Daniela Mota Teixeira

Lei da Reciprocidade Quadrática e Problemas Olímpicos.

Itabaiana

2021

Daniela Mota Teixeira

Lei da Reciprocidade Quadrática e Problemas Olímpicos.

Dissertação submetida ao Corpo Docente do Programa de Mestrado Profissional em Matemática da Universidade Federal de Sergipe como requisito para a obtenção do título de Mestre em Matemática.

Universidade Federal de Sergipe

Departamento de Matemática

Programa de Pós-Graduação

Orientador: Prof. Me. Samuel Brito Silva

Itabaiana

2021

lei da reciprocidade quadrática e problemas olímpicos

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Teixeira, Daniela Mota
T266a Lei da reciprocidade quadrática e problemas olímpicos / Daniela Mota Teixeira ; orientador Samuel Brito Silva. - Itabaiana, 2021.
79 f. : il.

Dissertação (mestrado profissional em Matemática) – Universidade Federal de Sergipe, 2021.

1. Matemática. 2. Aritmética – Estudo e ensino. 3. Funções de Legendre. I. Silva, Samuel Brito orient. II. Título.

CDU 51

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA –
PROMAT/PROFMAT

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Reciprocidade Quadrática e Problemas Olímpicos

por

Daniela Mota Teixeira

Aprovada pela banca examinadora:

Samuel Brito Silva
Prof. Me. Samuel Brito Silva - UFS
Orientador

Mateus Alegri
Prof. Dr. Mateus Alegri - UFS
Primeiro Examinador

Prof. Dr. Robson da Silva - UNIFESP
Segundo Examinador

São Cristóvão, 19 de março de 2021

Cidade Upiversitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Cristóvão. Tel. (00 55 79) 3194-6887
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat.ufs@gmail.com

Por todo apoio e incentivo, dedico este trabalho a minha família.

Agradecimentos

Gratidão a Deus por me proporcionar força e proteção em todos os momentos da minha vida, principalmente na conclusão desta etapa tão especial.

Agradeço a minha família por todo amor, incentivo e reconhecimento. Em especial, a minha mãe, meu pai e a minha irmã, por acreditarem em mim e por vibrarem comigo a cada conquista.

Ao meu orientador, Professor Samuel, agradeço por todos os ensinamentos, compreensão e paciência ao longo do curso e na elaboração deste trabalho.

Obrigada a todos os professores e colegas do PROFMAT por tanto aprendizado e experiências compartilhadas.

Agradeço também aos meus amigos e todas as pessoas que torcem por mim e que sempre me incentivam a seguir em frente.

A matemática é a rainha das ciências.
(Carl Friedrich Gauss)

Resumo

Nesta dissertação vamos conhecer técnicas que nos permitirão dizer se a congruência $x^2 \equiv a \ (mod \ m)$ admite ou não solução, isto equivale a dizer se a é ou não um resíduo quadrático módulo m, onde $a, m \in \mathbb{Z}$ e $(a, m) = 1$. Veremos ferramentas importantes como o símbolo de Legendre e o Lema de Gauss. Daí, demonstraremos a Lei da Reciprocidade Quadrática, teorema que intitula este trabalho. Além disso, apresentaremos algumas aplicações deste teorema, com destaque em problemas de olimpíadas internacionais de matemática.

Palavras-chaves: Símbolo de Legendre, Lei da Reciprocidade Quadrática, Olimpíadas de Matemática.

Abstract

In this dissertation we will know techniques that will allow us to tell if the congruence $x^2 \equiv a \ (mod \ m)$ admits or not solution, this is equivalent to saying whether or not a is a quadratic residue module m, where $a, m \in \mathbb{Z}$ and $(a, m) = 1$. We will see important tools such as Legendre symbol and Lemma of Gauss. Hence, we will demonstrate the Law of Quadratic Reciprocity, the theorem that calls this work. In addition, we will present some applications of this theorem, highlighting the problems of international mathematics olympiads.

Keywords: Legendre Symbol, Law of Quadratic Reciprocity, Mathematics Olympics.

Sumário

1 RESULTADOS PRELIMINARES 10
1.1 Divisibilidade 10
1.2 Congruência 14
1.3 Congruências Lineares 16
1.4 Teoremas de Euler, Fermat e Wilson 18

2 LEI DA RECIPROCIDADE QUADRÁTICA 21
2.1 Símbolo de Legendre 28
2.1.1 Lema de Gauss 31
2.2 Lei da Reciprocidade Quadrática 36
2.2.1 Demonstração de Kim 40
2.3 Símbolo de Jacobi 46
2.4 Aplicações 49
2.4.1 Infinidade de Números Primos 49
2.4.2 $\sqrt{2}$ é irracional 51

3 PROBLEMAS OLÍMPICOS 52
3.1 Olimpíada Internacional de Matemática 52
3.1.1 IMO-1996 52
3.1.2 IMO-1998 54
3.1.3 Olimpíada de Matemática do Vietnã-2004 55
3.1.4 Olimpíada de Matemática de Taiwan-1997 56
3.2 Eötvös-Kürschák Competition 56
3.3 AwesomeMath 57
3.4 American Mathematical Monthly 60

4 APLICAÇÃO EM SALA DE AULA 62

REFERÊNCIAS BIBLIOGRÁFICAS 75

Introdução

Encontrar soluções de equações polinomiais está entre os mais antigos e estudados procedimentos matemáticos. Em particular, neste trabalho estamos interessados em estudar as equações do tipo $Ay^2 + By + C \equiv 0 \ (mod\ n)$, chamadas de *equações quadráticas modulares*, que podem facilmente serem enxergadas como uma equação do tipo $x^2 \equiv a \ (mod\ m)$.

Certamente, responder se um dado número inteiro x ao quadrado deixa um resto a na divisão por um inteiro m ($x^2 \equiv a \ (mod\ m)$ em notação de congruência) é fácil caso esse m seja pequeno. Mas com certeza a tarefa se torna mais difícil a medida que tomamos m cada vez maiores. Neste trabalho estudaremos ferramentas que nos ajudarão nesse último caso.

Esse tipo de congruência é muito importante dentro de uma área específica da Matemática: a Teoria dos Números. Esta área é uma das mais antigas e importantes da Matemática e dedica-se ao estudo dos números inteiros e suas propriedades. Inicialmente conhecida apenas por aritmética, esta área tornou-se um dos pilares da matemática. Sua grande importância lhe garante presença em diversas competições matemáticas.

As competições matemáticas existem há muito tempo, desde o século XVI. Naquela época eram feitas por meio de apostas em quantias de dinheiro e até disputas por cátedras nas universidades. As Olimpíadas de Matemática são competições realizadas através de sequências de provas cujos participantes são alunos da educação básica, e em alguns casos há a presença de alunos de cursos de nível superior. Além da Teoria dos Números, outras áreas comuns nessas competições são: Álgebra, Combinatória e Geometria.

No Brasil, entre as várias competições matemáticas conhecidas, as mais importantes são a Olimpíada Brasileira de Matemática (OBM), criada em 1979, voltada para alunos do Ensino Fundamental, Médio e Superior de todas as instituições públicas e privadas do Brasil. Também temos a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), criada em 2006, é uma competição nacional voltada para estudantes da educação básica das redes pública e privada.

Em 2018, a aprovação da Base Nacional Comum Curricular (BNCC) trouxe uma organização curricular composta por uma base nacional comum e uma parte diversificada. Além disso, tivemos a chegada do Novo Ensino Médio, o que proporcionou a criação dos itinerários formativos que podem ser definidos como um conjunto de disciplinas ou projetos que poderão ser escolhidos pelos alunos com o intuito de aprofundar seus conhecimentos numa determinada área do conhecimento.

A possibilidade de ampliação de conhecimentos numa determinada área de estudo nos permite pensar em possíveis abordagens num itinerário formativo para a área de Matemática e suas Tecnologias. Considerando as análises feitas no início do texto, a Teoria de Resíduos Quadráticos é uma opção a ser trabalhada nesse momento, uma vez que a escolha por este itinerário mostra o desejo em ampliar seus conhecimentos em matemática. Além disso, o itinerário pode ser dedicado ao treinamento de estudantes para a participação em olimpíadas de matemática.

O PROFMAT visa atender, em sua maioria, professores da educação básica das escolas públicas com o objetivo de aprimorar o seu conhecimento matemático e aplicá-lo em sala. Diante disso, o trabalho de conclusão deve abordar temas que tenham alguma aplicação em sala de aula. Portanto este trabalho tem como um dos objetivos, servir como material de apoio para os professores de matemática da educação básica na elaboração de proposta de itinerário formativo de matemática no Novo Ensino Médio.

A dissertação está organizada em quatro partes. Na primeira delas, intitulada *Resultados Preliminares*, apresentaremos conhecimentos prévios como a definição de divisibilidade, congruência e suas respectivas propriedades, além dos Teoremas de Euler, Fermat, Chinês do Resto e Wilson.

Na segunda parte temos o capítulo cujo título é *Lei da Reciprocidade Quadrática* no qual começaremos analisando equações quadráticas da forma $x^2 \equiv a \ (mod \ m)$, que nos leva a definição de resíduo quadrático, conceito primordial para o desenvolvimento deste estudo. Definiremos o símbolo de Legendre, demonstraremos suas propriedades e o Lema de Gauss. Além disso, apresentaremos duas demonstrações distintas para a Lei da Reciprocidade Quadrática, teorema que intitula este trabalho. Ao final do capítulo apresentaremos uma generalização do símbolo de Legendre: o símbolo de Jacobi e, por último, algumas aplicações da teoria.

O terceiro capítulo é dedicado ao estudo de problemas olímpicos. Neste momento abordaremos alguns problemas que podem ser solucionados através da aplicação da teoria vista na segunda parte deste trabalho. Grande parte dos problemas trabalhados foram abordados em competições matemáticas internacionais cujo público, em sua maioria, é composto por alunos do ensino médio.

O trabalho é finalizado com uma breve proposta de abordagem do estudo de Resíduos Quadráticos em sala de aula. Além disso, trazemos o Anexo A no qual apresentamos uma coletânea de provas da Lei da Reciprocidade Quadrática. A lista possui 314 demonstrações com os métodos utilizados destacados e está organizada desde a sua primeira prova, feita por Legendre no ano de 1788 até a sua prova mais recente, feita por Brunyate e Clark no ano de 2014.

1 Resultados Preliminares

Neste capítulo apresentaremos alguns conceitos e resultados importantes para o desenvolvimento do estudo principal deste trabalho. Mostraremos importantes propriedades de divisibilidade e congruência. Entre os resultados, destacamos o Teorema Chinês do Resto e os Teoremas de Euler, Fermat e Wilson.

1.1 Divisibilidade

Definição 1.1. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$, dizemos que b é divisível por a se existir um $c \in \mathbb{Z}$ tal que $b = ac$, e escrevemos $a|b$. Caso b não seja divisível por a, escrevemos $a \nmid b$.*

Teorema 1.1. *Sejam $a, b \in \mathbb{Z}$*

1. *Se $a|b$, então $a|bc$ para qualquer $c \in \mathbb{Z}$.*
2. *Se $a|b$ e $b|c$, então $a|c$.*
3. *Se $a|b$ e $a|c$, então $a|(bx + cy)$ para quaisquer $x, y \in \mathbb{Z}$.*
4. *Se $a|b$ e $b|a$, então $a = \pm b$.*
5. *Se $a|b$, $a, b > 0$, então $a \leq b$.*
6. *Se $m \neq 0$, temos que $a|b$ se, e somente se, $ma|mb$.*

Demonstração:

1. Se $a|b$, então existe $x \in \mathbb{Z}$ tal que $b = ax$. Dado $c \in \mathbb{Z}$, temos que $bc = (ax)c = a(xc)$, logo $a|bc$.
2. Supondo que $a|b$ e $b|c$, existem $x, y \in \mathbb{Z}$ tais que $b = ax$ e $c = by$, assim $c = (ax)y = a(xy)$. Logo, $a|c$.
3. Considerando que $a|b$ e $a|c$ temos que $a|bx$ e $a|cy$ para $x, y \in \mathbb{Z}$, então existem $m, n \in \mathbb{Z}$ tais que $bx = am$ e $cy = an$. Assim, $bx + cy = am + an = a(m + n)$, isto é, $a|(bx + cy)$.
4. Se $a|b$ e $b|a$, existem $x, y \in \mathbb{Z}$ tais que $b = ax$ e $a = by$, assim $a = (ax)y = a(xy)$, mas isso implica que $xy = 1$, logo $x = y = \pm 1$. Portanto, $a = \pm b$.

5. Supondo que $a|b$, existe $x \in \mathbb{Z}$ tal que $b = ax$. Por hipótese, $a, b > 0$, isso implica que $x > 0$, logo $a \leq b$.

6. Supondo que $a|b$, existe $x \in \mathbb{Z}$ tal que $b = ax$. Dado $m \neq 0$ temos que $mb = max = (ma)x$, logo $ma|mb$. Reciprocamente, suponha que $ma|mb$, então existe $y \in \mathbb{Z}$ tal que $mb = (ma)y = m(ay)$, mas isso acarreta em $b = ay$. Portanto, $a|b$.

□

Teorema 1.2. *(Algoritmo da Divisão) Dados $a, b \in \mathbb{Z}$ com $a > 0$ temos que existem únicos $q, r \in \mathbb{Z}$ tais que $b = aq + r$ com $0 \leq r < a$.*

Demonstração: Seja $a > 0$, podemos afirmar que existe q inteiro tal que $aq \leq b < a(q + 1)$. Daí,

$$aq - aq \leq b - aq < aq + a - aq \Rightarrow 0 \leq b - aq < a.$$

Diante disso, se definirmos $r = b - aq$ garantiremos a existência de q e r com $0 \leq r < a$.

