a$, isto é, $ab - p$ é um inteiro menor que a. Logo, por hipótese, $\left(\frac{ab-p}{p}\right) = 1$, pois a é o menor resíduo não quadrático. Por outro lado, como $ab - p \equiv ab\,(mod\, p)$ vem que $\left(\frac{ab}{p}\right) = 1$. Por isso,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -\left(\frac{b}{p}\right) \Longrightarrow \left(\frac{b}{p}\right) = -1.$$

Daí, concluímos que $b \geq a$. Ora, como

$$(a-1)^2 = a^2 - 2a + 1 < a^2 - a \leq ab - a$$

e $0 < ab - p < a$, ou melhor, $0 < ab - a < p$ segue que $(a-1)^2 \leq ab - a < p$ implica em $a < 1 + \sqrt{p}$.

3.3 Caracterização dos Primos $p > 2$ para os Quais -1 e 2 são Resíduos Quadráticos

Observamos pelo que já foi visto que para qualquer primo $p > 2$ o inteiro 1 é um resíduo quadrático módulo p. O que faremos aqui é a caracterização dos primos $p > 2$ para os quais -1 e 2 são resíduos quadráticos ou não módulo p. Começamos, inicialmente, pelo inteiro -1.

Teorema 3.5. *Para p primo ímpar, temos que*

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & se \quad p \equiv 1\,(mod\,4), \\ -1 & se \quad p \equiv 3\,(mod\,4). \end{cases}$$

Demonstração: Como $p > 2$ é primo, então pelo algoritmo da divisão,

$$p = 4k + 1 \quad ou \quad p = 4k + 3,$$

com $k \in \mathbb{Z}$. Em termos de congruências, as igualdades acima implicam que

$$p \equiv 1\,(mod\,4) \quad ou \quad p \equiv 3\,(mod\,4).$$

Por outro lado, sabemos que pelo item (3) do Teorema 3.3

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

Mas, sendo $p = 4k + 1$,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{(4k+1)-1}{2}} = (-1)^{2k} = 1.$$

Logo, $\left(\frac{-1}{p}\right) = 1$ para $p \equiv 1\,(mod\,4)$. Agora, sendo $p = 4k + 3$ segue que

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{(4k+3)-1}{2}} = (-1)^{2k+1} = -1.$$

Portanto, $\left(\frac{-1}{p}\right) = -1$ se $p \equiv 3\,(mod\,4)$ e, assim, concluímos a demonstração. ■

No teorema acima, caracterizamos os primos $p > 2$ para os quais -1 é um resíduo quadrático ou não módulo p. Notemos que a mesma caracterização vale para o inteiro $p - 1$, pois $p - 1 \equiv -1\,(mod\,p)$. Por isso, para saber se a congruência $x^2 \equiv 40\,(mod\,41)$ tem ou não solução basta notar que $40 \equiv -1\,(mod\,41)$ e $41 \equiv 1\,(mod\,4)$. Posto isso, segue do resultado acima que $\left(\frac{40}{41}\right) = 1$. Agora, vamos caracterizar os mesmos primos para os quais a congruência quadrática $x^2 \equiv 2\,(mod\,p)$ tem ou não solução. Consideremos antes o seguinte:

Teorema 3.6. *Sejam 2 o numerador e p o denominador do símbolo de Legendre, com $p > 2$. Então,*

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

Demonstração: Nesta demonstração, vamos tomar os valores de r variando de 1 a $\frac{p-1}{2}$, ou seja, $r = 1, 2, ..., \frac{p-1}{2}$. Consideremos as seguintes congruências $p - r \equiv r(-1)^r \,(mod\, p)$ para r ímpar e $r \equiv r(-1)^r \,(mod\, p)$ para r par. Com efeito, pelo algoritmo da divisão, $r = 2k$ ou $r = 2k + 1$, com $k \in \mathbb{Z}$. Se $r = 2k$,

$$r \equiv r(-1)^r \equiv r(-1)^{2k} \equiv r \,(mod\, p).$$

Para $r = 2k + 1$,

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

Portanto, as duas congruências se verificam. Desse modo, se considerarmos as $\frac{p-1}{2}$ congruências

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

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

$$p - 3 \equiv 3(-1)^3 \,(mod\, p),$$

$$4 \equiv 4(-1)^4 \,(mod\, p),$$

$$\vdots$$

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

sendo $a = \frac{p-1}{2}$ se a for par ou $a = p - \frac{p-1}{2}$ se a for ímpar. Observamos que os números do lado esquerdo de cada congruência acima é par. Por isso, multiplicando membro a membro todas as congruências consideradas, teremos do lado esquerdo os produtos dos números pares compreendidos entre os números de 1 a p, enquanto do lado direito teremos o produto dos números de 1 a $\frac{p-1}{2}$ vezes $(-1)^{1+2+...+\frac{p-1}{2}}$. Isto é,

$$2 \cdot 4 \cdot 6 \cdot ... \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot \frac{p-1}{2} \cdot (-1)^{1+2+...+\frac{p-1}{2}} \,(mod\, p),$$

ou melhor,

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

Por outro lado, como $(\left(\frac{p-1}{2}\right)!, p) = 1$, podemos cancelar o fator $\left(\frac{p-1}{2}\right)!$ da ultima congruência e, por conseguinte

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

Agora, pelo Critério de Euler,

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

e, por transitividade,

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

o que implica que

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

■

Diante disto, provaremos a caracterização dos primos $p > 2$ para os quais 2 é resíduos quadrático ou não de p.

Teorema 3.7. *Para p um primo ímpar, temos*

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

Demonstração: Usando o teorema anterior, basta verificar os casos para $p \equiv \pm 1 \,(mod\, 8)$ e $p \equiv \pm 3 \,(mod\, 8)$. Assim, para $p \equiv 1 \,(mod\, 8)$ vem que $p = 8k + 1$, com $k \in \mathbb{Z}$. Logo,

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

Consequentemente,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2k(4k+1)} = 1.$$

Da mesma forma, para $p \equiv -1 \,(mod\, 8)$ temos que $p = 8k - 1$. Por isso,

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

Ou seja, $\frac{p^2-1}{8}$ é par e, por conseguinte, $\left(\frac{2}{p}\right) = 1$. De modo análogo, sendo $p \equiv 3 \,(mod\, 8)$, por definição de congruência, existe um inteiro k tal que $p = 8k + 3$. Com isto,

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8k+2)(8k+4)}{8} = (2k+1)(4k+1),$$

de maneira que $\frac{p^2-1}{8}$ é ímpar e, portanto, $\left(\frac{2}{p}\right) = -1$. Por fim, não muito diferente, consideremos p da forma $8k - 3$, isto é, $p = 8k - 3$. Desse modo,

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8k-4)(8k-2)}{8} = (2k-1)(4k-1),$$

acarretando que $\frac{p^2-1}{8}$ é ímpar. Portanto, $\left(\frac{2}{p}\right) = -1$ e, assim, o teorema esta demonstrado. ■

Pelo Teorema Fundamental da Aritmética, todo número inteiro a tal que $|a| > 1$ pode ser escrito de forma única, a memos da ordem dos fatores, como pruduto de números primos. Digamos, $a = \pm 2^{k_0} p_1^{k_1} ... p_r^{k_r}$ em que p_i são primos distintos, $k_i \in \mathbb{N}$ para todo $i = 1, 2, ..., r$ e $k_0 \in \mathbb{N} \cup \{0\}$. Assim, dado um primo $p > 2$ com $(a, p) = 1$, tem-se que

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right)^{k_0} \left(\frac{p_1}{p}\right)^{k_1} ... \left(\frac{p_r}{p}\right)^{k_r}.$$

Por isso, para avaliar o símbolo de Legendre $\left(\frac{a}{p}\right)$ equivale a avaliar os símbolos $\left(\frac{\pm 1}{p}\right)$, $\left(\frac{2}{p}\right)$ e $\left(\frac{p_i}{p}\right)$ para cada $i = 1, 2, ..., r$. Desse modo, como já caracterizamos os primos $p > 2$ para os quais ± 1 e 2 são resíduos quadráticos ou não de p, resulta caracterizar os mesmos primos para os quais p_i seja ou não um resíduo quadrático módulo p.

De modo geral, a teoria da caracterização para os primos $p > 2$ para os quais a é um resíduo quadrático ou não módulo p se reduz a tomar o inteiro a sendo um número primo ímpar. Em particular, para $a = 3$ a caracterização dos primos $p > 2$ é dada por

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{se } \ p \equiv \pm 1 \, (mod\, 12), \\ -1 & \text{se } \ p \equiv \pm 5 \, (mod\, 12). \end{cases}$$

Porém, a resolução deste problema, diante dos resultados já obtidos, é bastante trabalhosa e enfadonho. Para primos $q > 3$ fica muito mais díficil determinar a sua caracterização para os primos $p > 2$ e, principalmente, encontrar a sua solução. Mas, o que faremos no capítulo seguinte é aprensentar e demonstrar um resultado classíco da Teoria dos Números, a saber, Lei da Reciprocidade Quadrática, que falicitará a resolução destes tipos de problemas.

Capítulo 4

Lei da Reciprocidade Quadrática

A Lei da Reciprocidade Quadrática é um resultado de grande importância na Teoria Elementar dos Números. Ela também é de muita importância na Teoria Algébrica dos Números. Neste capítulo, vamos nós ater a resultados clássicos da Teoria Elementar dos Números. A mesma conecta a solução de duas congruências quadráticas $x^2 \equiv q\,(mod\,p)$ e $x^2 \equiv p\,(mod\,q)$ onde p e q são primos ímpares distintos. Também, vamos introduzuir um resultado que é devido a Gauss. Em sequência enunciaremos e demonstraremos, assim como suas consequências, a Lei da Reciprocidade Quadrática. Por fim, vamos caracterizar os primos $p > 2$ para os quais 3, 5, 7 e 11 são resíduos quadráticos módulo p.

4.1 Lema de Gauss

Inicialmente, antes de enunciar e demonstrar o Lema de Gauss, vamos considerar um caso particular com a finalidade de ilustrar no que será feito na demonstração do suposto Lema a considerar.

Sejam $a = 5$ e $p = 11$. Calculemos, agora, os restos dos seguintes números por 11:

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

cujo restos módulo 11 são 5, 10, 4, 9 e 3, respectivamente. Assim sendo, notemos que entre os restos considerados 3, 4 e 5 são menores que $\frac{11}{5}$ e, além disso, considerando os restos maiores que $\frac{11}{5}$ e tomando os números 11-9 e 11-10 obtemos os números 2 e 1, nesta ordem. Observamos ainda, que 2 e 1 juntamente com os restos menores que $\frac{11}{5}$ formam os números naturais de 1 a 5. Por fim, existem $r = 2$ restos maiores que $\frac{11}{5}$ e, ainda,

$$\left(\frac{a}{p}\right) = \left(\frac{5}{11}\right) = (-1)^2 = 1.$$

De fato, pelo Critério de Euler,

$$\left(\frac{5}{11}\right) \equiv 5^{\frac{11-1}{2}} \equiv 5^5 \equiv 5^3 \cdot 5^2 \equiv 4 \cdot 3 \equiv 1\,(mod\,11),$$

implicando que $\left(\frac{5}{11}\right) = 1$.