Para provar a unicidade, suponha que existem $q, r, q_1, r_1 \in \mathbb{Z}$ tais que $b = aq + r$ e $b = aq_1 + r_1$ com $0 \leq r, r_1 < a$. Observe que $r = b - aq$ e $r_1 = b - aq_1$. Suponha, sem perda de generalidade, que $r > r_1$, então $0 < r - r_1 < a$. Mas, $r - r_1 = b - aq - (b - aq_1) = a(q_1 - q)$, isso implica que $a|(r - r_1)$. Diante disso, devemos ter $r - r_1 = 0$, uma vez que $r, r_1 < a$. Logo, $r = r_1$ e, consequentemente, $q = q_1$.

□

Definição 1.2. *Os inteiros $a_1, \cdots, a_n$ não nulos têm um múltiplo comum b se $a_i|b$ para $i = 1, \cdots, n$. O menor desses múltiplos positivos é chamado de menor múltiplo comum e é denotado por $[a_1, \cdots, a_n]$.*

Definição 1.3. *O número inteiro $d \geq 0$ é o maior divisor comum de a e b, o qual denotamos por $(a, b) = d$ se:*

1. *$d|a$ e $d|b$;*

2. *Se $m \in \mathbb{Z}$ tal que $m|a$ e $m|b$ temos que $m|d$.*

Definição 1.4. *Dizemos que a e b são primos entre si quando $(a, b) = 1$.*

Lema 1.1. *(Bézout) Se d é o máximo divisor comum de a e b, então existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = (a, b) = ax_0 + by_0$.*

Demonstração: Seja o conjunto $S = \{ax + by | x, y \in \mathbb{Z}\}$. Note que esse conjunto possui números positivos, negativos e nulos ($x = y = 0$). Tomemos $x_0, y_0 \in \mathbb{Z}$ de modo que $ax_0 + by_0$ seja o menor inteiro positivo do conjunto S. Denotemos $ax_0 + by_0 = c$ e suponha que $c \nmid a$, pelo Teorema 1.2, existem $q, r \in \mathbb{Z}$ tais que $a = cq + r$, com $0 < r < c$. Assim, $r = a - cq = a - (ax_0 + by_0)q = a - ax_0q - by_0q = a(1 - x_0q) + b(-y_0q)$. Logo, $r \in S$, pois $(1 - x_0q), (-y_0q) \in \mathbb{Z}$. Temos então uma contradição, uma vez que $0 < r < c$ e c é o menor inteiro positivo de S. Portanto, $c|a$ e de modo análogo, $c|b$.

Como d é um divisor comum de a e b, existem inteiros $m, n \in \mathbb{Z}$ tais que $a = dm$ e $b = dn$ e, portanto, $c = ax_0 + by_0 = (dm)x_0 + (dn)y_0 = d(mx_0 + ny_0)$, o que implica que $d|c$ e, pelo Teorema 1.1, $d \leq c$. Mas o fato de d ser o maior divisor comum de a e b nos garante que $c \leq d$, logo só nos resta que $c = d$. Consequentemente, $d = c = ax_0 + by_0$.

□

Proposição 1.1. *Sejam a e b inteiros e p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Se $p|a$ não há nada a demonstrar. Se $p \nmid a$, temos que $(a, p) = 1$, então, pelo Lema 1.1, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$ax_0 + py_0 = 1.$$

Multiplicando a igualdade por b, temos que

$$abx_0 + pby_0 = b.$$

Como $p|ab$ segue que $p|abx_0$ além disso, $p|pby_0$, então $p|(abx_0 + pby_0)$. Portanto $p|b$.

□

Lema 1.2. *(Lema de Gauss) Se $c|ab$ e $(b, c) = 1$, então $c|a$.*

Demonstração: Como $c|ab$ e $(b, c) = 1$, temos que existe $n \in \mathbb{Z}$ tal que $ab = cn$ e $bx + cy = 1$ para determinados $x, y \in \mathbb{Z}$. Multiplicando a última igualdade por a, temos que $(bx)a + (cy)a = a$, isto é, $a = (ab)x + (ac)y = (cn)x + (ac)y = c(nx + ay)$, então $c|a$.

□

Proposição 1.2. *Para todo $m \in \mathbb{Z}$ temos que $(ma, mb) = m(a, b)$.*

Demonstração: Pelo Lema 1.1, temos que (ma, mb) é o menor inteiro positivo da forma $(ma)x_0 + (mb)y_0$, assim $(ma)x_0 + (mb)y_0 = m(ax_0 + by_0)$ o que implica que $ax_0 + by_0$ é o menor inteiro positivo escrito dessa forma, ou seja, $ax_0 + by_0 = (a, b)$. Portanto, $(ma, mb) = m(a, b)$.

□

Proposição 1.3. *Se $d|a$ e $d|b$ com $d > 0$, então* $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$. *Além disso, se* $g = (a, b)$, *então* $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

Demonstração: Pela Proposição 1.2 temos que $d\left(\frac{a}{d}, \frac{b}{d}\right) = \left(d\frac{a}{d}, d\frac{b}{d}\right) = (a, b)$. Logo, $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$.

Na segunda afirmação, como $(a, b) = g$ note que $g\left(\frac{a}{g}, \frac{b}{g}\right) = \left(g\frac{a}{g}, g\frac{b}{g}\right) = (a, b) = g$. Portanto, $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

□

Proposição 1.4. *Sejam $a, b, n \in \mathbb{N}$ tais que $(a, b) = 1$ e $ab = n^2$, então a e b são quadrados perfeitos.*

Demonstração: Considerando que $ab = n^2$, suponhamos que $(a, n) = d$, então podemos escrever $a = rd$ e $n = sd$ com $r, s \in \mathbb{Z}$. Pela Proposição 1.3, $(r, s) = 1$. Assim,

$$\begin{aligned} ab &= n^2 \\ (rd)b &= (sd)^2 \\ rb &= s^2 d \end{aligned}$$

Como $(r, s) = 1$ podemos afirmar que $(r, s^2) = 1$. Portanto $s^2 \nmid r$, então $s^2|b$, consequentemente $b = s^2 l$ para algum $l \in \mathbb{N}$, daí

$$\begin{aligned} rb &= s^2 d \\ rs^2 l &= s^2 d \\ rl &= d. \end{aligned}$$

Como $d|a$, $l|b$ e $(a, b) = 1$, temos que $(d, l) = 1$. Além disso, $rl = d$ e, pelo Lema 1.2, temos que $d|r$, ou seja, $r = \alpha d$. Assim

$$\begin{aligned} (\alpha d)l &= d \\ \alpha l &= 1 \end{aligned}$$

Portanto, $\alpha = l = 1$, diante disso, $b = s^2 l = s^2$ e $a = rd = \alpha d^2 = d^2$.

□

1.2 Congruência

Definição 1.5. *Seja m um inteiro não nulo, se $m|(a-b)$ dizemos que a é congruente a b módulo m e escrevemos $a \equiv b \ (mod\ m)$. Se $m \nmid (a-b)$, dizemos que a não é congruente a b módulo m e denotamos $a \not\equiv b \ (mod\ m)$.*

Teorema 1.3. *Sejam $a, b, c, d \in \mathbb{Z}$, então:*

1. *$a \equiv b \ (mod\ m)$, $b \equiv a \ (mod\ m)$ e $a - b \equiv 0 \ (mod\ m)$ são afirmações equivalentes.*
2. *Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então $a \equiv c \ (mod\ m)$.*
3. *Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $a + c \equiv b + d \ (mod\ m)$.*
4. *Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $ac \equiv bd \ (mod\ m)$.*
5. *Se $a \equiv b \ (mod\ m)$ e $d|m$, $d > 0$, então $a \equiv b \ (mod\ d)$.*
6. *Se $a \equiv b \ (mod\ m)$, então $ac \equiv bc \ (mod\ m)$ para $c > 0$.*

Demonstração:

1. Se $a \equiv b \ (mod\ m)$, pela Definição 1.5, $m|(a-b)$ e, por sua vez, $m|(b-a)$ o que equivale dizer que $b \equiv a \ (mod\ m)$. De modo análogo, se $a - b \equiv 0 \ (mod\ m)$, temos que $m|(a-b-0)$, isto é, $m|(a-b)$, o que implica que $a \equiv b \ (mod\ m)$.
2. Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, novamente pela Definição 1.5, $m|(a-b)$ e $m|(b-c)$, assim $m|(a-c)$. Logo, $a \equiv c \ (mod\ m)$.
3. Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$ sabemos que $m|(a-b)$ e $m|(c-d)$, então $m|[a+c-(b+d)]$, equivalentemente $a + c \equiv b + d \ (mod\ m)$.
4. Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$ temos que $m|(a-b)$ e $m|(c-d)$. Note que

$$\begin{aligned}(a-b)(c-d) &= ac - ad - bc + bd \\ &= ac - ad - bc + bd - bd + bd \\ &= ac - d(a-b) - b(c-d) - bd.\end{aligned}$$

   Como $m|(a-b)(c-d)$, $m|(a-b)$ e $m|(c-d)$, isso implica que $m|(ac-bd)$. Portanto, $ac \equiv bd \ (mod\ m)$.
5. Se $d|m$ temos que existe $r \in \mathbb{Z}$ tal que $m = rd$, e como $m|(a-b)$ temos que $rd|(a-b)$, ou seja, $d|(a-b)$. Logo, $a \equiv b \ (mod\ d)$.
6. O fato de $a \equiv b \ (mod\ m)$ implica que $m|(a-b)$. Tomemos $c > 0$, consequentemente $m|(ac-bc)$, logo $ac \equiv bc \ (mod\ m)$.

□

Teorema 1.4. *Dados $a, b, m_i \in \mathbb{Z}$ para $i = 1, \cdots, r$ temos que $a \equiv b \ (mod\ m_i)$ se, e somente se, $a \equiv b \ (mod\ [m_1, \cdots, m_r])$.*

Demonstração: Suponha que $a \equiv b \ (mod\ m_i)$, isto é, $m_i|(a-b)$ para $i = 1, \cdots, r$. Isso significa que $a - b$ é múltiplo comum de $m_1, \cdots, m_r$, daí $[m_1, \cdots, m_r] \mid (a-b)$. Logo, $a \equiv b \ (mod\ [m_1, \cdots, m_r])$.

De modo análogo, se $a \equiv b \ (mod\ [m_1, \cdots, m_r])$, temos que $[m_1, \cdots, m_r] \mid (a - b)$. Como $m_i \mid [m_1, \cdots, m_r]$ segue que $m_i \mid (a - b)$, logo $a \equiv b \ (mod\ m_i)$.

□

Definição 1.6. *Se $a \equiv k \ (mod\ m)$, dizemos que k é um resíduo de a módulo m.*

Definição 1.7. *Um conjunto $\{r_1, r_2, \cdots, r_s\}$ é chamado de sistema completo de resíduos módulo m se*

- *$r_i \not\equiv r_j \ (mod\ m)$ para $i \neq j$.*
- *Para todo $h \in \mathbb{Z}$, existe r_i tal que $h \equiv r_i \ (mod\ m)$, com $i = 1, \cdots, s$.*

Observação 1.1. *Um sistema completo de resíduos módulo m é todo conjunto de números inteiros cujos restos da divisão por m são exatamente os números $0, 1, 2, \cdots, m-1$, em qualquer ordem e sem repetições.*

Exemplo 1.1. *O conjunto $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8.*

Definição 1.8. *O sistema reduzido de resíduos módulo m é um conjunto de inteiros $r_1, \cdots, r_k$ tal que*

- *$(r_i, m) = 1$, para $i = 1, \cdots, k$.*
- *$r_i \not\equiv r_j \ (mod\ m)$ se $i \neq j$.*
- *Dado $n \in \mathbb{Z}$ tal que $(n, m) = 1$ temos que existe i tal que $n \equiv r_i \ (mod\ m)$.*

Observação 1.2. *Se S é um sistema completo de resíduos módulo m, um sistema reduzido de resíduos módulo m pode ser obtido de S considerando apenas os números de S que são primos com m.*

Exemplo 1.2. *O conjunto $\bar{S} = \{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8.*

1.3 Congruências Lineares

Proposição 1.5. *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência $ax \equiv b \ (mod\ m)$ possui solução se, e somente se, $(a, m)|b$.*

Demonstração: Suponhamos que a congruência $ax \equiv b \ (mod\ m)$ tenha solução x_0, então $m|(ax_0 - b)$, logo $ax_0 - my = b$, $y \in \mathbb{Z}$. Seja $d = (a, m)$, como $d|a$ e $d|m$, pelo Teorema 1.1, $d|(ax_0 - my)$, portanto $d = (a, m)|b$.

Reciprocamente, suponha que $(a, m)|b$, daí $b = k(a, m)$, $k \in \mathbb{Z}$. Pelo Lema 1.1, $ar + ms = (a, m)$. Multplicando por k, segue que $ark + msk = (a, m)k = b$. Tomemos $x_0 = rk$, então $m|(ax_0 - b)$, portanto a congruência $ax \equiv b \ (mod\ m)$ possui solução.

□

Teorema 1.5. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $ax \equiv 1 \ (mod\ m)$ possui solução se, e somente se, $(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, temos que z é solução da congruência se, e somente se, $z \equiv x_0 \ (mod\ m)$.*

Demonstração: Dada a congruência $ax \equiv 1 \ (mod\ m)$, suponhamos que admita solução, de acordo com a Proposição 1.5, $(a, m)|1$, logo $(a, m) = 1$. De modo análogo, como $(a, m) = 1$, a congruência $ax \equiv 1 \ (mod\ m)$ admite solução.

Considerando que x_0 é solução da equação $ax \equiv 1 \ (mod\, m)$, suponha que z também é solução da congruência dada, então $az \equiv ax_0 \ (mod\ m)$, daí $m|(az - ax_0)$. Pelo fato de $(a, m) = 1$ temos que $m|(z - x_0)$, logo $z \equiv x_0 \ (mod\ m)$.