Posto isto, faremos exatamente o que foi feito acima, ou seja, sendo p primo ímpar e r o número dos restos da divisão dos números $1a, 2a, ..., \frac{p-1}{2}a$ por p que são menores que $\frac{p}{2}$, mostraremos que $\left(\frac{a}{p}\right) = (-1)^r$.

Teorema 4.1. *Sejam $p > 2$ um número primo, a um inteiro tal que $(a, p) = 1$ e r o número de inteiros do conjunto*

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

que têm restos módulo p maiores que $\frac{p}{2}$. Então,

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

Demonstração: Tomemos os inteiros

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

O algoritmo da divisão garante que os restos dos inteiros acima módulo p são menores que p. Daqui em diante, pasaremos a denotar por $a_1, a_2, ..., a_s$ os restos menores que $\frac{p}{2}$ e, por, $b_1, b_2, ..., b_r$ os restos maiores que $\frac{p}{2}$ módulo p. Nesta ocasião, multiplicando membro a membro todas as congruências que foram obtidos os restos, tantos menores e maiores que $\frac{p}{2}$, obtemos a seguinte congruência

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

ou melhor,

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{s} a_i \prod_{i=1}^{r} b_i \,(mod\, p). \tag{4.1}$$

Agora, temos que $p - b_i$ é menor que $\frac{p}{2}$ para todo $i = 1, 2, ..., r$. Com efeito, sendo $b_i > \frac{p}{2}$, então

$$-b_i < \frac{p}{2} \Leftrightarrow p - b_i < p - \frac{p}{2} \Leftrightarrow p - b_1 < \frac{p}{2}.$$

Além do mais, $a_1, a_2, ..., a_s, p - b_1, p - b_2, ..., p - b_r$ são dois a dois incongruentes módulo p. De fato, mostremos primeiramente que os elementos de S são incongruentes entre si módulo p. Por absurdo, se $\alpha a \equiv \beta a \,(mod\, p)$, em que $1 \leq \alpha, \beta \leq \frac{p-1}{2}$ e $\alpha \neq \beta$, digamos $\alpha > \beta$, então $\alpha \equiv \beta \,(mod\, p)$, pois $(a, p) = 1$. Mas, isto é impossível, visto que $0 < \alpha - \beta < p$. Assim, se $a_i \equiv p - b_j \,(mod\, p)$, ou seja, $a_i \equiv -b_j \,(mod\, p)$, então como existem inteiros k_1 e k_2, com $1 \leq k_1, k_2 \leq \frac{p-1}{2}$, segue que $k_1 a \equiv -(k_2 a) \,(mod\, p)$. Logo,

$$k_1 + k_2 \equiv 0 \,(mod\, p),$$

o que é um absurdo, pois $k_1 + k_2 < p$. Portanto, $a_1, a_2, ..., a_s, p - b_1, p - b_2, ..., p - b_r$ são dois a dois incongruentes módulo p. Dessa maneira, $a_1, a_2, ..., a_s, p - b_1, p - b_2, ..., p - b_r$ são os inteiros $1, 2, ..., \frac{p-1}{2}$ numa determinada ordem. Consequentemente,

$$a_1 \cdot a_2 \cdot ... \cdot a_s \cdot (p - b_1) \cdot (p - b_2) \cdot ... \cdot (p - b_r) = \left(\frac{p-1}{2}\right)!.$$

Mas, para cada $i = 1, 2, ..., r$ tem-se que $p - b_i \equiv -b_i \, (mod\, p)$. Imediatamente,

$$(-1)^r \prod_{i=1}^{s} a_i \prod_{i=1}^{r} b_i \equiv \left(\frac{p-1}{2}\right)! \, (mod\, p). \tag{4.2}$$

Multiplicando a congruência (4.1) por $(-1)^r$ em ambos os membros e, por transitividade com a congruência (4.2), obtemos

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

Já que p e $\left(\frac{p-1}{2}\right)!$ são relativamente primos, podemos cancelar o fator comum $\left(\frac{p-1}{2}\right)!$. Fazendo isto, temos

$$(-1)^r a^{\frac{p-1}{2}} \equiv 1 \, (mod\, p). \tag{4.3}$$

Logo, usando o Critétio de Euler e a congruência (4.3), vem que

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

e, assim,

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

Por fim, como $p > 2$ é primo, $\left(\frac{a}{p}\right)$ e $(-1)^r$ assumem valores de 1 ou -1 e, assim sendo, segue que

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

■

O seguinte teorema é uma generalização do Lema de Gauss.

Teorema 4.2. *Se p é um primo ímpar e a um inteiro também ímpar tal que $(a, p) = 1$, então*

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

em que

$$m = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{p-1}{2} \cdot \frac{a}{p}\right].$$

Demonstração: Pelo algoritmo da divisão, existem $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ inteiros tais que

$$a = p\left[\frac{a}{p}\right] + r_1,$$

$$2a = p\left[\frac{2a}{p}\right] + r_2,$$

$$\vdots$$

$$\frac{p-1}{2} \cdot a = p\left[\frac{p-1}{2} \cdot \frac{a}{p}\right] + r_{\frac{p-1}{2}}.$$

Notemos que os restos $r_1, r_2, ..., r_{\frac{p-1}{2}}$ são exatamente os inteiros a_i e b_i definidos na prova do Lema de Gauss. Somando membro a membro as $\frac{p-1}{2}$ igualdades obtidas acima, vem que

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} p\left[\frac{ka}{p}\right] + \sum_{k=1}^{\frac{p-1}{2}} r_k,$$

ou melhor,

$$a \cdot \frac{p^2-1}{8} = p \cdot m + \sum_{k=1}^{\frac{p-1}{2}} r_k, \tag{4.4}$$

uma vez que $m = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$ e $\sum_{k=1}^{\frac{p-1}{2}} k = \frac{p^2-1}{8}$. Por outro lado, sabemos, pelo Lema de Gauss, que $r_1 + r_2 + ... + r_{\frac{p-1}{2}} = a_1 + a_2 + ... + a_s + b_1 + b_2 + ... + b_r$. Assim, denotando $S_a = a_1 + a_2 + ... + a_s$ e $S_b = b_1 + b_2 + ... + b_r$ a igualdade (4.4) equivale a seguinte igualdade

$$a \cdot \frac{p^2-1}{8} = p \cdot m + S_a + S_b. \tag{4.5}$$

Também, de acordo com a prova do teorema anterior, $a_1, a_2, ..., a_s, p - b_1, p - b_2, ..., p - b_r$ são os inteiros $1, 2, ..., \frac{p-1}{2}$ em alguma ordem determinada. Logo,

$$\frac{p^2-1}{8} = \sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{s} a_k + \sum_{k=1}^{r} p - b_k = \sum_{k=1}^{s} a_k - \sum_{k=1}^{r} b_k + rp,$$

isto é,

$$\frac{p^2-1}{8} = S_a - S_b + rp. \tag{4.6}$$

Agora, subtraindo membro a membro as igualdades (4.5) e (4.6) nesta ordem, temos que

$$\frac{p^2-1}{8}(a-1) = p(m-r) + 2S_b. \tag{4.7}$$

Por hipótese, p e a são ambos ímpares, então, $p-1$ e $a-1$ são pares. Por isso, existem inteiros α e β tais que $p - 1 = 2\alpha$ e $a - 1 = 2\beta$. Consequentemente,

$$\frac{p^2-1}{8}(a-1) = \frac{(p-1)(p+1)}{8}(a-1) = \frac{2\alpha \cdot (2\alpha+2)}{8} 2\beta = \beta\alpha(\alpha+1),$$

que é sempre um número par, ou seja, $\frac{p^2-1}{8}(a-1)$ é par. À vista disso, segue de (4.7) que 2 divide $p(m-r)$. Mas, $(2, p) = 1$ e, assim, 2 divide $m - r$. Portanto, isso nos diz que r e m têm sempre a mesma paridade e, por conseguinte, pelo famoso Lema de Gauss,

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

■

A generalização do Lema de Gauss pode nos conduzir a um método para determinar quando um inteiro a ímpar é ou não um resíduo quadrático módulo a um p primo ímpar

determinado, consinderando o fato de a e p serem relativamente primos. Por exemplo, para $a = 3$ e $p = 17$ tem-se que

$$m = \left[\frac{3}{17}\right] + \left[\frac{6}{17}\right] + \left[\frac{9}{17}\right] + \left[\frac{12}{17}\right] + \left[\frac{15}{17}\right] + \left[\frac{18}{17}\right] + \left[\frac{21}{17}\right] + \left[\frac{24}{17}\right] = 3.$$

Logo, pelo Teorema 4.2,

$$\left(\frac{3}{17}\right) = (-1)^3 = -1.$$

Portanto, 3 é um resíduo não quadrático módulo 17.

4.2 Prova da Lei da Reciprocidade Quadrática

Atualmente, existem mais de 300 provas da Lei da Reciprocidade Quadrática e, em particular, Gauss apresentou 8 demonstrações distintas. Porém, nesta seção apresentaremos a prova apresentada pelo matemático alemão Ferdinand Eisentein (1823-1852) usando argumentos geométricos.

Teorema 4.3 (**Lei da Reciprocidade Quadrática**). *Se p e q são ambos primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

Demonstração: De início, consideremos o retângulo ABCD de vértice $(0,0)$, $(\frac{p}{2},0)$, $(\frac{p}{2},\frac{q}{2})$ e $(0,\frac{q}{2})$ nos pontos A, B, C e D, respectivamente. Marcamos em seu interior os pontos que pertencem ao produto cartesiano dos conjuntos $\{1,2,\ldots,\frac{p-1}{2}\}$ e $\{1,2,\ldots,\frac{q-1}{2}\}$, conforme a figura abaixo.

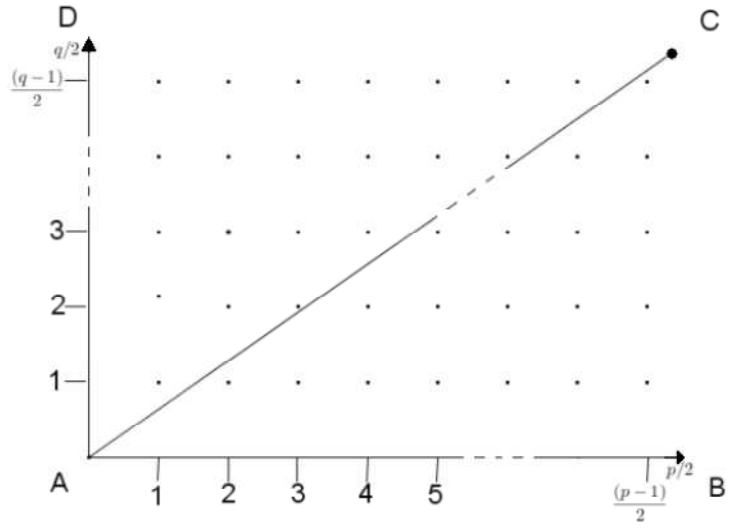

Figura 4.1: Modelo geométrico da Lei da Reciprocidade Quadrática

É claro que o número desses pontos interiores do retângulo é igual a

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right).$$

Consideremos, agora, a reta que passa pelos pontos A e C que, por sua vez, tem coeficiente angular $\frac{q}{p}$ cuja equação é dada por $y=\frac{q}{p}x$. Em seguida, como os números 1, 2,..., $\frac{p-1}{2}$ são todos relitivamente primos com p, então nenhum dos pontos interiores do retângulo de coordenadas inteiros pertence a esta reta. Desse modo, para cada $k \in \{1,2,\ldots,\frac{p-1}{2}\}$, o ponto $(k,\frac{qk}{p})$ pertence a reta $y=\frac{q}{p}x$. Por outro lado, como $\frac{qk}{p}$ não é um número inteiro, então o número de coordenadas inteiras da reta $x=k$ que estão acima do eixo-x e abaixo da reta $y=\frac{q}{p}x$ é igual a $\left[\frac{qk}{p}\right]$. Portanto, o número total m_1 de pontos de coordenadas inteiras do triângulo ABC é igual a

$$m_1=\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\cdots+\left[\frac{p-1}{2}\cdot\frac{q}{p}\right].$$