Sendo x_0 solução da congruência dada e $z \equiv x_0 \ (mod\ m)$, então $az \equiv ax_0 \equiv 1 \ (mod\ m)$. Portanto z é solução da congruência $ax \equiv 1 \ (mod\ m)$.

□

Observação 1.3. *Toda congruência $ax \equiv b \ (mod\ m)$ que possui solução é equivalente a uma congruência da forma $x \equiv c \ (mod\ m')$.*

Como a congruência $ax \equiv b \ (mod\ m)$ possui solução, então $d = (a, m)|b$. Considerando $a' = \dfrac{a}{d}$, $b' = \dfrac{b}{d}$ e $m' = \dfrac{m}{d}$, temos que a congruência acima é equivalente a $a'x \equiv b' \ (mod\ m')$, com $(a', m') = 1$. Sendo a'' o inverso multiplicativo de a' e tomando $c = a''b$ tem-se que $x \equiv c \ (mod\ m')$.

Exemplo 1.3. *A congruência $12x \equiv 36 \ (mod\ 28)$ admite solução, pois $4 = (12, 28)|36$. Além disso, $\dfrac{12}{4} = 3$, $\dfrac{36}{4} = 9$ e $\dfrac{28}{4} = 7$, com $(3, 7) = 1$. Logo, a congruência $3x \equiv 9 \ (mod$*

7) *é equivalente a congruência inicial. Note que* 5 *é o inverso multiplicativo de* 3 *módulo* 7*, então*

$$5.3x \equiv 5.9 \ (mod \ 7) \Rightarrow x \equiv 3 \ (mod \ 7).$$

Teorema 1.6. *(Teorema Chinês do Resto) Sejam* $m_1, \cdots, m_r$ *inteiros positivos que são primos entre si, dois a dois, e sejam* $c_1, \cdots, c_r$ *inteiros quaisquer. O sistema de congruências* $x \equiv c_i \ (mod \ m_i)$ *admite uma única solução módulo* $M = m_1 \cdot m_2 \cdots m_r$*. As soluções são*

$$x_0 = M_1 y_1 c_1 + \cdots + M_r y_r c_r + tM,$$

onde $t \in \mathbb{Z}$*,* $M_i = \dfrac{M}{m_i}$ *e* y_i *é solução de* $M_i y \equiv 1 \ (mod \ m_i)$*,* $i = 1, \cdots, r$*.*

Demonstração: Inicialmente mostraremos que x_0 é uma solução simultânea do sistema dado. Como $m_i | M_j$, se $i \neq j$ e $M_i y_i \equiv 1 \ (mod \ m_i)$ segue que

$$x_0 = M_1 y_1 c_1 + \cdots + M_r y_r c_r \equiv M_i c_i y_i \equiv c_i \ \ (mod \ \ m_i).$$

Por outro lado, se x' é outra solução do sistema, então $x_0 \equiv x' \ (mod \ m_i)$ para todo $i = 1, \cdots, r$. Visto que $(m_i, m_j) = 1$, para $i \neq j$, isso implica que $[m_1, \cdots, m_r] = m_1 \cdots m_r = M$ e, consequentemente, pelo Teorema 1.4, temos $x_0 \equiv x' \ (mod \ M)$.

□

Exemplo 1.4. *Aplicando o Teorema Chinês do Resto neste sistema*

$$\begin{cases} x \equiv 5 \ (mod \ 7) \\ x \equiv 7 \ (mod \ 11) \\ x \equiv 3 \ (mod \ 13) \end{cases} \tag{1.1}$$

temos que $M = 7.11.13 = 1001$*,* $M_1 = 143, M_2 = 91$ *e* $M_3 = 77$*.*

Considerando o sistema de equações

$$\begin{cases} 143x \equiv 1 \ (mod \ 7) \\ 91x \equiv 1 \ (mod \ 11) \\ 77x \equiv 1 \ (mod \ 13) \end{cases} \Rightarrow \begin{cases} 3x \equiv 1 \ (mod \ 7) \\ 3x \equiv 1 \ (mod \ 11) \\ 12x \equiv 1 \ (mod \ 13) \end{cases}$$

temos que as soluções para as respectivas equações são $y_1 = 5, y_2 = 4$ *e* $y_3 = 12$*. Portanto, a solução para o sistema 1.1 é dada por*

$$x_0 = 143.5.5 + 91.4.7 + 77.12.3 = 8895 \equiv 887 \ (mod \ 1001).$$

1.4 Teoremas de Euler, Fermat e Wilson

Definição 1.9. *A função $\phi : \mathbb{N} \to \mathbb{N}$, denominada por função de Euler, determina o número de elementos de um sistema reduzido de resíduos módulo m. De maneira simplificada, $\phi(m)$ denota a quantidade de números naturais entre 0 e $m-1$ que são primos com m. Consequentemente, $\phi(m) \leq m-1$, sendo que a igualdade acontece quando m é primo.*

Teorema 1.7. *Sejam a e m tais que $(a,m)=1$ e $r_1, r_2, \cdots, r_{\phi(m)}$ um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \cdots, ar_{\phi(m)}$ é um sistema reduzido de resíduos módulo m.*

Demonstração: Seja $r_1, \cdots, r_m$ um sistema completo de resíduos módulo m do qual foi retirado o sistema reduzido de resíduos módulo m: $r_1, r_2, \cdots, r_{\phi(m)}$. Como $(a,m) = 1$ temos que $(r_i, m) = 1$ se, e somente se, $(ar_i, m) = 1$, logo $ar_1, ar_2, \cdots, ar_{\phi(m)}$ também é um sistema reduzido de resíduos módulo m.

□

Teorema 1.8. *(Euler) Se $(a,m)=1$, então $a^{\phi(m)} \equiv 1 \ (mod\ m)$.*

Demonstração: Seja $r_1, r_2, \cdots, r_{\phi(m)}$ um sistema reduzido de resíduos módulo m, então, pelo Teorema 1.7, $ar_1, ar_2, \cdots, ar_{\phi(m)}$ é um sistema reduzido de resíduos módulo m e, portanto

$$ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \ (mod\ m).$$

Consequentemente

$$a^{\phi(m)} r_1 \cdot r_2 \cdots r_{\phi(m)} = ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \ (mod\ m).$$

Consequentemente, $m | (r_1 \cdot r_2 \cdots r_{\phi(m)})(a^{\phi(m)} - 1)$ e como $(r_1 \cdot r_2 \cdots r_{\phi(m)}, m) = 1$, pelo Lema 1.2, segue que $a^{\phi(m)} \equiv 1 \ (mod\ m)$.

□

Teorema 1.9. *(Pequeno Teorema de Fermat) Seja p um número primo, se $(a,p) = 1$, então $a^{p-1} \equiv 1 \ (mod\ p)$.*

Demonstração: Como p é primo temos que $\phi(p) = p-1$. Pelo Teorema de Euler, tem-se $a^{p-1} = a^{\phi(p)} \equiv 1 \ (mod\ p)$.

□

Corolário 1.1. *Sejam $a, p \in \mathbb{Z}$ tal que p é primo, então $a^p \equiv a \ (mod\ p)$.*

Demonstração: Temos que analisar dois casos: $p|a$ e $p \nmid a$. Se $p|a$, temos que $a \equiv 0$ $(mod\ p)$ e $a^p \equiv 0\ (mod\ p)$. Logo, $a^p \equiv a\ (mod\ p)$.

Se $p \nmid a$, pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1\ (mod\ p)$, então

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

□

Proposição 1.6. *Sejam $a, m \in \mathbb{Z}$, com $m \geq 2$, então existe $t \in \mathbb{N}$ tal que $a^t \equiv 1\ (mod\ m)$ se, e somente se, $(a, m) = 1$.*

Demonstração: Se $(a, m) = 1$, pelo Teorema de Euler, $a^{\phi(m)} \equiv 1\ (mod\ m)$. Tomemos $\phi(m) = t$, logo $a^t \equiv 1\ (mod\ m)$. Reciprocamente, suponhamos que $a^t \equiv 1\ (mod\ m)$ para algum $t \in \mathbb{N}$. Se $t = 1$, temos que $a \equiv 1\ (mod\ m)$, pela Definição 1.5, $m|(a-1)$, ou seja, $a - my = 1$, o que implica que $(a, m) = 1$. Caso $t > 1$, a congruência $ax \equiv 1$ $(mod\ m)$ tem a solução $x = a^{t-1}$, de acordo com o Teorema 1.5, podemos afirmar que $(a, m) = 1$.

□

Definição 1.10. *Considerando que $a, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$, o conjunto $A = \{h \in \mathbb{N}; a^h \equiv 1\ \ (mod\ \ m)\} \neq \varnothing$, pela Proposição 1.6. Definiremos a ordem de a com respeito a m como um número natural tal que*

$$ord_m(a) = min\{h \in \mathbb{N}; a^h \equiv 1\ \ (mod\ \ m)\}.$$

Proposição 1.7. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$. Temos que $a^t \equiv 1\ (mod\ m)$ se, e somente se, $ord_m(a)|t$.*

Demonstração: Suponha que $a^t \equiv 1\ (mod\ m)$. Queremos mostrar que $ord_m(a)|t$. Pelo algortimo da divisão, $t = ord_m(a)q + r$, onde $0 \leq r < ord_m(a)$. Temos que

$$1 \equiv a^t \equiv a^{ord_m(a)q+r} \equiv (a^{ord_m(a)})^q a^r \equiv a^r\ \ (mod\ m).$$

Portanto, $a^r \equiv 1\ (mod\ m)$. Como $ord_m(a)$ é o menor expoente que satisfaz $a^h \equiv 1$ $(mod\ m)$, temos que $r = 0$ e $ord_m(a)|t$.

Reciprocamente, suponha que $ord_m(a)|t$, então $t = ord_m(a) \cdot k$, daí

$$a^t = a^{ord_m(a)\cdot k} = (a^{ord_m(a)})^k \equiv 1^k = 1\ (mod\ m).$$

□

Corolário 1.2. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$. Temos que $ord_m(a)|\phi(m)$.*

Demonstração: Pelo Teorema de Euler, temos que $a^{\phi(m)} \equiv 1 \ (mod\ m)$. Além disso, a Proposição 1.7 nos diz que $ord_m(a)|t$, sendo t tal que $a^t \equiv 1 \ (mod\ m)$. Neste caso, seja $t = \phi(m)$, logo $ord_m(a)|\phi(m)$.

□

Teorema 1.10. *(Teorema de Wilson) Se p é um número primo, então $(p-1)! \equiv -1 \ (mod\ p)$.*

Demonstração: Se $p = 2$ ou $p = 3$, a congruência é facilmente verificada. Suponhamos que $p \geq 5$ primo. De acordo com o Teorema 1.5, a congruência $ax \equiv 1 \ (mod\ p)$ possui solução única módulo p, ou seja, dado $a \in \{1, \cdots, p-1\}$ existe um único $b \in \{1, \cdots, p-1\}$ de modo que $ab \equiv 1 \ (mod\ p)$. Por outro lado, se $a \in \{1, \cdots, p-1\}$ é tal que $a^2 \equiv 1 \ (mod\ p)$, então $p|(a^2 - 1)$, pela Proposição 1.1, $p|(a-1)$ ou $p|(a+1)$, mas isso só pode acontecer se $a = 1$ ou $a = p-1$. Então

$$\begin{aligned} 2 \cdots (p-2) &\equiv 1 \ (mod\ p) \\ 1 \cdot 2 \cdots (p-2) \cdot (p-1) &\equiv (p-1) \ (mod\ p). \end{aligned}$$

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

□

2 Lei da Reciprocidade Quadrática

Um dos objetos de estudo da Teoria dos Números são as equações polinomiais com coeficientes inteiros. Neste trabalho já vimos como determinar soluções para equações lineares modulares. Com efeito, dada a equação abaixo

$$ax \equiv b \ (mod \ m), \tag{2.1}$$

sabemos que se $(a, m)|b$ a equação admite solução. Além disso, se $(a, m) = 1$ com $m > 2$, pelo Teorema de Euler, $a^{\phi(m)-1}a = a^{\phi(m)} \equiv 1 \ (mod \ m)$, o que implica que $x \equiv a^{\phi(m)-1}b \ (mod \ m)$, portanto esta é a única solução para a equação 2.1.

Neste capítulo, veremos como analisar as soluções de equações quadráticas modulares. A priori, observe que, dada a equação da forma

$$Ay^2 + By + C \equiv 0 \ (mod\, n) \tag{2.2}$$

onde $A, B, C \in \mathbb{Z}$, $n > 1$ e $(A, n) = 1$, podemos escrevê-la de maneira equivalente como:

$$\begin{aligned} 4A^2y^2 + 4ABy + 4AC &\equiv 0 \ (mod \ 4An) && (2.3)\\ (2Ay + B)^2 &\equiv B^2 - 4AC \ (mod \ 4An). && (2.4)\\ x^2 &\equiv a \ (mod \ m). && (2.5) \end{aligned}$$

Onde $x = 2Ay + B$, $a = B^2 - 4AC$ e $m = 4An$. Para determinar a solução para a equação 2.2 é suficiente resolver o sistema

$$\begin{cases} x^2 \equiv a \ (mod \ m) \\ 2Ay + B \equiv x \ (mod \ m) \end{cases}$$

Isso nos motiva a apresentar a seguinte definição.

Definição 2.1. *Para todo a tal que $(a, m) = 1$, a é chamado de resíduo quadrático módulo m se a congruência $x^2 \equiv a \ (mod \ m)$ tiver solução. Se ela não possuir solução, dizemos que a não é um resíduo quadrático módulo m.*

Exemplo 2.1. *Os números $1, 2$ e 4 são resíduos quadráticos módulo 7, pois*

$$\begin{aligned} x &= 1 \Rightarrow x^2 \equiv 1 \ (mod \ 7)\\ x &= 2 \Rightarrow x^2 \equiv 4 \ (mod \ 7)\\ x &= 3 \Rightarrow x^2 = 9 \equiv 2 \ (mod \ 7)\\ x &= 4 \Rightarrow x^2 = 16 \equiv 2 \ (mod \ 7)\\ x &= 5 \Rightarrow x^2 = 25 \equiv 4 \ (mod \ 7)\\ x &= 6 \Rightarrow x^2 = 36 \equiv 1 \ (mod \ 7). \end{aligned}$$

Além disso, podemos dizer que as congruências $x^2 \equiv 1 \ (mod\ 7)$, $x^2 \equiv 2 \ (mod\ 7)$ *e* $x^2 \equiv 4 \ (mod\ 7)$ *possuem solução. Já as congruências* $x^2 \equiv 3 \ (mod\ 7)$, $x^2 \equiv 5 \ (mod\ 7)$ *e* $x^2 \equiv 6 \ (mod\ 7)$ *não admitem solução.*

Proposição 2.1. *Seja* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *a decomposição de* m *em fatores primos, a congruência* $x^2 \equiv a \ (mod\ m)$ *possui solução se, e somente se, cada congruência abaixo admitir solução*

$$x^2 \equiv a \ (mod\ p_i^{\alpha_i}), \ \ i = 1, \cdots, r.$$

Demonstração: Suponha que a equação $x^2 \equiv a \ (mod\ m)$ possui solução, sendo $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ temos que $m = [p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}]$, então, pelo Teorema 1.4, cada uma das congruências $x^2 \equiv a \ (mod\ p_i^{\alpha_i})$ com $i = 1, \cdots, r$ admite solução.

Reciprocamente, suponha que cada uma das congruências $x^2 \equiv a \ (mod\ p_i^{\alpha_i})$ admite solução a_i com $i = 1, \cdots, r$. Então, o Teorema Chinês do Resto nos garante que o sistema de equações simultâneas

$$x \equiv a_i \ (mod\ p_i^{\alpha_i}), \ \ i = 1, \cdots, r$$

possui uma solução x_0 tal que

$$\begin{aligned} x_0^2 \equiv {a_i}^2 &\equiv a \ (mod\ p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\ x_0^2 &\equiv a \ (mod\ m). \end{aligned}$$

Portanto, a equação $x^2 \equiv a \ (mod\ m)$ admite solução.

□

Exemplo 2.2. *A congruência* $x^2 \equiv 4 \ (mod\ 77)$ *possui 4 soluções, são elas:* $2, 9, -2$ *e* -9.

De fato, como $77 = 7.11$, de acordo com a Proposição 2.1, começaremos resolvendo as congruências $x^2 \equiv 4 \ (mod\ 7)$ e $x^2 \equiv 4 \ (mod\ 11)$.

Pelo Exemplo 2.1, as soluções para a congruência $x^2 \equiv 4 \ (mod\ 7)$ são 2 e 5. Já as soluções para a congruência $x^2 \equiv 4 \ (mod\ 11)$ são 2 e 9, uma vez que

$$\begin{aligned} x = 2 &\Rightarrow x^2 \equiv 4 \ (mod\ 11) \\ x = 9 &\Rightarrow x^2 = 9^2 = 81 \equiv 4 \ (mod\ 11). \end{aligned}$$

Temos duas soluções módulo 7 e duas soluções módulo 11, para determinarmos as soluções para a congruência módulo 77 consideraremos os seguintes sistemas.

$$\begin{cases} x \equiv 2 \ (mod\ 7) \\ x \equiv 2 \ (mod\ 11) \end{cases}$$

Pelo Teorema Chinês do Resto, temos que $M = 77$, $\mathrm{M}_1 = 11$ e $M_2 = 7$. As congruências $11y \equiv 1 \ (mod\ 7)$ e $7y \equiv 1 \ (mod\ 11)$ possuem as soluções $y_1 = 2$ e $y_2 = 8$, respectivamente. Assim, a única solução módulo 77 é

$$x = M_1 y_1 c_1 + M_2 y_2 c_2 = 11.2.2 + 7.8.2 = 156 \equiv 2 \ (mod\ 77).$$

$$\begin{cases} x \equiv 2 \ (mod\ 7) \\ x \equiv 9 \ (mod\ 11) \end{cases}$$

De modo análogo ao sistema anterior, temos que a única solução módulo 77 é

$$x = M_1 y_1 c_1 + M_2 y_2 c_2 = 11.2.2 + 7.8.9 = 548 \equiv 9 \ (mod\ 77).$$

$$\begin{cases} x \equiv 5 \ (mod\ 7) \\ x \equiv 2 \ (mod\ 11) \end{cases}$$

A solução módulo 77 para este sistema é

$$x = M_1 y_1 c_1 + M_2 y_2 c_2 = 11.2.5 + 7.8.2 = 222 \equiv -9 \ (mod\ 77).$$

$$\begin{cases} x \equiv 5 \ (mod\ 7) \\ x \equiv 9 \ (mod\ 11) \end{cases}$$

Novamente, pelo Teorema Chinês do Resto, temos que

$$x = M_1 y_1 c_1 + M_2 y_2 c_2 = 11.2.5 + 7.8.9 = 614 \equiv -2 \ (mod\ 77).$$

Proposição 2.2. *Sejam $a, p, r \in \mathbb{Z}$, onde p é um número primo ímpar e $r \geq 2$ tais que $(a, p) = 1$. A congruência $x^2 \equiv a \ (mod\ p^r)$ admite solução se, e somente se, a congruência $x^2 \equiv a \ (mod\ p)$ admite solução.*

Demonstração: Se $r \geq 2$, é claro que uma solução de $x^2 \equiv a \ (mod\ p^r)$ é solução de

$$x^2 \equiv a' \ (mod\ p^{r-1})$$

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

Para mostrar a recíproca, consideremos que $(a, p) = 1$, então $(a', p) = 1$. Sendo α' uma solução para a equação $x^2 \equiv a' \ (mod\ p^{r-1})$, mostraremos que a partir de α' podemos obter uma solução para $x^2 \equiv a \ (mod\ p^r)$.

Como α' é solução da equação $x^2 \equiv a' \ (mod\ p^{r-1})$, então existe $k \in \mathbb{Z}$ tal que $(\alpha')^2 = a' + kp^{r-1}$. Como $(a', p) = 1$ segue que $(\alpha', p) = 1$. Além disso, como $a \equiv a' \ (mod\ p^{r-1})$ temos que $a = a' + tp^{r-1}$ com $t \in \mathbb{Z}$.

Tomemos $\alpha = \alpha' + sp^{r-1}$, $s \in \mathbb{Z}$ de modo que α seja solução de $x^2 \equiv a \ (mod\ p^r)$, portanto

$$\begin{aligned} x^2 \equiv a \ (mod\ p^r) &\implies (\alpha' + sp^{r-1})^2 \equiv a \ (mod\ p^r) \\ &\implies (\alpha')^2 + 2\alpha' sp^{r-1} + (sp^{r-1})^2 \equiv a \ (mod\ p^r) \\ &\implies (\alpha')^2 + 2\alpha' sp^{r-1} + s^2 p^{2r-2} \equiv a \ (mod\ p^r) \\ &\implies (\alpha')^2 + 2\alpha' sp^{r-1} \equiv a \ (mod\ p^r). \end{aligned}$$

Uma vez que $(\alpha')^2 = a' + kp^{r-1}$ e $a = a' + tp^{r-1}$ implica que

$$\begin{aligned} a' + kp^{r-1} + 2\alpha' sp^{r-1} &\equiv a' + tp^{r-1} \ (mod\ p^r) \\ kp^{r-1} + 2\alpha' sp^{r-1} &\equiv tp^{r-1} \ (mod\ p^r) \\ 2\alpha' sp^{r-1} &\equiv tp^{r-1} - kp^{r-1} \ (mod\ p^r) \\ 2\alpha' s &\equiv t - k \ (mod\ p^r). \end{aligned}$$

Como $(2\alpha', p) = 1$, a equação acima admite única solução módulo p, a qual denotaremos por s_0. Consequentemente teremos uma única solução $\alpha = \alpha' + s_0 p^{r-1}$ para a congruência $x^2 \equiv a \ (mod\ p^r)$.

□

Exemplo 2.3. *A congruência* $x^2 \equiv 65 \ (mod\ 343)$ *possui* 53 *e* 290 *como soluções.*

De acordo com a Proposição 2.2, como $343 = 7^3$, vamos determinar as soluções da equação $x^2 \equiv 65 \ (mod\ 343)$ a partir da congruência $x^2 \equiv 65 \equiv 2 \ (mod\ 7)$, cujas soluções são 3 e 4 módulo 7.

Considerando a solução $x' = 3$, vamos construir uma solução para a congruência

$$x^2 \equiv 65 \equiv 16 \ (mod\ 7^2). \tag{2.6}$$

Temos que $3^2 = 2 + k.7$ e $16 = 2 + t.7$ com $k = 1$ e $t = 2$. Assim a congruência $2y.3 \equiv t - k = 1 \ (mod\ 7)$ possui $y' = 6$ como solução. Portanto, $x'' = 3 + y'.7 = 3 + 6.7 = 45$ é solução da equação 2.6. A partir da solução $x'' = 45$, vamos construir uma solução para a equação $x^2 \equiv 65 \ (mod\ 7^3)$. Note que $45^2 = 16 + k.7^2$ e $65 = 16 + t.7^2$, com $k = 41$ e $t = 1$, assim a congruência $2y.45 \equiv t - k = -40 \ (mod\ 7^2)$ tem como solução $y' = 5$, então $x = 45 + 5.7^2 = 290$.

Considerando a solução $x' = 4$, temos que $4^2 = 2 + k.7$ e $16 = 2 + t.7$, donde $k = 2$ e $t = 2$. A congruência $2y.4 \equiv k - t = 0 \ (mod\ 7)$ possui $y' = 0$ como solução. Portanto, $x'' = 4 + y'.7 = 4 + 0.4 = 4$ é solução da equação 2.6. Como $x'' = 4$, vamos observar que

$4^2 = 16 + k.7^2$ e $65 = 16 + t.7^2$, com $k = 0$ e $t = 1$, então a congruência $2y.4 \equiv k - t = 1$ $(mod\ 7^2)$ possui $y' = 1$ como solução. Logo, $x = 4 + 1.7^2 = 53$.

A partir de agora, para simplificar o processo, vamos restringir o nosso estudo a análise de equações quadráticas módulo p tal que p é um primo.

Proposição 2.3. *Dados a e p inteiros tais que $(a, p) = 1$ com p um primo ímpar, caso a congruência $x^2 \equiv a\ (mod\ p)$ possua solução, ela tem exatamente duas soluções incongruentes módulo p. Além do mais, se x_0 é uma solução da equação, a outra é $p - x_0$.*

Demonstração: Suponha que x_0 seja solução da equação $x^2 \equiv a\ (mod\ p)$, isto é, $x_0^2 \equiv a\ (mod\ p)$. Por outro lado,

$$x^2 \equiv a\ \ (mod\ \ p) \Rightarrow (p - x_0)^2 \equiv x_0^2 \equiv a\ \ (mod\ \ p).$$

Logo, $p - x_0$ também é solução da equação. Resta mostrar que não há mais do que duas soluções para esta congruência.

Suponha que x_1 também seja solução da equação, portanto $x_1^2 \equiv a\ (mod\ p)$. Assim, $x_0^2 \equiv x_1^2\ (mod\ p)$, o que implica que $(x_0 + x_1)(x_0 - x_1) \equiv 0\ (mod\ p)$, consequentemente $x_1 \equiv -x_0\ (mod\ p)$ ou $x_1 \equiv x_0\ (mod\ p)$. Portanto temos apenas duas soluções.

□

Exemplo 2.4. *A congruência $x^2 \equiv 9\ (mod\ 31)$ possui 3 e 28 como soluções.*

De fato, pela Proposição 2.3, temos que

$$\begin{aligned} x = 3 \ &\Rightarrow\ x^2 = 3^2 \equiv 9\ \ (mod\ \ 31) \\ x = 31 - 3 = 28 \ &\Rightarrow\ x^2 = 28^2 = 784 \equiv 9\ \ (mod\ \ 31). \end{aligned}$$

Proposição 2.4. *Se p for um primo da forma $4k+3$, então -1 não é resíduo quadrático módulo p.*

Demonstração: Suponha que existe x tal que $x^2 \equiv -1\ (mod\ p)$, então

$$\begin{aligned} x^2 \ &\equiv\ -1\ \ (mod\ \ p) \Rightarrow \\ (x^2)^{(p-1)/2} \ &\equiv\ (-1)^{(p-1)/2}\ \ (mod\ \ p). \end{aligned}$$

Uma vez que $p = 4k + 3$ é um primo ímpar, temos que $p - 1 = 4k + 2$ é um número par, logo $\dfrac{p-1}{2} = 2k + 1$ é ímpar. Portanto

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

Porém, o Teorema de Fermat nos diz que $x^{p-1} \equiv 1 \ (mod \ p)$, logo temos uma contradição.

□

Proposição 2.5. *Seja p um número primo ímpar. Os números $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ são dois a dois incongruentes e representam todos os resíduos quadráticos módulo p.*

Demonstração: Consideremos a congruência $x^2 \equiv a \ (mod \ p)$. Como

$$(p-a)^2 = p^2 - 2ap + a^2 \equiv a^2 \ (mod \ p)$$

temos que

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

para $a \in \{1, 2, \cdots, (p-1)\}$. Tomemos todos os resíduos módulo p e elevemo-nos ao quadrado.