Analogamente, considerando as interseções das retas $y=k$, paralelas ao eixo-x com a reta $y=\frac{q}{p}x$, obtemos da mesma forma que o número total m_2 de coordenadas inteiras no interior do triângulo ADC é, levando em conta que os pontos em questão são da forma $(\frac{pk}{q},k)$, igual a

$$m_2=\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\cdots+\left[\frac{q-1}{2}\cdot\frac{p}{q}\right].$$

Com tudo, segue a igualdade

$$m_1+m_2=\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right).$$

No entanto, pelo Teorema 4.2, tem-se

$$\left(\frac{q}{p}\right)=(-1)^{m_1} \quad \text{e} \quad \left(\frac{p}{q}\right)=(-1)^{m_2},$$

consequentemente,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{m_1}(-1)^{m_2}=(-1)^{m_1+m_2}$$

e, portanto,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

■

O teorema acima pode ser avistado como um algoritmo para determinar se um dado inteiro é ou não um resíduo quadrático módulo um primo $p>2$ dado. Senão vejamos, por exemplo, para avaliar o Símbolo de Legendre $\left(\frac{66}{53}\right)$ notemos, primeiramente, que $66\equiv 13\,(mod\,53)$. Por isso,

$$\left(\frac{66}{53}\right)=\left(\frac{13}{53}\right).$$

Imediatamente, tem-se que

$$\left(\frac{13}{53}\right)\left(\frac{53}{13}\right)=(-1)^{(\frac{13-1}{2})(\frac{53-1}{2})}=(-1)^{6\cdot 26}=1. \tag{4.8}$$

Agora, como $53 \equiv 1\,(mod\,13)$ segue que $\left(\frac{53}{13}\right) = \left(\frac{1}{13}\right) = 1$ e, assim, da equação (4.8) obtemos $\left(\frac{13}{53}\right) = 1$. Portanto, $\left(\frac{66}{53}\right) = 1$, isto é, a congruência quadrática $x^2 \equiv 66\,(mod\,53)$ tem solução.

Uma consequência bastante interessante do Teorema 4.3 é o seguinte:

Corolário 4.1. *Se p e q são primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} +1 & se \quad p \equiv 1\,(mod\,4) \quad ou \quad q \equiv 1\,(mod\,4), \\ -1 & se \quad p \equiv q \equiv 3\,(mod\,4) \end{cases}$$

Demonstração: Se p e q são primos ímpares distintos, então pela Lei da Reciprocidade Quadrática,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

Por outro lado, se $p \equiv 1\,(mod\,4)$ ou $q \equiv 1\,(mod\,4)$, então existem inteiros k_1 e k_2 tais que

$$p = 4k_1 + 1 \quad \text{ou} \quad q = 4k_2 + 1.$$

Para $p = 4k_1 + 1$,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = (-1)^{2k_1\left(\frac{q-1}{2}\right)} = 1.$$

O mesmo vale para $q = 4k_2 + 1$. Já para $p \equiv q \equiv 3\,(mod\,4)$, existem k_1 e k_2 inteiros tais que

$$p = 4k_1 + 3 \quad \text{e} \quad p = 4k_2 + 3.$$

Daí,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = (-1)^{(2k_1+1)(2k_2+1)} = -1,$$

o que prova nossa afirmação. ■

Exemplo 4.1. *Sejam p e q primos ímpares, com $p = q + 4a$, a inteiro positivo. Mostrar que*
a) $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$
b) $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

Solução: *a*) Como $q + 4a \equiv 4a\,(mod\,q)$,

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

b) Pela Lei da Reciprocidade Quadrática,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)},$$

ou melhor,

$$\left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\left(\frac{q}{p}\right).$$

Por outro lado,

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right),$$

uma vez que $p = q + 4a$ e $p - 4a \equiv -4a\,(mod\,p)$. Logo, pelo item a) juntamente com esses dois últimos fatos, temos que

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

Desse modo,

$$\left(\frac{a}{q}\right) = (-1)^{(\frac{p-1}{2})(\frac{q+1}{2})}\left(\frac{a}{p}\right).$$

Por fim, constatemos que $p - q = 4a$ isto é, $p \equiv q\,(mod\,4)$. Assim, como p e q são primos ímpares distintos, então

$$p \equiv q \equiv 1\,(mod\,4) \;\text{ ou }\; p \equiv q \equiv 3\,(mod\,4).$$

Se $p \equiv q \equiv 1\,(mod\,4)$, então $\frac{p-1}{2}$ é par. Em seguida,

$$(-1)^{(\frac{p-1}{2})(\frac{q+1}{2})} = 1.$$

Também, verifica-se que se $p \equiv q \equiv 3\,(mod\,4)$, então $\frac{q+1}{2}$ é par e, consequentemente,

$$(-1)^{(\frac{p-1}{2})(\frac{q+1}{2})} = 1.$$

Portanto,

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

4.3 Alguns Símbolos Especiais

Na Seção 3.3 caracterizamos os primos $p > 2$ para os quais -1 e 2 são ou não resíduos quadráticos módulo p. Não muito diferente da Seção 3.3, a menos da construção, vamos caracterizar os primos $p > 2$ para os quais 3, 5, 7 e 11 são resíduos quadráticos ou não módulo p. Porém, essa tal caracterização será consequência de um resultado que chamaremos de Teorema da Caracterização que, por sua vez caracteriza, de modo geral, os primos ímpares q tal que a congruência $x^2 \equiv q\,(mod\,p)$ tem solução.

De inicio, consideremos o seguinte teorema.

Teorema 4.4. *Se p e q são primos ímpares distintos, então*

$$\overline{q} \in R_p \Leftrightarrow \overline{(-1)^{\frac{p-1}{2}}p} \in R_q.$$

Demonstração: Primeiramente, suponhamos que $\overline{q} \in R_p$. Assim, por definição $x^2 \equiv q\,(mod\,p)$ tem solução. Logo, $\left(\frac{q}{p}\right) = 1$. Por outro lado,

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} \quad \text{e} \quad \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}.$$

Desse modo, das duas igualdades acima, tem-se que

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}. \tag{4.9}$$

Agora, pela Lei da Reciprocidade Quadrática,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

e, por hipótese, deduzimos que

$$\left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}. \tag{4.10}$$

Substituindo a igualdade (4.9) em (4.10), temos

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = \left(\frac{p}{q}\right)$$

e, assim,

$$\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{p}{q}\right)^2 = 1.$$

Portanto, $\overline{(-1)^{\frac{p-1}{2}}p} \in R_q$. Reciprocamente, vamos supor que $\overline{(-1)^{\frac{p-1}{2}}p} \in R_q$, isto é,

$$\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = 1,$$

ou melhor,

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) = 1.$$

Ainda, da igualdade (4.9), concluimos que

$$(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\left(\frac{p}{q}\right) = 1.$$

Com isso, multiplicando ambos os lados dessa última igualdade por $\left(\frac{p}{q}\right)$ ocorre que

$$(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = \left(\frac{p}{q}\right).$$

Daí, pela Lei da Reciprocidade Quadrática, atingimos que $\left(\frac{q}{p}\right) = 1$. Portanto, $\overline{q} \in R_p$. ■

Uma consequêcia do Teorema acima é a caracterização dos primos ímpares $p > 3$ tal que 3 é ou não um resíduo quadrático de p.

Proposição 4.1. *Se $p > 3$ é um primo ímpar, então*

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & se \quad p \equiv \pm 1 \,(mod\, 12), \\ -1 & se \quad p \equiv \pm 5 \,(mod\, 12). \end{cases}$$

Demonstração: Pelo Teorema 4.4,

$$\overline{3} \in R_p \Leftrightarrow \overline{(-1)^{\frac{p-1}{2}} p} \in R_3.$$

Mas, $R_3 = \{\overline{1}\}$. Assim,

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} p \equiv 1 \,(mod\, 3). \tag{4.11}$$

Notemos o seguinte, se caso $\frac{p-1}{2}$ for par, então $p \equiv 1 \,(mod\, 4)$. Logo, $(-1)^{\frac{p-1}{2}} = 1$ e, assim, como $(3, 4) = 1$ segue que $p \equiv 1 \,(mod\, 12)$. Caso $\frac{p-1}{2}$ seja ímpar, então $p \equiv -1 \,(mod\, 4)$ e $(-1)^{\frac{p-1}{2}} = -1$. Desse modo, novamente pelo motivo de 3 e 4 serem primos entri si, segue que $p \equiv -1 \,(mod\, 12)$. Por isso, detemos que 3 é um resíduo quadrático módulo p para $p \equiv \pm 1 \,(mod\, 12)$. Por fim, observemos que da equivalência (4.11) obtemos

$$\left(\frac{3}{p}\right) = -1 \Leftrightarrow (-1)^{\frac{p-1}{2}} p \not\equiv 1 \,(mod\, 3).$$

Também, sob a congruência módulo 12

$$p \equiv 1, \quad p \equiv 5, \quad p \equiv 7 \equiv -5 \quad \textbf{ou} \quad p \equiv 11 \equiv -1.$$

Portanto,

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{se} \quad p \equiv \pm 1 \,(mod\, 12), \\ -1 & \text{se} \quad p \equiv \pm 5 \,(mod\, 12). \end{cases}$$

■

Estamos a um passo para enunciar e demonstrar o Teorema da Caracterização, mas antes disso consideremos o sequinte lema:

Lema 4.1. *Sejam $q > 2$ um número primo e $b \in \mathbb{Z}$ tal que $\left(\frac{b}{q}\right) = 1$ e $b \equiv 1 \,(mod\, 4)$. Então, existe um número ímpar $a \in \{1, 3, ..., q-2\}$ de modo que $b \equiv a^2 \,(mod\, 4q)$.*

Demonstração: Por hipótese, $\left(\frac{b}{q}\right) = 1$, ou seja, a congruência quadrática $x^2 \equiv b \,(mod\, q)$ tem solução, digamos a. Por isso, podemos supor que $a \in \{1, 3, ..., q-2\}$. É claro que $q - a$ também é solução de $x^2 \equiv b \,(mod\, q)$ e, ainda, $q - a \in \{1, 3, ..., q-2\}$. Por outro lado, notemos que a e $q - a$ tem paridades diferentes. Com efeito, como q é um primo ímpar, segue que existe um inteiro k_1 tal que $q = 2k_1 + 1$. Se a for par, então $a = 2k_2$, com $k_2 \in \mathbb{Z}$. Daí, $q - a = 2(k_1 - k_2) + 1$, isto é, $q - a$ é ímpar, visto que a é par. De modo análogo, se a for ímpar, então $a = 2k_2 + 1$ e, assim, $q - a = 2(k_1 - k_2)$. Logo, $q - a$ é par, pois a é ímpar. Portanto, sem perca de generalidade, podemos supor que a seja ímpar. Com isto, $a^2 \equiv 1 \,(mod\, 4)$. Agora, como $b \equiv 1 \,(mod\, 4)$ segue que $b \equiv a^2 \,(mod\, 4)$. Contudo,

$$q \mid b - a^2 \quad \textbf{e} \quad 4 \mid b - a^2.$$

Agora, como $(4, q) = 1$ concluímos que $4q \mid b - a^2$, isto é, $b \equiv a^2 \,(mod\, 4q)$. ■

Diante dos fatos obtidos, estamos em condições de enunciar e demonstrar o Teorema da Caracterização. A mesma, afirma que dados dois primo ímpares distintos p e q podemos caracterizar os primos p tal que q é um resíduo quadrático módulo p.

Teorema 4.5 (Teorema da Caracterização). *Sejam q e p números primos distintos, ambos ímpares. Então, as seguintes condições são equivalentes:*

(i) q é um resíduo quadrático módulo p;

(ii) Existe um inteiro ímpar $a \in \{1, 3, \ldots, q-2\}$ tal que $p \equiv a^2 \,(mod\, 4q)$ ou $p \equiv -a^2 \,(mod\, 4q)$.

Demonstração: Suponhamos que q é um resíduo quadrático módulo p, isto é, $\left(\frac{q}{p}\right) = 1$. Assim, pelo Teorema 4.4

$$\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = 1.$$

Agora, se $p \equiv 1 \,(mod\, 4)$, então $(-1)^{\frac{p-1}{2}}p \equiv p \equiv 1 \,(mod\, 4)$. Caso seja $p \equiv 3 \,(mod\, 4)$, então $(-1)^{\frac{p-1}{2}}p \equiv -p \equiv -3 \equiv 1 \,(mod\, 4)$. Por isso, em ambos os casos, $(-1)^{\frac{p-1}{2}}p \equiv 1 \,(mod\, 4)$. Deste modo, pelo Lema 4.1 segue que existe um inteiro ímpar $a \in \{1, 3, \ldots, q-2\}$ tal que

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

Portanto,

$$p \equiv a^2 \,(mod\, 4q) \;\text{ ou }\; p \equiv -a^2 \,(mod\, 4q),$$

visto que $(-1)^{\frac{p-1}{2}}p = p$ se $p \equiv 1 \,(mod\, 4)$ ou $(-1)^{\frac{p-1}{2}}p = -p$ se $p \equiv 3 \,(mod\, 4)$.

Reciprocamente, suponhanhos que existe um inteiro ímpar $a \in \{1, 3, \ldots, q-2\}$ tal que $p \equiv a^2$ ou $-a^2 \,(mod\, 4q)$. No ato de $p \equiv a^2 \,(mod\, 4q)$ para algum $a \in \{1, 3, \ldots, q-2\}$, então $p \equiv a^2 \,(mod\, 4)$ e como para todo inteiro ímpar tem-se que $a^2 \equiv 1 \,(mod\, 4)$ logo segue a congruência $p \equiv a^2 \equiv 1 \,(mod\, 4)$. Assim sendo, pelo Corolário 4.1 temos

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1.$$

Mas, como $\left(\frac{p}{q}\right) = 1$, segue que $\left(\frac{q}{p}\right) = 1$. Agora, no caso em que $p \equiv -a^2 \,(mod\, 4q)$, para algum $a \in \{1, 3, \ldots, q-2\}$, acarreta em $-p \equiv a^2 \,(mod\, 4)$ e, também, pelo fato de a ser ímpar $-p \equiv a^2 \equiv 1 \,(mod\, 4)$, isto é, $p \equiv 3 \,(mod\, 4)$. Daí, podemos concluir que

$$\left(\frac{-p}{q}\right) = 1 \;\text{ e }\; \left(\frac{-1}{p}\right) = -1.$$

Por outro lado, pela Lei da Reciprocidade Quadrática,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

Multiplicando a igualdade acima por $\left(\frac{-1}{q}\right)$ chegamos a seguinte igualdade

$$\left(\frac{-1}{q}\right)\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}\left(\frac{-1}{q}\right),$$

ou melhor,

$$\left(\frac{-p}{q}\right)\left(\frac{q}{p}\right) = \left[(-1)^{\frac{p-1}{2}}\right]^{\frac{q-1}{2}}\left(\frac{-1}{q}\right).$$

Mas, tendo em vista que $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$ e $\left(\frac{-p}{q}\right) = 1$ concluímos que

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}}(-1)^{\frac{q-1}{2}}.$$

Logo, $\left(\frac{q}{p}\right) = 1$. e, portanto, em ambos os casos, q é um resíduo quadrático módulo p. ■

O Teorema da Caracterização, permite caracterizar os primos $p > 2$ para qual o primo $q > 2$ seja um resíduo quadrático módulo p. Em termos lógico, apartir do Teorema anterior ganhamos um novo resultado, especificamente falando, o Teorema 4.5 é um proposição bicondicional, por isso se denominarmos o item i) de proposição a e o item ii) por b, então o Teorema da Caracterização é uma bicondicional das proposições a e b, em símbolos, $a \longleftrightarrow b$. Assim, a bicondicional $\sim a \longleftrightarrow \sim b$ é uma proposição logicamente equivaelnte a proposição $a \longleftrightarrow b$, onde o símbolo " $\sim$ " é a negação da proposição considerada. Como mostramos a validade da bicondicional $a \longleftrightarrow b$, isto é, o Teorema 4.5, então a proposição $\sim a \longleftrightarrow \sim b$ é verdadeira. Então, a proposição $\sim a \longleftrightarrow \sim b$ é exatamente o seguinte resultado:

Teorema 4.6. *Sejam q e p números primos distintos, ambos ímpares. Então, as seguintes condições são equivalentes:*

(i) q é um resíduo não quadrático módulo p;

(ii) Para todo inteiro ímpar $a \in \{1, 3, \ldots, q-2\}$ tem-se que $p \equiv a^2 \,(mod\, 4q)$ e $p \not\equiv -a^2 \,(mod\, 4q)$.

Portanto, temos em mãos as ferramentas necessárias para caracterizar os primos $p > 2$ tal que um número primo ímpar dado seja ou não um resíduo quadrático módulo p. Faremos agora as caracterizações para os primos 5, 7 e 11.

Proposição 4.2. *Se $p \neq 5$ é um primo ímpar, então*

$$\left(\frac{5}{p}\right) = \begin{cases} +1 & se \quad p \equiv 1, 9, 11 \text{ } ou \text{ } 19 \,(mod\, 20), \\ -1 & se \quad p \equiv 3, 7, 13 \text{ } ou \text{ } 17 \,(mod\, 20). \end{cases}$$

Demonstração: Pelo Teorema da Caracterização, 5 é um resíduo quadrático módulo p se, e somente se, existe $a \in \{1, 3\}$ tal que

$$p \equiv a^2 \,(mod\, 20) \quad \text{ou} \quad p \equiv -a^2 \,(mod\, 20).$$

Assim, para os possíveis valores de a temos que

$$p \equiv 1^2 \,(mod\, 20), \quad p \equiv -1^2 \,(mod\, 20), \quad p \equiv 3^2 \,(mod\, 20) \;\text{ ou }\; p \equiv -3^2 \,(mod\, 20).$$

Portanto, $\left(\frac{5}{p}\right) = 1$ se, e só se, $p \equiv 1, 9, 11$ ou $19 \,(mod\, 20)$. Por outro lado, pelo Teorema 4.6 5 é um resíduo não quadrático se, e somente se, para todo inteiro $a \in \{1, 3, 5\}$ tem-se que

$$p \not\equiv a^2 \,(mod\, 20) \;\text{ e }\; p \not\equiv -a^2 \,(mod\, 20).$$

Mas, os únicos restos possíveis para p módulo 20 para tal condição são 3, 7, 13 ou 17. Assim, $p \equiv 3, 7, 13$ ou $17 \,(mod\, 20)$ e, portanto, nossa declaração esta provada. ■

Proposição 4.3. *Se $p \neq 7$ é um primo ímpar, então*

$$\left(\frac{7}{p}\right) = \begin{cases} +1 & se \quad p \equiv 1, 3, 9, 19, 25 \;\; ou \;\; 27 \,(mod\, 28), \\ -1 & se \quad p \equiv 5, 11, 13, 15, 17 \;\; ou \;\; 23 \,(mod\, 28). \end{cases}$$

Demonstração: Pelo Teorema 4.5, 7 é um resíduo quadrático módulo p se, e só se, existe um inteiro $a \in \{1, 3, 7\}$ tal que

$$p \equiv a^2 \,(mod\, 28) \;\text{ ou }\; p \equiv -a^2 \,(mod\, 28).$$

Assim, para os prováveis valores de a vem que $p \equiv 1, 3, 9, 19, 25$ ou $27 \,(mod\, 28)$ é uma condição necessária e suficiente para $\left(\frac{7}{p}\right) = 1$. Por outro lado, pelo algoritmo da divisão os restos, possíveis, de p módulo 28 são 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25 ou 27. Agora, pelo teorema equivalente ao Teorema da Caracterização os restos viáveis para p tais que 7 seja um resíduo não quadrático de p são 5, 11, 13, 15, 17 ou 23. Logo,

$$\left(\frac{7}{p}\right) = -1 \Leftrightarrow p \equiv 5, 11, 13, 15, 17 \text{ ou } 23 \,(mod\, 28).$$

■

Por fim, vamos caracterizar os primos $p > 2$, $p \neq 11$, para que 11 seja um resíduo quadrático ou não módulo p. O Teorema da Caracterização afirma que 11 é resíduo quadrático de p se, e somente se, existe um inteiro $a \in \{1, 3, 5, 7, 9\}$ tal que

$$p \equiv a^2 \,(mod\, 44) \;\text{ ou }\; p \equiv -a^2 \,(mod\, 44).$$

Desse modo, temos a seguinte equivalência

$$\left(\frac{11}{p}\right) = 1 \Leftrightarrow p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39 \text{ ou } 43 \,(mod\, 44).$$

Agora, como p é um número primo ímpar diferente de 11, então pelo algoritmo da divisão, os restos viáveis de p módulo 44 são, exatamente, 1, 3, 5, 7, 9, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 35, 37, 39, 41 ou 43. Por isso, de acordo com o Teorema 4.6, para que 11 seja um resíduo não quadrático módulo p devemos ter que

$$p \not\equiv 1, 5, 7, 9, 19, 25, 35, 37, 39 \text{ e } 43 \,(mod\, 44).$$

Em vista disso, para a condição considerada é necessário e suficiente que

$$p \equiv 3, 13, 15, 17, 21, 23, 27, 29, 31 \text{ ou } 41 \, (mod\, 44).$$

Portanto,

$$\left(\frac{11}{p}\right) = \begin{cases} +1 & \text{se} \quad p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39 \text{ ou } 43 \, (mod\, 44), \\ -1 & \text{se} \quad p \equiv 3, 13, 15, 17, 21, 23, 27, 29, 31 \text{ ou } 41 \, (mod\, 44). \end{cases}$$

Capítulo 5

Aplicações

Neste capítulo, encerraremos a pesquisa com algumas aplicações da teoria já apresentada, bem como a infinidade de números primos de formas particulares, teste de primalidade, em especial o Teste de Pépin, que por sua vez é um teste clássicos de primalidade baseados em congruências para decidir se números de Fermat são primos ou compostos. Também, demonstraremos a irracionalidade de certos números usando a Lei da Reciprocidade Quadrática.