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

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

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

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

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

Resta mostrar que esses números são dois a dois incongruentes. De fato, suponhamos que $a, b \in \left\{1, 2, \cdots, \frac{p-1}{2}\right\}$ e $a^2 \equiv b^2 \ (mod \ p)$. Assim, $p|(a^2 - b^2)$, pela Proposição 1.1, $p|(a+b)$ ou $p|(a-b)$, o que é impossível, uma vez que $a+b, a-b < p$. Portanto, todos os elementos do conjunto $\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}$ são incongruentes.

□

Observação 2.1. *A Proposição anterior nos permite afirmar que existem $\frac{p-1}{2}$ resíduos quadráticos módulo p e, de modo análogo, existem $\frac{p-1}{2}$ resíduos não quadráticos módulo p.*

Exemplo 2.5. *Se* $p = 11$ *temos que* $\dfrac{11-1}{2} = 5$*, portanto os resíduos quadráticos módulo* 11 *são* $1^2, 2^2, 3^2, 4^2, 5^2$*, ou seja,* $1, 3, 4, 5, 9$*.*

Proposição 2.6. *Sejam* $p > 2$ *um número primo e* $a \in \mathbb{Z}$ *tal que* $(a, p) = 1$*, então*

1. $a^{\frac{p-1}{2}} \equiv \pm 1 \ (mod\ p)$*.*
2. $a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ *se, e somente se, a é resíduo quadrático módulo p.*
3. $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$ *se, e somente se, a não é resíduo quadrático módulo p.*

Demonstração: Dado $\mathcal{R} = \{1, \cdots, p-1\}$ um conjunto reduzido de resíduos módulo p.

1. Pelo teorema de Fermat temos

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

Então

$$\begin{aligned} 0 &\equiv (a^{\frac{p-1}{2}})^2 - 1 \ \ (mod\ \ p) \\ 0 &\equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \ \ (mod\ \ p). \end{aligned}$$

O que equivale a $p|(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, mas como p é primo, segue que $p|(a^{\frac{p-1}{2}} - 1)$ ou $p|(a^{\frac{p-1}{2}} + 1)$. Logo, $a^{\frac{p-1}{2}} \equiv \pm 1 \ (mod\ p)$.

2. Suponhamos que a é um resíduo quadrático módulo p. Assim, existe $\alpha \in \mathbb{Z}$ tal que $\alpha^2 \equiv a \ (mod\ p)$. Pelo Teorema de Fermat temos que

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

uma vez que $p \nmid a$ e, consequentemente, $p \nmid \alpha$. Portanto, $p|(a^{\frac{p-1}{2}} - 1)$.

Reciprocamente, suponhamos que a não é um resíduo quadrático módulo p. Dado $c \in \mathcal{R}$, temos que $(c, p) = 1$, então a congruência $cx \equiv a \ (mod\ p)$ possui solução única no conjunto $\mathcal{R}$.

Considere que c' é solução da congruência $cx \equiv a \ (mod\ p)$. Além disso, $c \neq c'$, caso contrário teríamos $a \equiv cc' \equiv c^2 \ (mod\, p)$, mas isto seria uma contradição. Agrupemos os elementos de $\mathcal{R}$ de modo que $cc' \equiv a \ (mod\ p)$. Pelo teorema de Wilson, temos que

$$\begin{aligned} 1 \cdot 2 \cdots (p-1) &\equiv (c_1 c_1')(c_2 c_2') \cdots (c_{\frac{p-1}{2}} c_{\frac{p-1}{2}}') \ \ (mod\ \ p) \\ (p-1)! &\equiv a^{\frac{p-1}{2}} \ \ (mod\ \ p) \\ -1 &\equiv a^{\frac{p-1}{2}} \ \ (mod\ \ p). \end{aligned}$$

A partir disso e, pelo Item 1, podemos afirmar que $p \nmid (a^{\frac{p-1}{2}} - 1)$, isto é, $a^{\frac{p-1}{2}} \not\equiv 1$ $(mod\ p)$.

3. A demonstração deste item é equivalente a do item anterior.

□

Exemplo 2.6. *A equação* $x^2 \equiv 8\ (mod\ 13)$ *não admite solução, uma vez que* $8^{\frac{13-1}{2}} = 8^6 \equiv -1\ (mod\ 13)$*, equivalentemente, temos que* $13|(8^{\frac{13-1}{2}} + 1)$*. Portanto,* 8 *não é um resíduo quadrático módulo* 13*.*

2.1 Símbolo de Legendre

Nesta seção conheceremos uma importante ferramenta para analisar a congruência $x^2 \equiv a\ (mod\ p)$. Tal ferramenta é denominada símbolo de Legendre, em homenagem ao matemático Adrien-Marie Legendre (1752-1833). A partir disso ficará mais fácil verificar se um inteiro é ou não um resíduo quadrático módulo p.

Definição 2.2. *Se* p *é um número primo e* $a \in \mathbb{Z}$ *define-se o símbolo de Legendre como:*

1. $\left(\frac{a}{p}\right) = 0$*, se* $p|a$*.*

2. $\left(\frac{a}{p}\right) = 1$*, se* $(a,p) = 1$ *e* $x^2 \equiv a\ (mod\ p)$ *possui solução.*

3. $\left(\frac{a}{p}\right) = -1$*, se* $(a,p) = 1$ *e* $x^2 \equiv a\ (mod\ p)$ *não possui solução.*

Exemplo 2.7. *O número* 2 *é um resíduo quadrático módulo* 7*, de acordo com o Exemplo* 2.1*, então* $\left(\frac{2}{7}\right) = 1$*. Já o número* 5 *não é um resíduo quadrático módulo* 7*, portanto* $\left(\frac{5}{7}\right) = -1$*.*

Teorema 2.1. *(Critério de Euler) Seja* p *um primo ímpar tal que* $(a,p) = 1$*, então*

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

Demonstração: Considerando que $(a,p) = 1$, temos que

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

pelo Teorema de Fermat. Como $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1\ (mod\ p)$, isso implica que $a^{\frac{p-1}{2}} \equiv \pm 1\ (mod\ p)$.

Suponhamos que $\left(\frac{a}{p}\right) = 1$, então a congruência $x^2 \equiv a \ (mod\ p)$ admite solução. Consideremos $\alpha \in \mathbb{Z}$ tal que $\alpha^2 \equiv a \ (mod\ p)$. Como $(a, p) = 1$, temos que $(\alpha, p) = 1$, novamente pelo Teorema de Fermat, $\alpha^{p-1} \equiv 1 \ (mod\ p)$. Portanto

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

Consideremos agora que $\left(\frac{a}{p}\right) = -1$, note que

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

equivalentemente

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

Como p é primo, temos que $p|(a^{\frac{p-1}{2}} - 1)$ ou $p|(a^{\frac{p-1}{2}} + 1)$. Diante disso e como a não é resíduo quadrático módulo p podemos concluir que $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$, assim fica provado o Critério de Euler.

□

Exemplo 2.8. *Note que*

$$3^{\frac{7-1}{2}} = 3^3 = 27 \equiv 6 \equiv -1 \ (mod\ 7),$$

portanto $\left(\frac{3}{7}\right) = -1$. *Analogamente*

$$4^{\frac{7-1}{2}} = 4^3 = 64 \equiv 1 \ (mod\ 7),$$

o que implica que $\left(\frac{4}{7}\right) = 1$.

Teorema 2.2. *Seja p um primo ímpar, então*

1. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
2. *Se* $a \equiv b \ \ (mod\ \ p)$, *então* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. *Se* $(a, p) = 1$, *então* $\left(\frac{a^2}{p}\right) = 1$ *e* $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.
4. $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Demonstração:

1. Pela Teorema 2.1,

$$\begin{aligned}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) &\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}} \ (mod\ p)\\ &\equiv (ab)^{\frac{p-1}{2}} \ (mod\ p)\\ &\equiv \left(\frac{ab}{p}\right).\end{aligned}$$

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

2. Suponha que $a \equiv b \ (mod\ p)$, então

$$\begin{aligned}\left(\frac{a}{p}\right) &\equiv a^{\frac{p-1}{2}} \ (mod\ p)\\ &\equiv b^{\frac{p-1}{2}} \ (mod\ p)\\ &\equiv \left(\frac{b}{p}\right).\end{aligned}$$

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

3. Dado que $(a,p) = 1$ segue que $(a^2)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \ (mod\ p)$, pela Proposição 2.6, logo $\left(\frac{a^2}{p}\right) = 1$. Além disso, $\left(\frac{a^2b}{p}\right) = \left(\frac{a^2}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)$.

4. Como p é primo e $(1,p) = 1$ tem-se que $\left(\frac{1}{p}\right) = \left(\frac{1^2}{p}\right) = 1$. Além disso, note que $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \ (mod\ p)$, portanto $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

□

Proposição 2.7. *Suponha que p é um primo ímpar. Seja n o menor inteiro positivo que não é resíduo quadrático módulo p. Então $n < 1 + \sqrt{p}$.*

Demonstração: Seja m o menor inteiro positivo tal que $mn > p$, ou seja, $(m-1)n < p < mn$. Assim

$$\begin{aligned}mn - n < p < mn &\Rightarrow mn - mn - n < p - mn < mn - mn\\ &\Rightarrow -n < p - mn < 0\\ &\Rightarrow 0 < mn - p < n.\end{aligned}$$

O fato de n ser o menor número que não é resíduo quadrático módulo p implica que $mn - p$ é resíduo quadrático módulo p. Logo, a equação $x^2 \equiv (mn - p)\ (mod\ p)$ admite solução, e além disso

$$x^2 \equiv (mn - p) \equiv mn\ (mod\ p).$$

Pelo Teorema 2.2 temos que

$$\begin{aligned} 1 &= \left(\frac{mn-p}{p}\right) \\ &= \left(\frac{mn}{p}\right) \\ &= \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \\ &= -\left(\frac{m}{p}\right) \\ \Rightarrow -1 &= \left(\frac{m}{p}\right). \end{aligned}$$

Logo, m não é um resíduo quadrático módulo p. Como n é o menor não resíduo quadrático módulo p podemos afirmar que $m \geq n > 0$, e por sua vez

$$n - 1 < n$$

$$(n-1)^2 < n(n-1) \leq n(m-1) < p.$$

Portanto, $(n-1)^2 < p$ o que implica que $n < 1 + \sqrt{p}$.

□

2.1.1 Lema de Gauss

Lema 2.1. *(Lema de Gauss) Para todo p primo ímpar tal que $(a, p) = 1$ considere os inteiros $a, 2a, 3a, \cdots, \left(\frac{p-1}{2}\right)a$ e os seus resíduos módulo p. Se n denota o número de resíduos que são maiores que $\frac{p}{2}$, então $\left(\frac{a}{p}\right) = (-1)^n$.*

Demonstração: Consideremos $r_1, r_2, \cdots, r_n$ os resíduos que são maiores que $\frac{p}{2}$, e sejam $s_1, s_2, \cdots, s_k$ os resíduos menores que $\frac{p}{2}$. Assim, temos que todos esses números são distintos e não nulos.

O fato de $r_1, r_2, \cdots, r_n > \frac{p}{2}$ implica que $p - r_1, p - r_2, \cdots, p - r_n < \frac{p}{2}$ e são todos distintos entre si. Além disso, os números $p - r_i$ com $i = 1, \cdots, n$ são distintos dos números

s_j com $j = 1, \cdots, k$. Do contrário, se $p - r_i = s_j$ para algum par (i, j), então $r_i \equiv \beta a \ (mod\ p)$ e $s_j \equiv \gamma a \ (mod\ p)$ para $1 \leq \beta, \gamma \leq (p-1)/2$, daí $p - \beta a \equiv \gamma a \ (mod\ p)$. A partir disso temos que $a(\beta + \gamma) \equiv 0 \ (mod\ p)$ e como $(a, p) = 1$ isso implica que $\beta + \gamma \equiv 0 \ (mod\ p)$. Como $1 \leq \beta, \gamma \leq (p-1)/2$, note que $\beta + \gamma < p - 1$, portanto $p \nmid (\beta + \gamma)$. Logo, temos uma contradição.

Então $p - r_1, p - r_2, \cdots, p - r_n$ são todos distintos dos números $s_1, s_2, \cdots, s_k$. Além disso, todos esses números pertencem ao conjunto $\left\{1, 2, \cdots, \frac{p-1}{2}\right\}$. Como $n + k = \frac{p-1}{2}$, temos que

$$\begin{aligned}
(p - r_1) \cdot (p - r_2) \cdots (p - r_n) \cdot s_1 \cdot s_2 \cdots s_k &= 1 \cdot 2 \cdots \frac{p-1}{2} \Rightarrow \\
(-r_1) \cdot (-r_2) \cdots (-r_n) \cdot s_1 \cdot s_2 \cdots s_k &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \ (mod\ p) \Rightarrow \\
(-1)^n \cdot (r_1) \cdot (r_2) \cdots (r_n) \cdot s_1 \cdot s_2 \cdots s_k &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \ (mod\ p) \Rightarrow \\
(-1)^n \cdot a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \ (mod\ p) \Rightarrow \\
(-1)^n \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! &\equiv \left(\frac{p-1}{2}\right)! \ (mod\ p) \\
(-1)^n \cdot a^{\frac{p-1}{2}} &\equiv 1 \ (mod\ p) \\
(-1)^n \cdot (-1)^n \cdot a^{\frac{p-1}{2}} &\equiv (-1)^n \ (mod\ p) \\
(-1)^{2n} \cdot a^{\frac{p-1}{2}} &\equiv (-1)^n \ (mod\ p).
\end{aligned}$$

Assim, $a^{\frac{p-1}{2}} \equiv (-1)^n \ (mod\ p)$, pelo Teorema 2.1, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \ (mod\ p)$, o que implica que $\left(\frac{a}{p}\right) = (-1)^n$.