5.1 Infinidade de Números Primos

Euclides ($\simeq 350\ a.C.$) foi o primeiro matemático a provar que o conjunto P dos números primos é infinito, isto é,

$$P = \{2, 3, 5, 7, 11, \ldots\}.$$

Nesta seção, vamos mostrar que existem infinitos primos da forma $3k+1$, $5k-1$ e $8k-1$, com k pecorrendo os números naturais. É importante observar que nem toda forma representativa de uma sequência de números primos gera primos infinitamente. Por exemplo, para a forma do tipo $k^3 - 1$ existe apenas um número primo para tal, a saber 7. De fato, basta notar que $k^3 - 1 = (k-1)(k^2 + k + 1)$ de maneira que $k = 2$ é a única solução para $k^3 - 1$ ser primo.

De início, consideremos o resultado seguinte:

Teorema 5.1. *Existem infinitos primos da forma* $3k+1$*, com* $k \in \mathbb{N}$.

Demonstração: Suponhamos por contradição que os primos da forma $3k+1$ seja finito, digamos $p_1, p_2, \ldots, p_r$, para algum r natural. Primeiramente, averiguemos que o primo 2 não pode ser da forma $3k+1$, se fosse, existiria $\alpha \in \mathbb{N}$ tal que $2 = 3\alpha + 1$ o que implicaria que 3 divide 1, o que é um absurdo. Do mesmo modo, $3 \neq p_i$ para cara $i = 1, 2, \ldots r$, pois $3 \neq 3k+1$ para todo $k \in \mathbb{N}$. Por isso, tomemos o número

$$n = (2p_1p_2 \cdots p_i)^2 + 3.$$

Tomemos também, um divisor primo p de n. É claro que $p \neq 2$, pois n é um inteiro positivo ímpar. Ainda, na mesma linha de raciocínio, p não pode ser nenhum dos primos $3, p_1, p_2, \ldots, p_i$. De fato, se fosse $p = 3$, então 3 dividiria p_i, para algum $i = 1, 2, \ldots r$, mas isso não pode acontecer. Caso seja $p = p_i$, então $p_i \mid 3$ o que não é possível, visto que $p_i \neq 3$ para todo $i = 1, 2, \ldots r$. Logo, p é da forma $3k + 2$, isto é, em termos de congruência, $p \equiv -1\,(mod\,3)$ e, como p divide n, temos que

$$(2p_1p_2 \cdots p_i)^2 \equiv -3\,(mod\,p),$$

o que nos diz que $\left(\frac{-3}{p}\right) = 1$. No entanto,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)}\left(\frac{3}{p}\right). \tag{5.1}$$

Todavia, pela Lei da Reciprocidade Quadrática,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\left(\frac{3-1}{2}\right)\left(\frac{p-1}{2}\right)} = (-1)^{\frac{p-1}{2}}. \tag{5.2}$$

Das igualdades (5.1) e (5.2) obtemos que

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

Sendo $p \equiv -1\,(mod\,3)$ segue que

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1,$$

o que é um absurdo pois $\left(\frac{-3}{p}\right) = 1$. O absurdo provém do fato de que o conjunto dos primos da forma $3k + 1$ é finito. Portanto, existem infinitos primos da forma $3k + 1$, com $k \in \mathbb{N}$. ■

Teorema 5.2. *Existem infinitos primos da forma* $5k - 1$, *onde* $k \in \mathbb{N}$.

Demonstração: De início, suponhamos que o conjunto dos números primos da forma $5k - 1$, onde $k \in \mathbb{N}$, seja finito. Digamos, $p_1, p_2, \ldots, p_r$ para algum inteiro positivo r. Tomemos o inteiro

$$n = 5(2p_1p_2 \cdots p_i)^2 - 1$$

e, também, um fator primo p de n. Observa-se que $p \neq 5$ e n é um inteiro ímpar e, assim, $p \neq 2$. Agora, averiguemos que p não é nenhum dos primos da forma $5k - 1$. De fato, se fosse implicaria que 1 é multiplo de p, mas isso é um absurdo. Por isso, p deve ser da forma

$$5k + 1, \quad 5k + 2 \quad \text{ou} \quad 5k + 3.$$

Se $p = 5k + 3$, então $p \equiv 3\,(mod\,5)$ e, por conseguinte,

$$\left(\frac{p}{5}\right) = \left(\frac{3}{5}\right) = -1, \tag{5.3}$$

uma vez que 3 é um resíduo não quadrático módulo 5. Por outro lado, como $p \mid n$, segue que $5(2p_1p_2\cdots p_i)^2 \equiv 1\,(mod\,p)$. Daí,

$$\left(\frac{5(2p_1p_2\cdots p_i)^2}{p}\right) = \left(\frac{1}{p}\right),$$

o que implica que $\left(\frac{5}{p}\right) = 1$. Mas, pela Lei da Reciprocidade Quadrática,

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\left(\frac{5-1}{2}\right)\left(\frac{p-1}{2}\right)} = 1. \tag{5.4}$$

Como $\left(\frac{5}{p}\right) = 1$, da igualdade (5.4) conclui-se que $\left(\frac{p}{5}\right) = 1$ o que contradiz o fato da igualdade (5.3). Logo, p não é da forma $5k+3$. Caso p seja da forma $5k+2$, então $p \equiv 2\,(mod\,5)$. Contudo, 2 é um resíduo não quadrático módulo 5. Por isso,

$$\left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1, \tag{5.5}$$

o que é novamente uma contradição, pois já deduzimos que $\left(\frac{p}{5}\right) = 1$. Desse modo, p deve ser apenas da forma $5k+1$. No entanto, isso é ilógico, pois se todos os fatores primos de n for desta forma, então n também seria desta forma o que não é verdade. Portanto, existem infinitos primos da forma $5k-1$. ■

Através do resultado acima, podemos mostrar que outra classe de números primos é infinito. Vejamos, para primos da forma $5k-1$, tem-se imediatamente que k é par, pois se caso k fosse ímpar, teríamos que $5k-1$ é par. Com efeito, sendo k ímpar, existiria um inteiro positivo λ tal que $k = 2\lambda + 1$. Por esse motivo,

$$5k - 1 = 5(2\lambda + 1) - 1 = 10\lambda + 4,$$

o que já não seria mas um número primo. À vista disso, o inteiro k é par, enunciemos $k = 2\lambda$, com λ um número natural. Assim, os primos $p = 5k-1$ podem ser visto da forma $p = 10\lambda - 1$. Portanto, do Teorema 5.2 existem infinitos primos da forma $10\lambda - 1$, com $\lambda \in \mathbb{N}$. Em outras palavras, existem infinitos primos cujo últimos dígitos são 9.

Teorema 5.3. *Existem infinitos primos da forma $8k-1$, com $k \in \mathbb{N}$.*

Demonstração: Sejam $n > 1$ um número natural arbitrário e N tal que

$$N = 2(n!)^2 - 1.$$

Tomemos um divisor primo p de N. Desta maneira, $2(n!)^2 \equiv 1\,(mod\,p)$. Daí,

$$\left(\frac{2(n!)^2}{p}\right) = \left(\frac{1}{p}\right) = 1. \tag{5.6}$$

Mas, sendo o símbolo de Legendre uma função totalmente multiplicativa temos

$$\left(\frac{2(n!)^2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{(n!)^2}{p}\right) = \left(\frac{2}{p}\right). \tag{5.7}$$

Logo, segue das igualdades (5.6) e (5.7) que $\left(\frac{2}{p}\right) = 1$. Agora, pelo Teorema 3.7

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \,(mod\, 8).$$

Ou seja, é necessário e suficiente que p seja da forma $8k+1$ ou $8k-1$, com $k \in \mathbb{N}$. Por outro lado, p não pode ser da forma $8k+1$. Caso contrário, se os fatores primos de N fossem desta forma implicaria que N também seria da forma $8k+1$, mas isso é um absurdo, pois N é da forma $8k-1$. Para tal verificação, basta notar que para $n > 1$, $4 \mid (n!)^2$ e, consequentemente, $8 \mid 2(n!)^2$. Logo, existe $k \in \mathbb{Z}$ tal que $2(n!)^2 = 8k$ se, e só se, $N = 2(n!)^2 - 1 = 8k - 1$. Portanto, para cada n deve existir um divisor p de N da forma $8k-1$ e, assim, fica provado nossa afirmação. ■

5.2 Teste de Primalidade

O Símbolo de Legendre pode facilitar o processo de testar se um determinado número natural é primo ou não. É o que faremos nesta seção.

Um teste de primalidade clássico na Teoria Elementar dos Números, é o teste chamado Crivo de Eratóstenes. Dado um número natural $n > 3$ o Crivo de Eratóstenes consiste em testar a divisibilidade de n para os primos $p \leq \sqrt{n}$. Porém, o teste tem uma deficiência, está é, a medida que n cresce, $\sqrt{n}$ também cresce de modo que para um n suficientemente grande a quantidades de primos a se testar no Crivo de Eratóstenes é um número consideravelmente grande. Por exemplo, para $n = 40801$ devemos tomar os primos $p < \sqrt{40801} < 202$ para testar a primalidade de $n = 40801$. Assim, a lista deste primos são

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59,\ 61,$$

$$67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97,\ 101,\ 103,\ 107,\ 109,\ 113,\ 127,\ 131,\ 137,$$

$$139,\ 149,\ 151,\ 157,\ 163,\ 167,\ 173,\ 179,\ 181,\ 191,\ 193,\ 197,\ 199.$$

Essa lista contém 46 números primos. A Lei de Reciprocidade Quadrática nos fornece uma redução desses primos de modo a facilitar o processo de testa se n é primo ou não. Antes de mostrar a eficiência da Lei de Reciprocidade Quadrática no teste de primalidade vamos considerar o seguinte resultado:

Teorema 5.4. *Sejam $p > 2$ um número primo e $n \in \mathbb{N}$ tais que $p < n$. Então, p divide n se, e somente se, a é um resíduo quadrático módulo n implica que a é um resíduo quadráticos módulo p, com $a \in \mathbb{Z}$.*

Demonstração: Suponhamos que p divide n, assim, é claro que a congruência $x^2 \equiv a \,(mod\, n)$ implica na congruência $x^2 \equiv a \,(mod\, p)$. Reciprocamente, vamos supor que para qualquer inteiro

a resíduo quadrático módulo n implica que a é um resíduo quadrático módulo p. Por outro lado, notemos que $nk \equiv 0\,(mod\, n)$ para todo inteiro k, isto é, nk é um quadrático módulo n. Então, por hipótese, $p \mid nk$ ou nk é um resíduo quadrático módulo p para todo $k \in \mathbb{Z}$. A última condição não pode acontecer, visto que existe algum inteiro b tal que b não é um resíduo quadrático módulo p, ou seja, $\left(\frac{b}{p}\right) = -1$. Daí, teriamos $\left(\frac{n}{p}\right) = -1$. Contudo, n é genérico, podendo ele ser resíduo quadrático ou não módulo p. Desse modo, existe b tal que nb seria um quadrado módulo n mas não seria quadrático módulo p o que contraria a hipótese considerada inicialmente. Portanto, p divide n. ■

Mediante um exemplo, vamos mostrar a ultilidade da Lei da Reciprocidade Quadrática no teste de primalidade. Seja $n = 40801$. Notemos que 3 é um resíduo quadrático módulo n, pois $202^2 \equiv 3\,(mod\, 40801)$. Então, pelo teorema anterior 3 é um resíduo quadrático de p, para algum fator primo p de $n = 40801$ e, assim, pela Proposição 4.1 $p \equiv \pm 1\,(mod\, 12)$. Por isso, entre os primos $p < 202$ devemos apenas testar aqueles que satisfazem $p \equiv \pm 1\,(mod\, 12)$. Os primos menores que 202 satisfazendo esta congruência são

$$11,\quad 13,\quad 23,\quad 37,\quad 47,\quad 59,\quad 61,\quad 71,\quad 73,\quad 83,\quad 97,$$

$$107,\quad 109,\quad 131,\quad 157,\quad 167,\quad 179,\quad 181,\quad 191,\quad 193.$$

Com isto, conseguimos reduzir a lista para apenas 20 números primos ao invés de 46. Verifica-se também que 2 é um resíduo quadrático módulo 40801. Assim, para um fator primo p de 40801 deve ser da forma $8k \pm 1$, isto é, $p \equiv \pm 1\,(mod\, 8)$. Desse modo, referente a nova lista de primos $p < 202$, devemos considerar apenas os primos que p tais que $p \equiv \pm 1\,(mod\, 8)$. São eles:

$$23,\quad 47,\quad 71,\quad 73,\quad 97,\quad 167,\quad 191,\quad 193.$$

No total de 46 primos para testar a divisibilidade de 40801 reduzimos a 8 números primos. Por fim, verificando a divisibilidade de 40801 por cada um dos últimos 8 primos restante concluímos que $n = 40801$ é primo.

O Símbolo de Legendre também nos fornece métodos para testa a primalidade de números tendo formas particulares. Um exemplo disto é o famoso Teste de Pépin, um teste de primalidade para números de Fermat. O teste é nomeado para um matemático francês, Théophile Pépin (1826-1904). Pépin foi responsavél por 5 demonstrações da Lei da Reciprocidade Quadrática e no ano 1877 formulou o teste para a verificação quando um número de Fermat é primo ou composto.

Antes de apresentarmos o Teste de Pépin vamos conhecer um pouco sobre os números de Fermat. Números da forma $F_n = 2^{2^n} + 1$, com n sendo um inteiro não negativo, são chamados *números de Fermat*. Os 5 primeiros números de Fermat são

$$F_0 = 3,\quad F_1 = 5,\quad F_2 = 17,\quad F_3 = 257\ \text{ e }\ F_4 = 65537.$$

Esses 5 números são todos primos e como F_5 é um número de 10 dígitos testar sua primalidade é um trabalho díficil, ainda mais na época de Fermat. Com isso, Fermat conjecturou que todos os números de Fermat são primos. Porém, Leonhard Euler em 1732 mostrou que 641 é um fator primo de F_5, ou seja, que F_5 é composto. O próximo número de Fermat é F_6 que tem como número de dígitos igual a 20 e é um número composto, uma vez que Landry e Lasseur provaram que 274177 é um fato primo de F_6 no ano de 1880.

Os números de Fermat cresce rapidamente e sua verificação de primalidade fica cada vez mais complicada e complexa de se determinar. Até hoje os únicos primos de Fermat são F_0, F_1, F_2, F_3 e F_4 e, também, até 2010 já eram conhecidos 243 números de Fermat composto. Diante disso, segue alguns problemas em aberto relacionados com esses números:

1. Existe uma infinidade de números de Fermat primos?
2. Existe uma infinidade de números de Fermat composto?

Nesse sentido, vamos enunciar e demonstrar o teste de Pépin que pode ser usado para determinar se um número de Fermat é primo ou composto.

Teorema 5.5 (**Teste de Pépin**). *Seja $F_n = 2^{2^n}+1$, com $n \geq 2$. Então, as seguintes condições são equivalentes:*

(i) $F_n = 2^{2^n} + 1$ *é primo e* $\left(\frac{3}{F_n}\right) = -1$,

(ii) $3^{\frac{F_n-1}{2}} \equiv -1 \,(mod\, F_n)$.

Demonstração: Suponhamos que a condição (i) seja válida. Então, pelo Critério de Euler

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \equiv -1 \,(mod\, F_n).$$

Reciprocamente, vamos supor que a condição (ii) seja satisfeita. Assim,

$$3^{\frac{F_n-1}{2}} \equiv -1 \,(mod\, F_n)$$

implica que $3^{F_n-1} \equiv 1 \,(mod\, F_n)$. Pelo Teorema 1.18 segue que F_n é primo. Por fim, pelo Critério de Euler,

$$\left(\frac{3}{F_n}\right) \equiv 3^{\frac{F_n-1}{2}} \equiv -1 \,(mod\, F_n).$$

Portanto, fica provado o Teste de Pépin. ■

Apesar de que o Teste de Pépin seja um teste para decidir se um determinado número F_n de Fermat é primo ou não, o teste nunca provou que outro número de Fermat maior que F_4 é número primo. Porém, o mesmo é um resultado muito prático na exploração de determinar números de Fermat composto. Por exemplo, em 1905 Morehead e Western usando o teste de

Pépin verificaram que F7 é composto. Também, em 1909 mostraram que F8 é composto e, além disso, determinaram um fator primo para cada caso. O teste de Pépin só foi executado oito vezes e o último número de Fermat já testado pelo teste de Pépin é F_{24}, o maior já conhecido. Isso graças aos matemáticos Mayer, Papadopoulus e Crandall no ano 1999.

5.3 $\sqrt{2}$ é Irracional

Nesta seção, vamos mostrar que raiz de 2 não é um número racional usando a teoria apresentada até agora. Euclides foi o primeiro matemático a provar a irracionalidade de 2, ele usou o método *reductio ad absurdum* juntamente com aritmética. Por isso, faremos aqui, uma demonstração usando o método *reductio ad absurdum* ligadamente com alguns conceitos da Teoria dos Resíduos Quadráticos.

Teorema 5.6. $\sqrt{2}$ *é irracional.*

Demonstração: Suponhamos por absurdo que $\sqrt{2} \in \mathbb{Q}$. Assim, existem a e b inteiros tais que

$$\sqrt{2} = \frac{a}{b},$$

com $b \neq 0$. Consequetemente,

$$2b^2 = a^2.$$

Tomemos um primo p ímpar tal que $p \equiv \pm 3 \,(mod\, 8)$. Por outro lado, é notório que as congruências abaixo têm soluções:

$$x^2 \equiv a^2 \,(mod\, p) \quad \text{e} \quad x^2 \equiv b^2 \,(mod\, p).$$

Logo, pelo símbolo de Legendre, $\left(\frac{a^2}{p}\right) = 1$ e $\left(\frac{b^2}{p}\right) = 1$. Mas, como $a^2 \equiv 2b^2 \,(mod\, p)$, então

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{2b^2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{2}{p}\right),$$

o que é um absurdo, pois pelo Teorema 3.7 $\left(\frac{2}{p}\right) = -1$ para todo primo da forma $p = 8k \pm 3$, com $k \in \mathbb{Z}$. Portanto, $\sqrt{2}$ é irracional. ■

De modo análogo, podemos provar através de resíduos quadráticos a existência de outros números irracionais, senão vejamos.

Teorema 5.7. $\sqrt{3}$ *é irracional.*

Demonstração: Vamos supor que $\sqrt{3}$ é um número racional. Assim, existem inteiros a e $b \neq 0$ tais que

$$\sqrt{3} = \frac{a}{b}.$$

Elevando ambos aos lados ao quadrado da igualdade acima obtemos que

$$3b^2 = a^2.$$

Por outro lado, tomemos um número primo p ímpar tal que $p \equiv \pm 5\,(mod\,12)$. É claro que as congruências abaixo têm soluções:

$$x^2 \equiv a^2\,(mod\,p) \quad \text{e} \quad x^2 \equiv b^2\,(mod\,p).$$

Logo, pelo símbolo de Legendre, $\left(\frac{a^2}{p}\right) = \left(\frac{b^2}{p}\right) = 1$. Mas, sendo $a^2 \equiv 3b^2\,(mod\,p)$, então

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{3b^2}{p}\right) = \left(\frac{3}{p}\right),$$

o que é um contradição, uma vez que pelo Teorema 4.1 $\left(\frac{3}{p}\right) = -1$ e, por conseguinte, $\sqrt{3}$ é irracional. ■

Exemplo 5.1. *Mostre que $\sqrt[4]{3}$ é um número irracional.*

Solução: Por absurdo, suponhamos que $\sqrt[4]{3} \in \mathbb{Q}$. Assim, existem inteiros a e b, com $b \neq 0$, tais que $\sqrt[4]{3} = \frac{a}{b}$. Logo,

$$\sqrt[4]{3} = \frac{a}{b} \quad \Leftrightarrow \quad 3b^4 = a^4.$$

Verifica-se que as congruências $x^2 \equiv a^4\,(mod\,p)$ e $x^2 \equiv b^4\,(mod\,p)$ têm soluções, a saber a^2 e b^2, respectivamente, com $p > 2$ primo. Desse modo, $\left(\frac{a^4}{p}\right) = \left(\frac{b^4}{p}\right) = 1$. Por outro lado, como $3b^4 = a^4$ segue que

$$1 = \left(\frac{a^4}{p}\right) = \left(\frac{3b^4}{p}\right) = \left(\frac{3}{p}\right).$$

Portanto, tomando $p \equiv \pm 5\,(mod\,12)$ concluímos que $\sqrt[4]{3}$ é um número irracional.

Apêndice A - Classes Residuais

Neste apêndice, vamos tratar do conceito de classe residual módulo um inteiro m, que por sua vez, é de grande importancia para a Teoria dos Números. Daqui em diante, passaremos a considerar sempre que $m \geq 1$.

Definição 5.1. *Chama-se* ***classe residual (ou inteiros) módulo*** m *de um inteiro* a *o conjunto formado por todos os inteiros que são congruentes a* a *módulo* m *e denotaremos por* $\overline{a}$*. Simbolicamente,*

$$\overline{a} = \{x \in \mathbb{Z} : a \equiv x \,(mod\, m)\}.$$

Nota-se que $a \in \overline{a}$. De fato, basta notar que $a \equiv a \,(mod\, m)$. Outro fato importante sobre classes residuais segue abaixo.

Teorema 5.8. *Sejam* a *e* b *dois inteiros quaisquer. Então, as classes residuais módulo* m $\overline{a}$ *e* $\overline{b}$ *são iguais se, e somente se,* $a \equiv b \,(mod\, m)$.

Demonstração: Suponhamos que $\overline{a} = \overline{b}$. É claro que $a \in \overline{a}$ se, e só se, $a \in \overline{b}$ e, por definição, $a \equiv b \,(mod\, m)$. Reciprocamente, vamos supor que $a \equiv b \,(mod\, m)$. Por outro lado, tomemos o inteiro x tal que $x \in \overline{a}$. Assim, $a \equiv x \,(mod\, m)$ e, por hipótese, segue que $b \equiv x \,(mod\, m)$. Logo, $x \in \overline{b}$, isto é, $\overline{a} \subset \overline{b}$. Tomemos, agora, $y \in \overline{b}$, com $y \in \mathbb{Z}$. Daí, $y \equiv b \,(mod\, m)$, mas sendo $a \equiv b \,(mod\, m)$ temos que $y \equiv a \,(mod\, m)$ e, por conseguinte, $\overline{b} \subset \overline{a}$. Portanto, das duas inclusões obtida segue a igualdade, isto é, $\overline{a} = \overline{b}$. ■

O inteiro a é chamado de **representante de** $\overline{a}$ **módulo** m. Também, diz-se que a classe residual $\overline{a}$ é **determinada** ou **definida** pelo inteiro a. Por essas razões, dois inteiros a e b são representantes módulo m se, e somente se, $a \equiv b \,(mod\, m)$.