□

Exemplo 2.9. *Sendo* $a = 5$ *e* $p = 13$, *temos que* $\frac{p-1}{2} = 6$, *assim consideremos os seguintes múltiplos de* 5

$$1.5, 2.5, 3.5, 4.5, 5.5, 6.5.$$

Note que

$$\begin{aligned}
1.5 &\equiv 5 \ (mod\ 13) \\
2.5 &\equiv 10 \ (mod\ 13) \\
3.5 = 15 &\equiv 2 \ (mod\ 13) \\
4.5 = 20 &\equiv 7 \ (mod\ 13) \\
5.5 = 25 &\equiv 12 \ (mod\ 13) \\
6.5 = 30 &\equiv 4 \ (mod\ 13).
\end{aligned}$$

Assim os resíduos são $2, 4, 5, 7, 10, 12$. *Como apenas três deles são maiores que* $\frac{13}{2}$, *pelo Lema de Gauss, temos que* $\left(\frac{5}{13}\right) = (-1)^3 = -1$. *Logo,* 5 *não é um resíduo quadrático módulo* 13.

Definição 2.3. *Para todo* $x \in \mathbb{R}$, *o símbolo* $\lfloor x \rfloor$ *denota o maior número inteiro que é menor ou igual que* x.

Lema 2.2. *(Lema de Thue) Seja* p *um número primo e* $a \in \mathbb{Z}$ *tal que* $(a, p) = 1$. *A congruência* $ax \equiv y \ (mod\ p)$ *admite uma solução* (x_0, y_0) *tal que* $1 \leq |x_o| < \sqrt{p}$ *e* $1 \leq |y_o| < \sqrt{p}$.

Demonstração: A congruência $ax \equiv y \ (mod\ p)$ implica que $p|(ax - y)$. Seja $k = \lfloor \sqrt{p} \rfloor + 1$ e consideremos o conjunto $S = \{ax - y |\ 0 \leq x \leq k-1, 0 \leq y \leq k-1\}$. Note que temos k valores para x e k valores possíveis para y, portanto temos k^2 possíveis soluções. Como $k = \lfloor \sqrt{p} \rfloor + 1 > \sqrt{p}$ temos que $k^2 > \sqrt{p}\sqrt{p} = p$. Isso implica que o conjunto S possui números congruentes módulo p.

Tomemos $0 \leq x_1, x_2, y_1, y_2 \leq k - 1 < \sqrt{p}$ tais que

$$ax_1 - y_1 \equiv ax_2 - y_2 \ (mod\ p)$$

com $x_1 \neq x_2$ ou $y_1 \neq y_2$. Daí, $a(x_1 - x_2) \equiv y_1 - y_2 \ (mod\ p)$. Caso $x_1 = x_2$ teríamos $x_1 - x_2 = 0$, o que implicaria que $y_1 - y_2 \equiv 0 \ (mod\ p)$, portanto $y_1 = y_2$. De modo análogo, se $y_1 - y_2 = 0$ teríamos $y_1 = y_2$, então $a(x_1 - x_2) \equiv 0 \ (mod\ p)$, isto é, $p|a(x_1 - x_2)$. Por hipótese $p \nmid a$, então $p|(x_1 - x_2)$, mas $x_1 - x_2 < p$, logo $x_1 - x_2 = 0$, isto é, $x_1 = x_2$. Portanto devemos ter $x_1 \neq x_2$ e $y_1 \neq y_2$.

Denotemos $x_0 = x_1 - x_2$ e $y_0 = y_1 - y_2$, assim $ax_0 \equiv y_0 \ (mod\ p)$ para $1 \leq |x_o| < \sqrt{p}$ e $1 \leq |y_o| < \sqrt{p}$.

□

Teorema 2.3. *Se* p *é um número primo ímpar tal que* $(a, 2p) = 1$, *então* $\left(\frac{a}{p}\right) = (-1)^t$ *quando* $t = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor$.

Demonstração: Consideremos o conjunto $\left\{1a, 2a, \cdots, \left(\frac{p-1}{2}\right)a\right\}$. Fazendo a divisão de ja por p, obtemos um quociente $\left\lfloor \frac{ja}{p} \right\rfloor$. Assim

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{(p-1)/2} r_j,$$

onde r_j com $j = 1, \cdots, \dfrac{p-1}{2}$ são os restos da divisão de ja por p. Além disso,

$$\sum_{j=1}^{(p-1)/2} ja = a\left(1 + 2 + 3 + \cdots + \frac{p-1}{2}\right) = a\left(\frac{p^2-1}{8}\right).$$

Denotemos por $t = \displaystyle\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor$ e $B + C = \displaystyle\sum_{j=1}^{(p-1)/2} r_j$, sendo $B = b_1 + \cdots + b_n$ a soma dos restos da divisão de ja por p que são maiores que $\dfrac{p}{2}$ e $C = c_1 + \cdots + c_k$ a soma dos restos da divisão de ja por p que são menores que $\dfrac{p}{2}$. Logo

$$a\left(\frac{p^2-1}{8}\right) = pt + B + C. \tag{2.7}$$

Na demonstração do Lema de Gauss vimos que se $b_1, \cdots, b_n$ são os restos da divisão de ja por p que são maiores que $\dfrac{p}{2}$, então $p - b_1, \cdots, p - b_n$ são menores que $\dfrac{p}{2}$. Além disso, vimos que os resíduos $p - b_1, \cdots, p - b_n, c_1, \cdots, c_k$ são os elementos do conjunto $\{1, 2, \cdots, (p-1)/2\}$, logo

$$\begin{aligned}
\sum_{j=1}^{(p-1)/2} j &= p - b_1 + \cdots + p - b_n + c_1 \cdots + c_k \\
\sum_{j=1}^{(p-1)/2} j &= np - b_1 - \cdots - b_n + c_1 \cdots + c_k \\
\sum_{j=1}^{(p-1)/2} j &= np - B + C.
\end{aligned}$$

Consequentemente

$$\left(\frac{p^2-1}{8}\right) = np - B + C. \tag{2.8}$$

Considerando as igualdades 2.7 e 2.8 e fazendo a subtração entre elas temos que

$$(a-1)\frac{p^2-1}{8} = p(t-n) + 2B.$$

Por hipótese $(a, 2p) = 1$, o que significa que a é ímpar, assim $(a-1)$ é par. Logo, $(a-1)\dfrac{p^2-1}{8}$ é par, então $p(t-n) + 2B$ também é par. Como $2B$ é par, segue que $(t-n)$ também é par, daí podemos concluir que t e n admitem a mesma paridade. Pelo Lema de Gauss, $\left(\dfrac{a}{p}\right) = (-1)^n$, portanto $\left(\dfrac{a}{p}\right) = (-1)^t$.

□

Exemplo 2.10. *A equação $X^2 - 13Y = 5$ não possui solução.*

De fato, caso a equação tivesse solução, 5 seria resíduo quadrático módulo 13, porém isso não acontece. Note que

$$t = \left\lfloor \frac{5}{13} \right\rfloor + \left\lfloor \frac{10}{13} \right\rfloor + \left\lfloor \frac{15}{13} \right\rfloor + \left\lfloor \frac{20}{13} \right\rfloor + \left\lfloor \frac{25}{13} \right\rfloor + \left\lfloor \frac{30}{13} \right\rfloor = 5.$$

Portanto, $\left(\frac{5}{13}\right) = (-1)^t = (-1)^5 = -1$, o que implica que 5 não é um resíduo quadrático módulo 13.

Corolário 2.1. *Seja p primo, então* $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Demonstração: Seja p primo, o caso $p = 2$ implica que $\left(\frac{2}{p}\right) = 0$. Suponha que $p > 2$ e considere o conjunto $\left\{a, 2a, \cdots, \left(\frac{p-1}{2}\right)a\right\}$. Neste caso, como $a = 2$, podemos reescrever os elementos do conjunto acima como $\left\{2, 4, \cdots, \left(\frac{p-1}{2}\right)2\right\}$. Fazendo a divisão de $2j$ por p temos que $\left\lfloor \frac{2j}{p} \right\rfloor$ é o quociente dessa divisão.

Como $\left\lfloor \frac{2}{p} \right\rfloor = \left\lfloor \frac{4}{p} \right\rfloor = \cdots = \left\lfloor \frac{\left(\frac{p-1}{2}\right)2}{p} \right\rfloor = 0$. Neste caso, $t = \left\lfloor \frac{2}{p} \right\rfloor + \left\lfloor \frac{4}{p} \right\rfloor + \cdots + \left\lfloor \frac{\left(\frac{p-1}{2}\right)2}{p} \right\rfloor = 0$. Então

$$\begin{aligned} \sum_{j=1}^{(p-1)/2} 2j &= \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{2j}{p} \right\rfloor + \sum_{j=1}^{(p-1)/2} r_j \\ 2\sum_{j=1}^{(p-1)/2} j &= \sum_{j=1}^{(p-1)/2} r_j. \end{aligned}$$

Denotemos por $A + B = \sum_{j=1}^{(p-1)/2} r_j$, onde r_j com $j = 1, \cdots, \frac{p-1}{2}$ são os restos da divisão de $2j$ por p. Neste caso, A é a soma dos restos que são maiores que $\frac{p}{2}$ e B é a soma dos restos que são menores que $\frac{p}{2}$. Então

$$2\sum_{j=1}^{(p-1)/2} j = 2 \cdot \frac{p^2-1}{8}.$$

Portanto

$$2 \cdot \frac{p^2-1}{8} = A + B. \tag{2.9}$$

Sendo $A = \alpha_1 + \cdots + \alpha_n$ e $B = b_1 + \cdots + b_k$ com $\alpha_1, \cdots, \alpha_n$ os restos maiores que $\frac{p}{2}$, então $p - \alpha_1, \cdots, p - \alpha_n$ são menores que $\frac{p}{2}$. A partir disso

$$\begin{aligned} \sum_{j=1}^{(p-1)/2} j &= (p - \alpha_1) + \cdots + (p - \alpha_n) + b_1 + \cdots + b_k \\ \sum_{j=1}^{(p-1)/2} j &= np - A + B. \end{aligned}$$

Consequentemente

$$\frac{p^2 - 1}{8} = pn - A + B. \tag{2.10}$$

Considerando as igualdades 2.9 e 2.10 e fazendo a subtração entre elas, temos que

$$\frac{p^2 - 1}{8} = -pn + 2A$$

$$\frac{p^2 - 1}{8} + pn = 2A.$$

Observe que os números $\frac{p^2 - 1}{8}$ e n têm a mesma paridade, então pelo Lema de Gauss, $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{(p^2-1)/8}$.

□

2.2 Lei da Reciprocidade Quadrática

O próximo teorema é um dos mais importantes dentro da Teoria dos Números. A Lei da Reciprocidade Quadrática foi conjecturada por Leonard Euler (1707-1783) e Adrien-Marie Legendre (1752-1833) no século XVIII.

A primeira demonstração da Lei da Reciprocidade Quadrática foi feita por Johann Carl Friedrich Gauss (1777-1855), em 1796. Ele demonstrou o teorema de oito maneiras diferentes ao longo da sua vida. Por considerá-lo tão importante, Gauss o chamou de Teorema Áureo em seu livro *Disquisitones Arithmeticae*.

Até o ano de 2014, o teorema possuia 314 demonstrações desde a sua conjectura. Neste trabalho apresentaremos duas destas demonstrações. A prova a seguir foi feita pelo matemático Ferdinand Gotthold Max Eisenstein (1823-1852), na primeira metade do século XIX.

Teorema 2.4. *(Lei da Reciprocidade Quadrática) Se p e q são primos ímpares distintos, então*

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

Demonstração: Consideremos um retângulo ABCD cujos vértices são $A = (0,0)$, $B = \left(\frac{p}{2}, 0\right)$, $C = \left(\frac{p}{2}, \frac{q}{2}\right)$ e $D = \left(0, \frac{q}{2}\right)$.

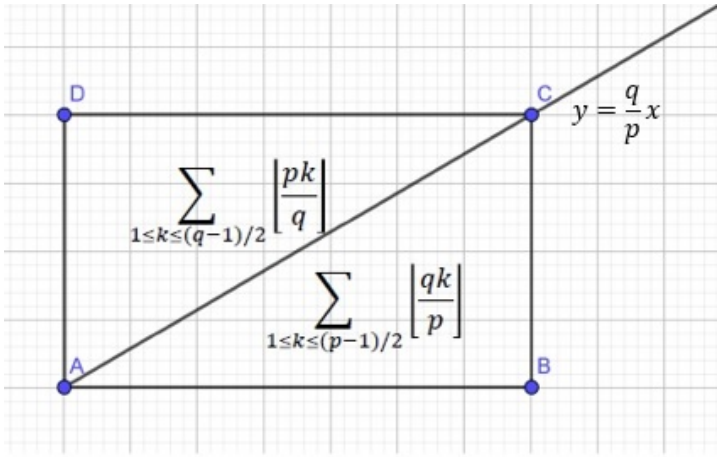

Figura 1 – Retângulo ABCD

Marquemos no interior deste retângulo pontos (x, y) tais que $1 \le x \le (p-1)/2$ e $1 \le y \le (q-1)/2$. Assim, temos $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ pontos interiores ao retângulo.

Consideremos a reta que passa pela diagonal do retângulo, isto é, pelos pontos A e C cuja equação é dada por $y = \frac{q}{p}x$. Dado $k \in \{1, 2, \cdots, (p-1)/2\}$, temos que o ponto $\left(k, \frac{q}{p}k\right)$ pertence a reta $y = \frac{q}{p}x$. Como $k \in \mathbb{N}$ isso implica que $\frac{qk}{p} \notin \mathbb{N}$. Portanto, o número de pontos com coordenadas inteiras no interior do triângulo ABC é:

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

Analogamente, consideremos $k \in \{1, 2, \cdots, (q-1)/2\}$, substituindo na equação $y = \frac{q}{p}x$ temos que $x = \frac{p}{q}k$. Do mesmo modo, $x = \frac{p}{q}k \notin \mathbb{N}$. O número de pontos cujas coordenadas são inteiras e estão no interior do triângulo ACD é:

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

Além disso

$$m_1 + m_2 = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Pelo Teorema 2.3 temos que

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

Logo

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

Portanto

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

□

Exemplo 2.11. *Se p é primo temos que*

$$\left(\frac{5}{p}\right) = \begin{cases} 1, \text{ se } p \equiv 1, 4 \ (mod\ 5) \\ -1, \text{ se } p \equiv 2, 3 \ (mod\ 5) \end{cases}$$

Com efeito, pela Lei da Reciprocidade Quadrática temos que

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

Isso implica que $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$, portanto:

- Se $p \equiv 1 \ (mod\ 5)$, pelo Teorema 2.2, temos que $\left(\frac{1}{5}\right) = 1$.
- Se $p \equiv 2 \ (mod\ 5)$, pelo Corolário 2.1, $\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = (-1)^3 = -1$.
- Se $p \equiv 3 \ (mod\ 5)$, de acordo com o Teorema 2.1, podemos afirmar que $3^{\frac{5-1}{2}} = 3^2 \equiv -1 \ (mod\ 5)$, por sua vez $\left(\frac{3}{5}\right) = -1$.
- Se $p \equiv 4 \ (mod\ 5)$, pelo Teorema 2.2, segue que $\left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = (-1)^2 = 1$.

Logo, 5 é um resíduo quadrático módulo p para $p \equiv 1 \ (mod\ 5)$ ou $p \equiv 4 \ (mod\ 5)$, e 5 não é resíduo quadrático módulo p quando $p \equiv 2 \ (mod\ 5)$ ou $p \equiv 3 \ (mod\ 5)$.

Exemplo 2.12. *O número* 51 *não é um resíduo quadrático módulo* 71.

De fato, como $51 = 3.17$ temos que $\left(\frac{51}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{17}{71}\right)$. Pela Lei da Reciprocidade Quadrática

$$\begin{aligned} \left(\frac{3}{71}\right)\left(\frac{71}{3}\right) &= (-1)^{\left(\frac{3-1}{2}\right)\left(\frac{71-1}{2}\right)} \\ &= (-1)^{35} \\ &= -1. \end{aligned}$$

Isso implica que $\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right) = -\left(\frac{2}{3}\right) = 1$.

De maneira análoga

$$\begin{aligned}\left(\frac{17}{71}\right)\left(\frac{71}{17}\right) &= (-1)^{(\frac{17-1}{2})(\frac{71-1}{2})} \\ &= (-1)^{8.35} \\ &= 1.\end{aligned}$$

A partir disso, temos que $\left(\frac{17}{71}\right) = \left(\frac{71}{17}\right) = \left(\frac{3}{17}\right) = -1$.

Portanto, $\left(\frac{51}{71}\right) = -1$, ou seja, 51 não é um resíduo quadrático módulo 71.

Corolário 2.2. *Se p e q são primos ímpares distintos, temos que*

1. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$, *se* $p \equiv 1 \ (mod\ 4)$ *ou* $q \equiv 1 \ (mod\ 4)$.

2. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$, *se* $p \equiv q \equiv 3 \ (mod\ 4)$.

Demonstração: Pela Lei da Reciprocidade Quadrática temos que

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

1. Sem perda de generalidade consideremos $p \equiv 1 \ (mod\ 4)$, então $p = 1 + 4k$, $k \in \mathbb{Z}$. Logo
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} = (-1)^{2k\frac{q-1}{2}} = 1.$$

2. Considerando que $p \equiv q \equiv 3 \ (mod\ 4)$, existem inteiros k e s tais que $p = 3 + 4k$ e $q = 3 + 4s$. Assim
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} = (-1)^{(2k+1)(2s+1)} = -1.$$

□

Corolário 2.3. *Sejam p e q primos tais que $p = q + 4a$, $a \in \mathbb{Z}$, então*

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

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

Demonstração:

1. Como $p = q + 4a \equiv 4a \ (mod\ q)$, segue que
$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{2}{q}\right)^2\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right).$$

2. Pela Lei da Reciprocidade Quadrática temos que
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})},$$
isso implica que
$$\left(\frac{p}{q}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}\left(\frac{q}{p}\right). \tag{2.11}$$
Por outro lado,
$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right) \tag{2.12}$$
uma vez que $p = q + 4a$ e $p - 4a \equiv -4a \ (mod\ p)$.
Considerando que $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$ e as equações 2.11 e 2.12
$$\left(\frac{a}{q}\right) = \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right).$$
Portanto
$$\left(\frac{a}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q+1}{2}}\left(\frac{a}{p}\right).$$
Como $p-q = 4a$, isso implica que $p \equiv q \ (mod\ 4)$. Além disso, como p e q são primos ímpares distintos, caso $p \equiv 1 \ (mod\ 4)$, então $\frac{p-1}{2}$ é par. Assim, $(-1)^{\frac{p-1}{2}\frac{q+1}{2}} = 1$. De maneira análoga, se $q \equiv 3 \ (mod\ 4)$, segue que $\frac{q+1}{2}$ é par, portanto $(-1)^{\frac{p-1}{2}\frac{q+1}{2}} = 1$. Logo, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

□

2.2.1 Demonstração de Kim

Nesta seção apresentaremos outra prova para a Lei da Reciprocidade Quadrática. Esta demonstração foi feita por Sey Y. Kim, no ano de 2004 [19]. Antes da prova do teorema, enunciaremos dois lemas que servirão como base para a demonstração matemática deste resultado. Consideremos o conjunto a seguir:

Sejam p, q dois primos ímpares distintos e defina
$$C = \left\{a; 1 \leq a \leq \frac{pq-1}{2}\right\}$$
tal que $(a, pq) = 1$ e considere $A = \prod_{a \in C} a$.

Lema 2.3. $A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \ (mod\ p)$ *e* $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \ (mod\ q)$.

Demonstração: Consideremos os conjuntos $D = \left\{a; 1 \leq a \leq \frac{pq-1}{2}\right\}$ em que $(a,p) = 1$ e $E = \left\{q \cdot 1, q \cdot 2, \cdots, q \cdot \frac{p-1}{2}\right\}$. Podemos admitir que E é um subconjunto de D, além disso, podemos escrever os elementos de D da seguinte forma:

$$\frac{pq-1}{2} = \frac{p-1}{2}q + \frac{q-1}{2}. \tag{2.13}$$

Assim, $C = D - E$ e pelo Teorema 2.1 temos

$$\begin{aligned} \prod_{a \in D} a = \prod_{a \in E} a \cdot \prod_{a \in C} a &= q \cdot 2q \cdots \frac{p-1}{2}q \cdot A & (2.14)\\ &= q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! A & (2.15)\\ &\equiv \left(\frac{q}{p}\right) \left(\frac{p-1}{2}\right)! A \ (mod\ p). & (2.16) \end{aligned}$$

De modo análogo, podemos escrever a equação 2.13 como

$$\frac{pq-1}{2} = \frac{q-1}{2}p + \frac{p-1}{2}. \tag{2.17}$$

Supondo sem perda de generalidade que $p < q$, temos que

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

Considerando os elementos do conjunto D e o Teorema de Wilson, note que

$$\begin{aligned} \prod_{a \in D} &\equiv (1 \cdot 2 \cdots (p-1))^{\frac{q-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) & (2.18)\\ &\equiv ((p-1)!)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! & (2.19)\\ &\equiv (-1)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \ (mod\ p) & (2.20) \end{aligned}$$

Assim, por 2.16 e 2.20 temos que

$$\begin{aligned} \left(\frac{q}{p}\right) \left(\frac{p-1}{2}\right)! A &\equiv (-1)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \ (mod\ p)\\ \left(\frac{q}{p}\right) A &\equiv (-1)^{\frac{q-1}{2}} \ (mod\ p)\\ A &\equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \ (mod\ p). \end{aligned}$$

De modo análogo, $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \ (mod\ q)$.

□

A partir do Lema acima podemos afirmar que $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$ se, e somente se, $A \equiv 1\ (mod\ pq)$ ou $A \equiv -1\ (mod\ pq)$.

Lema 2.4. *$A \equiv 1\ (mod\ pq)$ ou $A \equiv -1\ (mod\ pq)$ se, e somente se, $p \equiv q \equiv 1\ (mod\ 4)$.*

Demonstração: Suponhamos que $A \equiv 1\ (mod\ pq)$ ou $A \equiv -1\ (mod\ pq)$ e consideremos $d = pq$. Analisaremos as congruências $x^2 \equiv 1\ (mod\ d)$ e $x^2 \equiv -1\ (mod\ d)$.

Para determinar as soluções da congruência $x^2 \equiv 1\ (mod\ d)$ basta observar as equações: $x^2 \equiv 1\ (mod\ p)$ e $x^2 \equiv 1\ (mod\ q)$. A primeira dessas congruências, de acordo com a Proposição 2.3, possui as soluções 1 e $p-1$. Já a segunda congruência possui 1 e $q-1$ como soluções. Para determinar as soluções da congruência módulo d resolveremos os seguintes sistemas de equações.

$$\begin{cases} x \equiv 1\ \ (mod\ \ p) \\ x \equiv 1\ \ (mod\ \ q) \end{cases}$$

Pelo Teorema 1.4 sabemos que $x \equiv 1\ (mod\ d)$ é solução do sistema. Além disso, pelo Teorema Chinês do Resto, tomemos $M = d$, $M_1 = q$ e $M_2 = p$. Assim, consideremos as equações $qy \equiv 1\ (mod\ p)$ e $py \equiv 1\ (mod\ q)$ que possuem como soluções $y_1 = \alpha$ e $y_2 = \beta$, respectivamente. Portanto, a única solução do sistema módulo d é

$$x = M_1y_1c_1 + M_2y_2c_2 = q.\alpha.1 + p.\beta.1 \equiv q\alpha + p\beta\ \ (mod\ \ d).$$

Consequentemente, $x \equiv q\alpha + p\beta \equiv 1\ (mod\ d)$.

$$\begin{cases} x \equiv 1\ \ (mod\ \ p) \\ x \equiv q-1\ \ (mod\ \ q) \end{cases}$$

De modo análogo, a única solução do sistema módulo d é

$$x = M_1y_1c_1 + M_2y_2c_2 = q.\alpha.1 + p.\beta.(q-1) \equiv q\alpha - p\beta\ \ (mod\ \ d).$$

$$\begin{cases} x \equiv p-1\ \ (mod\ \ p) \\ x \equiv 1\ \ (mod\ \ q) \end{cases}$$

Analogamente, a única solução deste sistema é

$$x = M_1y_1c_1 + M_2y_2c_2 = q.\alpha.(p-1) + p.\beta.1 \equiv p\beta - q\alpha\ \ (mod\ \ d).$$

$$\begin{cases} x \equiv p-1 \equiv -1 \ (mod \ p) \\ x \equiv q-1 \equiv -1 \ (mod \ q) \end{cases}$$

Neste caso, pelo Teorema 1.4, a solução desse sistema é $x \equiv -1 \ (mod \ d)$.

Denotemos $z = q\alpha - p\beta \ (mod \ d)$, assim $-z = -(q\alpha - p\beta) \ (mod \ d)$. Logo, temos quatro soluções para a congruência $x^2 \equiv 1 \ (mod \ d)$, são elas: $1, -1, z, -z \ (mod \ d)$.

De maneira análoga resolveremos a congruência $x^2 \equiv -1 \ (mod \ d)$. De acordo com a Proposição 2.4, as equações $x^2 \equiv -1 \ (mod \ p)$ e $x^2 \equiv -1 \ (mod \ q)$ possuem solução se, e somente se, $p \equiv q \equiv 1 \ (mod \ 4)$.

Suponhamos que γ e $p - \gamma$ são soluções da equação $x^2 \equiv -1 \ (mod \ p)$ e que θ e $q - \theta$ são soluções de $x^2 \equiv -1 \ (mod \ q)$. Logo, para determinar as soluções da equação módulo d consideraremos os seguintes sistemas e o Teorema Chinês do Resto.

$$\begin{cases} x \equiv \gamma \ (mod \ p) \\ x \equiv \theta \ (mod \ q) \end{cases}$$

De acordo com o Teorema Chinês do Resto, $M = d$, $M_1 = q$ e $M_2 = p$. Consideremos as equações $qy \equiv 1 \ (mod \ p)$ e $py \equiv 1 \ (mod \ q)$ cujas soluções são $y_1 = \alpha$ e $y_2 = \beta$, respectivamente. A única solução módulo $M = d$ é

$$x = M_1 y_1 c_1 + M_2 y_2 c_2 = q\alpha\gamma + p\beta\theta \ (mod \ d).$$

$$\begin{cases} x \equiv p - \gamma \ (mod \ p) \\ x \equiv \theta \ (mod \ q) \end{cases}$$

A única solução para este sistema é

$$\begin{aligned} x = M_1 y_1 c_1 + M_2 y_2 c_2 = q\alpha(p-\gamma) + p\beta\theta &= pq\alpha - q\alpha\gamma + p\beta\theta \\ &\equiv -q\alpha\gamma + p\beta\theta \ (mod \ d). \end{aligned}$$

$$\begin{cases} x \equiv \gamma \ (mod \ p) \\ x \equiv q - \theta \ (mod \ q) \end{cases}$$

De maneira análoga, a única solução para o sistema acima é

$$\begin{aligned} x = M_1 y_1 c_1 + M_2 y_2 c_2 = q\alpha\gamma + p\beta(q-\theta) &= q\alpha\gamma + p\beta q - p\beta\theta \\ &\equiv q\alpha\gamma - p\beta\theta \ (mod \ d). \end{aligned}$$

$$\begin{cases} x \equiv p - \gamma \ (mod \ p) \\ x \equiv q - \theta \ (mod \ q) \end{cases}$$

Finalmente determinaremos a solução para o último sistema

$$\begin{aligned} x = M_1y_1c_1 + M_2y_2c_2 = q\alpha(p-\gamma) + p\beta(q-\theta) &= q\alpha p - q\alpha\gamma + p\beta q - p\beta\theta \\ &\equiv -q\alpha\gamma - p\beta\theta \ (mod\ d). \end{aligned}$$

Tomemos $u = q\alpha\gamma + p\beta\theta \ (mod\ d)$, então $-u = -(q\alpha\gamma + p\beta\theta) \ (mod\ d)$. De modo análogo, denotemos $v = q\alpha\gamma - p\beta\theta \ (mod\ d)$, logo $-v = -(q\alpha\gamma - p\beta\theta) \ (mod\ d)$. Portanto temos quatro soluções para a equação $x^2 \equiv -1 \ (mod\ d)$, são elas: $u, -u, v, -v \ (mod\ d)$.