Teorema 5.9. *Sejam* $\overline{a}$ *e* $\overline{b}$ *duas classes residuais módulo* m *tais que* $\overline{a} \cap \overline{b} \neq \emptyset$*. Então,* $\overline{a} = \overline{b}$.

Demonstração: Realmente, se $\overline{a} \cap \overline{b} \neq \emptyset$, então existe um inteiro x tais que $x \in \overline{a}$ e $x \in \overline{b}$. Daí,

$$x \equiv a \,(mod\, m) \quad \text{e} \quad x \equiv b \,(mod\, m)$$

e, por transitividade, tem-se que $a \equiv b \,(mod\, m)$. Logo, pelo teorema anterior $\overline{a} = \overline{b}$. ■

Teorema 5.10. *Sejam* $\overline{a}$ *e* $\overline{b}$ *duas classes residuais módulo* m *tais que* $\overline{a} \neq \overline{b}$*. Então,* $\overline{a} \cap \overline{b} = \emptyset$.

Demonstração: Com efeito, suponhamos por absurdo que $\overline{a} \cap \overline{b} \neq \emptyset$. Logo, existe um inteiro x tais que $x \in \overline{a}$ e $x \in \overline{b}$, isto é,

$$x \equiv a\,(mod\, m) \quad \text{e} \quad x \equiv b\,(mod\, m).$$

Desse modo, $a \equiv b\,(mod\, m)$ e, consequentemente, $\overline{a} = \overline{b}$. Mas, isso é uma contradição, uma vez que, por hipótese, $\overline{a} \neq \overline{b}$. Portanto, $\overline{a} \cap \overline{b} = \emptyset$. ■

O conjunto de todas as classes residuais módulo m é denominado por $\mathbb{Z}_m$, ou seja,

$$\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\}.$$

Em particular, $\mathbb{Z}_1 = \{\overline{0}\}$, visto que $1 \mid a$ para todo inteiro a. O resultado abaixo mostra $\mathbb{Z}_m$ tem exatamente m elementos, senão vejamos o seguinte:

Teorema 5.11. *O conjunto $\mathbb{Z}_m$ possui exatamente m classes residuais módulo m distintas, a saber,*

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots \overline{m-1}\}.$$

Demonstração: Seja n um inteiro qualquer. Por definição,

$$\overline{n} = \{x \in \mathbb{Z} : n \equiv x\,(mod\, m)\}.$$

Ora, pelo algoritmo da divisão existem inteiros q e r tais que

$$n = mq + r, \quad \text{com} \quad 0 \leq r \leq m-1.$$

Desse modo, $n - r = nq$ e, pelo Teorema 5.8, segue que

$$n \equiv r\,(mod\, m) \Leftrightarrow \overline{n} = \overline{r}.$$

Logo, a classe do inteiro n é a classe de r, onde $0 \leq r \leq m-1$. Em contrapartida, suponhamos que exista $0 \leq k \leq m-1$ tais que $\overline{r} = \overline{s}$. Sem perca de generalidade, vamos supor que $r < s$. Assim,

$$\overline{r} = \overline{s} \Leftrightarrow r \equiv s\,(mod\, m) \Leftrightarrow m \mid s - r,$$

o que é um absurdo, pois $s - r < m$. Portanto, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots \overline{m-1}\}$. ■

Anexo A - Coletânea de Provas da Lei da Reciprocidade Quadrática

Segue abaixo uma lista de 314 provas da Lei da Reciprocidade Quadrática conhecida até 2015. Nesta lista, especificamos o autor, o ano e o método usado nas demonstrações. Sendo ela, feita por base na referência [1].

Tabela 5.1: Coletânea de Provas da Lei da Reciprocidade Quadrática

Posição	Autor	Ano	Método
1	Legendre	1788	Formas Quadráticas; incompleto
2	Gauss 1	1801	Indução; 8 de abril de 1796
3	Gauss 2	1801	Formas Quadráticas; 27 de junho de 1796
4	Gauss 3	1808	Lema de Gauss
5	Gauss 4	1811	Ciclotomia; maio de 1801
6	Gauss 5	1818	Lema de Gauss; agosto de 1807
7	Gauss 6	1818	Soma de Gauss; agosto de 1807
8	Cauchy	1829	Gauss 6
9	Jacobi	1830	Gauss 6
10	Dirichlet 1	1835	Gauss 4
11	Lebesgue 1	1838	$N(x_1^2 + \cdots x_q^2 \equiv 1 \, mod \, p)$
12	Lebesgue 2	1838	Lema de Gauss
13	Schönemann	1839	Equação Periódica Quadrática
14	Cauchy	1840	Gauss 4
15	Eisenstein 1	1844	Generalização da Soma de Jacobi

Posição	Autor	Ano	Método
16	Eisenstein 2	1844	Gauss 6
17	Eisenstein 3	1844	Lema de Gauss
18	Eisenstein 4	1844	Seno
19	Kummer 1	1846	Equação Periódica
20	Liouville	1847	Ciclotomia
21	Eisenstein 5	1847	Produtos Infinitos
22	Lebesgue 3	1847	Eisenstein 2
23	Lebesgue 4	1847	Liouville
24	Lebesgue 5	1847	Eisenstein 1
25	Lebesgue 6	1847	Lebesgue 1
26	Schaar 1	1847	Lema de Gauss
27	Plana	1851	Soma de Gauss
28	Schaar 2	1852	Gauss 4
29	Genocchi 1	1853	Lema de Gauss
30	Genocchi 2	1853	Liouville
31	Genocchi 3	1853	Seno de Eisenstein
32	Dirichlet 2	1854	Gauss 1
33	Genocchi 4	1854	Liouville
34	Schaar 3	1854	Gauss 4
35	Lebesgue 7	1860	Gauss 7, 8
36	Sylvester	1860	Eisenstein 3 (geometria)
37	Kummer 2	1862	Formas Quadráticas
38	Kummer 3	1862	Formas Quadráticas
39	Dedekind 1	1863	Formas Quadráticas
40	Gauss 7	1863	Períodos Quadráticos; Setembro de 1796
41	Gauss 8	1863	Períodos Quadráticos; Setembro de 1796
42	Jenkins	1867	Gauss 4
43	Mathieu	1867	Ciclotomia
44	Von Staudt	1867	Ciclotomia
45	Heime	1868	Lema de Gauss
46	Bouniakowski	1869	Lema de Gauss

Posição	Autor	Ano	Método
47	Stern	1870	Lema de Gauss
48	Zeller	1872	Lema de Gauss
49	Zolotarev	1872	Permutações
50	Kronecker 1	1876	Seno de Eisenstein
51	Schering 1	1876	Gauss 3
52	Kronecker 2	1876	Lema de Gauss
53	Mansion	1876	Zeller
54	Dedekind 2	1877	Gauss 6
55	Dedekind 3	1877	Soma Dedekind
56	Pellet 1	1878	Stickelberger-Voronoi
57	Pépin 1	1878	Ciclotomia
58	Sochocki	1878	Funções teta
59	Schering 2	1879	Lema de Gauss
60	Petersen	1879	Lema de Gauss
61	Genocchi 5	1880	Lema de Gauss
62	Kronecker 3	1880	Gauss 4
63	Kronecker 4	1880	Períodos Quadráticos
64	Voigt	1881	Lema de Gauss
65	Pellet 2	1882	Mathieu 1867
66	Busche	1883	Lema de Gauss
67	Gegenbauer 1	1884	Lema de Gauss
68	Gegenbauer 2	1884	Kronecker
69	Gegenbauer 3	1884	Schering
70	Kronecker 5	1884	Lema de Gauss
71	Bork	1885	Eisenstein geometria
72	Schering 3	1885	Lema de Gauss
73	Schering 4	1885	Lema de Gauss
74	Kronecker 6	1885	Gauss 3
75	Kronecker 7	1885	Gauss 3
76	Kronecker 8	1885	Lema de Gauss
77	Kronecker 9	1885	Lema de Gauss

Posição	Autor	Ano	Método
78	Kronecker 10	1885	Lema de Gauss
79	Bock	1886	Lema de Gauss
80	Eichenberg 1	1886	Schering 1
81	Eichenberg 2	1886	Schering 1
82	Eichenberg 3	1886	Schering 1
83	Hermes	1887	Indução
84	Lerch 1	1887	Gauss 3
85	Busche 2	1888	Lema de Gauss
86	Hacks	1889	Schering
87	Kronecker 11	1889	Lema de Gauss
88	Tafelmacher 1	1889	Stern
89	Tafelmacher 2	1889	Stern/Schering
90	Tafelmacher 3	1889	Schering
91	Busche 3	1890	Lema de Gauss
92	Franklin	1890	Lema de Gauss
93	Kronecker 12	1890	Gauss 4
94	Lucas	1890	Lema de Gauss
95	Pépin 2	1890	Gauss 2
96	Fields	1891	Lema de Gauss
97	Gegenbauer 4	1891	Lema de Gauss
98	Gegenbauer 5	1893	Lema de Gauss
99	Gegenbauer 6	1893	Zeller
100	Gegenbauer 7	1893	Petersen
101	Gegenbauer 8	1893	Lema de Gauss
102	Heinitz	1893	Lema de Gauss
103	Schmidt 1	1893	Lema de Gauss
104	Schmidt 2	1893	Lema de Gauss
105	Schmidt 3	1893	Indução
106	Gegenbauer 9	1894	Lema de Gauss
107	Hasenöhrl	1894	Lema de Gauss
108	Bang	1894	Indução

Posição	Autor	Ano	Método
109	Mertens 1	1894	Lema de Gauss
110	Mertens 2	1894	Soma de Gauss
111	Busche 4	1896	Lema de Gauss
112	Lange 1	1896	Lema de Gauss
113	De la Vallée Poussin	1896	Gauss 2
114	Lange 2	1897	Lema de Gauss
115	Lange 3	1897	Lema de Gauss
116	Hilbert	1897	Teoria da Classe
117	Hilbert	1897	Ciclotomia
118	Alexejewsky	1898	Schering
119	Pépin 3	1898	Legendre
120	Pépin 4	1898	Gauss 5
121	König	1899	Indução
122	Lerch 2	1899	Kronecker 4
123	Fischer	1900	Resultantes
124	Scheibner 1	1900	Zeller
125	Scheibner 2	1900	Kronecker
126	Scheibner 3	1900	Gauss 3
127	Scheibner 4	1900	Eisenstein geometria
128	Scheibner 5	1900	Seno de Eisenstein
129	Scheibner 6	1900	Gauss 4
130	Scheibner 7	1900	Gauss 4
131	McClintock	1902	Lema de Gauss
132	Takagi	1903	Zeller
133	Lerch 3	1903	Gauss 5
134	Mertens 3	1904	Eisenstein 4
135	Mirimanoff e Hensel	1905	Stickelberger-Voronoi
136	Cornacchia	1909	Períodos quadráticos
137	Busche 5	1909	Zeller
138	Busche 6	1909	Eisenstein
139	Busche 7	1909	Eisenstein

Posição	Autor	Ano	Método
140	Aubry	1910	Eisenstein 3
141	Aubry	1910	Voigt
142	Aubry	1910	Kronecker
143	Pépin 5	1911	Gauss 2
144	Petr	1911	Mertens 3
145	Pocklington	1911	Gauss 3
146	Dedekind 4	1912	Zelle
147	Dedekind 5	1912	Zeller
148	Dedekind 6	1912	Zeller
149	Dedekind 7	1912	Zeller
150	Heawood	1913	Eisenstein 3
151	McDonnell	1913	Ciclotômico
152	Frobenius 1	1914	Zolotarev
153	Frobenius 2	1914	Zeller
154	Frobenius 3	1914	Gauss 5
155	Frobenius 4	1914	Gauss 3
156	Frobenius 5	1914	Eisenstein 3
157	Lasker	1916	Stickelberger-Voronoi
158	Cerone	1917	Eisenstein 4
159	Bartelds e Schuh	1918	Lema de Gauss
160	Stieltjes	1918	Pontos Reticulares
161	Teege 1	1920	Legendre
162	Arwin	1924	Formas quadráticas
163	Teege 2	1925	Ciclotomia
164	Rédei 1	1925	Lema de Gauss
165	Rédei 2	1926	Lema de Gauss
166	Whitehead	1927	Teoria da Classe (Kummer)
167	Petr 2	1927	Funções teta
168	Skolem 1	1928	Teoria da Classe
169	Petr 3	1934	Kronecker
170	Van Veen	1934	Eisenstein 3

Posição	Autor	Ano	Método
171	Fueter	1935	Álgebras de Quatérnios
172	Whiteman	1935	Lema de Gauss
173	Dockeray	1938	Eisenstein 3
174	Kapferer	1939	Liouville
175	Scholz	1939	Gauss 3
176	Dörge	1942	Lema de Gauss
177	Rédei 3	1944	Gauss 5
178	Lewy	1946	Ciclotomia
179	Petr 4	1946	Ciclotomia
180	Furquim de Almeida	1948	Determinantes de Vandermonde
181	Skolem 2	1948	Gauss 2
182	Aigner	1950	Gauss 3
183	Barbilian	1950	Eisenstein 1
184	Delsarte	1950	Determinantes de Vandermonde
185	Rédei 4	1951	Gauss 3
186	Brandt 1	1951	Gauss 2
187	Brandt 2	1951	Somas de Gauss
188	Brewer	1951	Mathieu e Pellet
189	Zassenhaus	1952	Corpos Finitos
190	Riesz	1953	Permutações
191	Fröhlich	1954	Teoria das Classes dos Corpos
192	Ankeny	1955	Ciclotomia
193	D. H. Lehmer	1957	Lema de Gauss
194	C. Meyer 1	1957	Somas Dedekind
195	C. Meyer 2	1957	Zolotarev
196	Holzer	1958	Somas de Gauss
197	Rédei 5	1958	Polinômio ciclotômico
198	Reichardt	1958	Gauss 3
199	Vandiver, Weaver	1958	Zeller-Frobenius
200	Carlitz	1960	Gauss 1
201	Kubota 1	1961	Ciclotomia

Posição	Autor	Ano	Método
202	Kubota 2	1961	Somas de Gauss (Hecke)
203	Kubota 3	1961	Seno de Eisenstein
204	Skolem 3	1961	Períodos quadráticos
205	Skolem 4	1961	Ciclotomia
206	Skolem 5	1961	Corpos Finitos
207	Hausner	1961	Somas de Gauss
208	Swan 1	1962	Stickelberger-Voronoi
209	Koschmieder	1963	Eisenstein, seno
210	Gerstenhaber	1963	Eisenstein, seno
211	Rademacher 1964	1964	Análise de Fourier Finita
212	Weil	1964	Funções teta
213	Kloosterman	1965	Holzer
214	Chowla	1966	Corpos Finitos
215	Burde	1967	Lema de Gauss
216	Kaplan 1	1969	Eisenstein
217	Kaplan 1	1969	Congruências Quadráticas
218	Kubota 4	1970	Funções teta
219	Birch	1971	K-Teoria
220	Reshetukha	1971	Somas de Gauss
221	Agou	1972	Corpos Finitos
222	Brenner	1973	Zolotarev
223	Honda	1973	Somas de Gauss
224	Milnor e Husemöller	1973	Weil 1964
225	Zagier	1973	Somas de Dedekind
226	Allander	1974	Lema de Gauss
227	Berndt e Evan	1974	Lema de Gauss
228	Hirzebruch e Zagier	1974	Somas de Dedekind
229	Rogers	1974	Legendre
230	Berndt	1975	Gauss 3
231	Castaldo	1976	Lema de Gauss
232	Springer	1976	Somas de Gauss

Posição	Autor	Ano	Método
233	Burde	1977	Ciclotômico
234	Friedlander e Rosen	1977	Gauss 3
235	Frame	1978	Kronecker 3 (sinais)
236	Hurrelbrink	1978	K-Teoria
237	Auslander e Tolimieri	1979	Transformação de Fourier
238	Rosen	1979	Somas de Dedekind
239	Ryan	1979	Lema de Gauss
240	Corro	1980	Somas de Gauss
241	Brown	1981	Gauss 1
242	Cuculière	1981	Tate
243	Goldschmidt	1981	Ciclotomia
244	Kac	1981	Eisenstein, seno
245	Barcanescu	1983	Zolotarev
246	Barrucand e Laubie	1983	Stickelberger-Voronoi
247	Zantema	1983	Grupos de Brauer
248	Ely	1984	Lebesgue 1
249	Eichler	1985	Funções teta
250	Gérardin	1986	Gauss 4
251	Barrucand e Laubie	1987	Stickelberger-Voronoi
252	Peklar	1989	Lema de Gauss
253	Barnes	1990	Zolotarev
254	Swan 2	1990	Ciclotomia
255	Rousseau 1	1990	Álgebra Exterior
256	Rousseau 2	1991	Permutações
257	Keune	1991	Determinantes de Vandermonde
258	Kubota 5	1992	Geometria
259	Russinoff	1992	Lema de Gauss
260	Garrett	1992	Weil 1964
261	Motose 1	1993	Álgebras de Grupo
262	Laubenbacher, Pengelley	1994	Eisenstein geometria
263	Rousseau 3	1994	Zolotarev

Posição	Autor	Ano	Método
264	Cornaros	1995	Permutações
265	Young	1995	Soma de Gauss
266	Brylinski	1997	Ações de Grupos
267	Merindol	1997	Eisenstein, seno
268	Watanabe	1997	Zolotarev
269	Ishii	1998	Gauss 4
270	Beck	1999	Somas Dedekind
271	Motose 2	1999	Álgebras de Grupo
272	Zahidi	1999	Stickelberger-Voronoi
273	Lemmermeyer	2000	Lebesgue 1, Ely
274	Meyer	2000	Somas Dedekind
275	Tangedal	2000	Eisenstein geometria
276	Chapman	2000	Sequências Recorrentes
277	Girstmair	2001	Eichler
278	Hammick	2001	Rousseau
279	Murty	2001	Schur
280	Décaillot	2002	Lucas
281	Luo	2003	Rousseau
282	Motose 3	2003	Determinantes de Vandermonde
283	Motose 4	2003	Determinantes de Vandermonde
284	Kim	2004	Rousseau 2
285	Z.W. Sun	2004	Scholz
286	Duke e Hopkins	2005	Teoria dos Grupos
287	Murty e Pacelli	2005	Funções teta
288	Szyjewski	2005	Zolotarev
289	Arkhipova	2006	Gauss 4
290	Robbins	2006	Zolotarev
291	Kumar	2007	Rousseau
292	Kumar	2007	Keune
293	Kumar	2007	Swan
294	Castryck	2008	Lebesgue 1

Posição	Autor	Ano	Método
295	Gurevich, Hadani e Howe	2008	Schur, Weil
296	Kunisky	2008	Rousseau 2
297	Jakimczuk	2009	Lebesgue 1
298	Schechtman	2009	Gauss 4
299	Chebolu, Minac e Reis	2009	Representações
300	Kuroki e Katayama	2009	Takagi
301	Hambleton e Scharaschkin	2010	Resultantes (Swan 2)
302	Jerábek	2010	Gauss 3
303	Verdure	2010	Curvas Elípticas
304	Steiner	2010	Rousseau 2
305	Szyjewski 2	2011	Zolotarev
306	Dicker	2012	Determinantes
307	Hambleton e Scharaschkin	2012	Cônicas Pell
308	Karlsson	2012	Soma de Gauss
309	Zver	2012	Somas de Dedekind
310	Baker, Shurman	2013	Zolotarev
311	Demchenko e Gurevich	2013	Grupos Formais
312	Caldero e Germoni	2013	Lebesgue 1
313	Burda e Kadets	2013	Períodos Quadráticos
314	Brunyate e Clark	2014	Zolotarev

Referências Bibliográficas

[1] BAUMGART, O. *The Quadratic Reciprocity Law* Birkhäuser, Dordrecht Heidelberg Londres, New York, 2015.

[2] CRANDALL, R. E., MAYER, E. W. e PAPADOPOULOS J. S. *The twenty-fourth Fermat number is composite.* Math. Comp, 72, 2003, 1555-1572 (2003).

[3] DUDLEY, U. *Elementary Number Theory* (2ª edição) Dover Publications, Inc. Mineola, New York, 2008.

[4] ENDLER, O. *Teoria dos Números Algébricos* (1ª edição). IMPA, Projeto Euclides, Rio de Janeiro, 1986

[5] FILHO, E. A. *Teoria Elementar dos Números* (3ª edição). Nobel, São Paulo, 1985.

[6] HARDY, G. H and WRIGHT, E. M. *An Introduction to the Theory of Numbers* (6th ed.). Oxford University Press, London, 2008.

[7] HEFAZ, A. *Elementos de Aritmética* (2ª edição). SBM, Rio de janeiro, 2011.

[8] RIBENBOIM, P. *Números Primos: Velhos Mistérios e Novos Recordes* (1ª edição). CMU, IMPA, Rio de Janeiro, 2012.

[9] SANTOS, J. P. O. *Introdução à Teoria dos Números* (3ª edição). CMU, IMPA, Rio de Janeiro, 2009.

[10] SIDKI, S. *Introdução à Teoria dos Números* (1ª edição) IMPA, Rio de Janeiro, 1975.

[11] SIERPINSKI, W. *Elementary Theory of Number* (trans. Hulanicki). Panstwowe Wydawnictwo Naukowe, Warsaw, 1964.

[12] SINGH, S. *O Último Teorema de Fermat* (13ª edição). Editora Record Ltda, Rio de Janeiro, 2012.

[13] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura* (2ª edição). Editora da Universidade Estadual da Paraíba (coedição: Editora livraria da Física), Campina Grande/São Paulo, 2015.

[14] VIEIRA, V. L. *Um Curso Básco em Teoria dos Números* (1ª edição). Editora da Universidade Estadual da Paraíba (coedição: Editora livraria da Física), Campina Grande/São Paulo, 2015.