Observando as soluções encontradas para as equações $x^2 \equiv 1 \ (mod\ d)$ e $x^2 \equiv -1 \ (mod\ d)$ e considerando que $d - y \equiv -y \ (mod\ d)$, note que se $k \in C$ temos que $1 \leq k \leq \dfrac{pq-1}{2}$ excluídos os números tais que $(k, pq) = 1$, por sua vez, $\dfrac{pq+1}{2} \leq d - k \leq pq - 1$, logo $(d-k) \notin C$. De maneira análoga, dado $k' \notin C$ isso implica que $\dfrac{pq+1}{2} \leq k' \leq pq-1$, consequentemente, $1 \leq d - k' \leq \dfrac{pq-1}{2}$, ou seja, $(d - k') \in C$.

Diante disso, podemos afirmar que quatro das soluções encontradas não pertencem ao conjunto C, mas as outras quatro soluções pertencem a C. Chamemos de G o conjunto formado por estas soluções. Note que para cada $a \in C$ deve existir $a' \in C$ tal que $a \cdot a' \equiv \pm 1 \ (mod\ d)$. Considerando o conjunto G, temos que $a = a'$, então

$$G = \{a \in C : a = a'\} = \{a \in C : a^2 \equiv \pm 1 \ (mod\ d)\}.$$

Observemos que

$$A = \prod_{a \in C} a \equiv \pm \prod_{a \in G} a \ (mod\ d).$$

Note que

$$\begin{aligned} \pm z \cdot u &= \pm(q\alpha - p\beta) \cdot (q\alpha\gamma + p\beta\theta) \\ &\equiv \pm[q^2\alpha^2\gamma - p^2\beta^2\theta] \\ &\equiv \pm(q\alpha + p\beta) \cdot (q\alpha\gamma - p\beta\theta) \\ &\equiv \pm[1 \cdot (q\alpha\gamma - p\beta\theta)] \\ &\equiv \pm(q\alpha\gamma - p\beta\theta) \ (mod\ d). \end{aligned}$$

Logo, $\pm z \cdot u \equiv \pm v \ (mod\ d)$.

Se $p \equiv q \equiv 1 \ (mod\ 4)$ segue que

$$\begin{aligned} \prod_{a \in G} a &\equiv \pm(1 \cdot z \cdot u \cdot v) \\ &\equiv \pm[1 \cdot z \cdot u \cdot (z \cdot u)] \\ &\equiv \pm(z^2 \cdot u^2) \\ &\equiv \mp 1 \ (mod\ d). \end{aligned}$$

Do contrário teríamos

$$\prod_{a\in G} a \equiv \pm(1\cdot z) \not\equiv \pm 1 \ (mod\ d).$$

□

Teorema 2.5. *(Lei da Reciprocidade Quadrática) Se p e q são primos ímpares distintos, então*

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

Demonstração: Pelos Lemas 2.3 e 2.4 temos que $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$ se, e somente se, $p \equiv q \equiv 1\ (mod\ 4)$.

Sendo p e q primos ímpares distintos, analisaremos quatro possíveis casos:

- $p \equiv 1\ (mod\ 4)$ e $q \equiv -1\ (mod\ 4)$;
- $p \equiv -1\ (mod\ 4)$ e $q \equiv 1\ (mod\ 4)$;
- $p \equiv -1\ (mod\ 4)$ e $q \equiv -1\ (mod\ 4)$;
- $p \equiv 1\ (mod\ 4)$ e $q \equiv 1\ (mod\ 4)$.

Mostraremos o primeiro caso, as outras demonstrações são análogas. Sendo $p \equiv 1\ (mod\ 4)$ e $q \equiv -1\ (mod\ 4)$ temos que $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \neq (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$, consequentemente $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = -(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$, então

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

Como $\frac{p+1}{2}$ é ímpar e $\frac{q+1}{2}$ é par, isso implica que $(-1)^{\frac{p+1}{2}\frac{q+1}{2}} = 1$, portanto

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

Note que

$$\begin{aligned}\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) &= \frac{pq-p-q+1}{4} = \frac{pq+p+q+1}{4} - \frac{p+q}{2}\\ &= \left(\frac{p+1}{2}\right)\left(\frac{q+1}{2}\right) - \left(\frac{p-1}{2}+\frac{q-1}{2}+1\right)\\ &\equiv \left(\frac{p+1}{2}\right)\left(\frac{q+1}{2}\right) + \left(\frac{p-1}{2}+\frac{q-1}{2}+1\right)\ (mod\ 2).\end{aligned}$$

Portanto

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

□

2.3 Símbolo de Jacobi

Nesta seção apresentaremos o símbolo de Jacobi, que é uma generalização do símbolo de Legendre. Foi desenvolvido em 1837 pelo matemático Carl Gustav Jakob Jacobi (1804-1851). O símbolo de Jacobi, diferente do símbolo de Legendre, é utilizado em números compostos.

Definição 2.4. *(Símbolo de Jacobi) Seja Q um inteiro positivo ímpar de modo que $Q = q_1 \cdot q_2 \cdots q_s$, onde q_j com $j = 1, \cdots, s$ são primos ímpares não necessariamente distintos. Então o símbolo de Jacobi $\left[\frac{P}{Q}\right]$ é definido como*

$$\left[\frac{P}{Q}\right] = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right)$$

onde $\left(\frac{P}{q_j}\right)$ é o símbolo de Legendre.

Observação 2.2. *Dados $P = 3$ e $Q = 7$ temos que $\left[\frac{3}{7}\right] = \left(\frac{3}{7}\right) = -1$, uma vez que $x^2 \equiv 3 \ (mod\ 7)$ não admite solução. De modo geral, se Q é um primo ímpar, o símbolo de Jacobi e o símbolo de Legendre se resumem a um mesmo processo.*

Observação 2.3. *Se $(P, Q) > 1$, então $\left[\frac{P}{Q}\right] = 0$.*

Observação 2.4. *Se $(P, Q) = 1$, temos que $\left[\frac{P}{Q}\right] = \pm 1$. Se P é um resíduo quadrático módulo Q, então P é um resíduo quadrático módulo q_j, onde $q_j | Q$, assim $\left(\frac{P}{q_j}\right) = 1$ para todo q_j com $j = 1, \cdots, s$. Portanto, $\left[\frac{P}{Q}\right] = 1$.*

Observação 2.5. *O fato de $\left[\frac{P}{Q}\right] = 1$ não significa que P é um resíduo quadrático módulo Q. Por exemplo, $\left[\frac{2}{15}\right] = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1$, mas $\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = -1$, implicando que a equação $x^2 \equiv 2 \ (mod\ 15)$ não possui solução.*

Teorema 2.6. *Suponha que Q e Q' são ímpares positivos, então*

1. $\left[\frac{P}{Q}\right]\left[\frac{P}{Q'}\right] = \left[\frac{P}{QQ'}\right]$.

2. $\left[\frac{P}{Q}\right]\left[\frac{P'}{Q}\right] = \left[\frac{PP'}{Q}\right]$.

3. *Se* $(P,Q)=1$, *então* $\left[\frac{P}{Q^2}\right] = \left[\frac{P^2}{Q}\right] = 1$.

4. *Se* $(PP', QQ') = 1$, *então* $\left[\frac{P'P^2}{Q'Q^2}\right] = \left[\frac{P'}{Q'}\right]$.

5. $P' \equiv P \ (mod\ Q)$ *implica que* $\left[\frac{P'}{Q}\right] = \left[\frac{P}{Q}\right]$.

Demonstração: Sejam $Q = q_1 \cdots q_m$ e $Q' = r_1 \cdots r_n$ tais que q_i e r_j com $i = 1, \cdots, m$ e $j = 1, \cdots, n$ são primos ímpares.

1. $$\left[\frac{P}{Q}\right]\left[\frac{P}{Q'}\right] = \left(\frac{P}{q_1}\right)\cdots\left(\frac{P}{q_m}\right)\left(\frac{P}{r_1}\right)\cdots\left(\frac{P}{r_n}\right) = \left[\frac{P}{q_1\cdots q_m r_1 \cdots r_n}\right] = \left[\frac{P}{QQ'}\right].$$

2. $$\begin{aligned}\left[\frac{P}{Q}\right]\left[\frac{P'}{Q}\right] = \left(\frac{P}{q_1}\right)\cdots\left(\frac{P}{q_m}\right)\left(\frac{P'}{q_1}\right)\cdots\left(\frac{P'}{q_m}\right) &= \left(\frac{P}{q_1}\right)\left(\frac{P'}{q_1}\right)\cdots\left(\frac{P}{q_m}\right)\left(\frac{P'}{q_m}\right) \\ &= \left(\frac{PP'}{q_1}\right)\cdots\left(\frac{PP'}{q_m}\right) \\ &= \left[\frac{PP'}{Q}\right].\end{aligned}$$

3. Como $(P,Q)=1$ e $\left[\frac{P^2}{Q}\right] = \left(\frac{P^2}{q_1}\right)\cdots\left(\frac{P^2}{q_m}\right)$, podemos afirmar que $(P,q_i)=1$ para $i = 1, \cdots, m$. Pelo Teorema de Fermat e pelo Teorema 2.1 temos que

   $$(P^2)^{\frac{q_i-1}{2}} = (P^{\frac{q_i-1}{2}})^2 = P^{q_i-1} \equiv 1 \ (mod\ q_i)$$

   isto é, $\left(\frac{P^2}{q_i}\right) = 1$, portanto $\left[\frac{P^2}{Q}\right] = 1$. Note também que

   $$\left[\frac{P^2}{Q}\right] = \left[\frac{P}{Q}\right]\left[\frac{P}{Q}\right] = \left[\frac{P}{Q}\right]^2 = 1.$$

4. Suponha que $(PP', QQ') = 1$, isso implica que $(P', Q) = (P, Q') = (P, Q) = (P', Q') = 1$. Pelos itens 1 e 2, temos que

   $$\left[\frac{P'P^2}{Q'Q^2}\right] = \left[\frac{P'}{Q'}\right]\left[\frac{P'}{Q^2}\right]\left[\frac{P^2}{Q'}\right]\left[\frac{P^2}{Q^2}\right] = \left[\frac{P'}{Q'}\right]$$

pois, pelo item 3, $\left[\frac{P'}{Q^2}\right] = \left[\frac{P^2}{Q'}\right] = 1$ e $\left[\frac{P^2}{Q^2}\right] = 1$, uma vez que $(P^2, Q) = 1$.

5. Suponha que $P' \equiv P \ (mod\, Q)$, como $\left[\frac{P'}{Q}\right] = \left(\frac{P'}{q_1}\right)\cdots\left(\frac{P'}{q_m}\right)$ e $\left[\frac{P}{Q}\right] = \left(\frac{P}{q_1}\right)\cdots\left(\frac{P}{q_m}\right)$, segue que $\left(\frac{P'}{q_i}\right) = \left(\frac{P}{q_i}\right)$ para $i = 1, \cdots, m$. Portanto, $\left[\frac{P'}{Q}\right] = \left[\frac{P}{Q}\right]$.

□

Exemplo 2.13. *Sendo $P = 11$ e $Q = 35$, como $35 = 5.7$, pela Definição 2.4, temos que* $\left[\frac{11}{35}\right] = \left(\frac{11}{5}\right)\left(\frac{11}{7}\right)$.

Pelo Teorema 2.2, $11 \equiv 1 \ (mod\ 5)$, *então* $\left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$. *De modo análogo,* $11 \equiv 4 \ (mod\ 7)$, *pelo Teorema 2.1,* $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) \equiv 4^{\frac{7-1}{2}} \equiv 4^3 \equiv 1 \ (mod\ 7)$. *Portanto,* $\left[\frac{11}{35}\right] = 1$.

Teorema 2.7. *Se $Q > 0$ é ímpar, então* $\left[\frac{-1}{Q}\right] = (-1)^{\frac{Q-1}{2}}$ *e* $\left[\frac{2}{Q}\right] = (-1)^{\frac{Q^2-1}{8}}$.

Demonstração: Sendo $Q = q_1 \cdot q_2 \cdots q_m$, note que

$$\left[\frac{-1}{Q}\right] = \prod_{i=1}^{m}\left(\frac{-1}{q_i}\right) = \prod_{i=1}^{m}(-1)^{\frac{q_i-1}{2}} = (-1)^{\sum_{i=1}^{m}\frac{q_i-1}{2}}.$$

Caso a e b sejam ímpares, temos que

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{ab-a-b+1}{2} = \frac{(a-1)(b-1)}{2} \equiv 0 \ (mod\ 2)$$
$$\Rightarrow \frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \ (mod\ 2).$$

Aplicando essa propriedade repetidas vezes, podemos afirmar que

$$\sum_{i=1}^{m}\frac{(q_i-1)}{2} \equiv \frac{1}{2}\left(\prod_{i=1}^{m} q_i - 1\right) \equiv \frac{Q-1}{2} \ (mod\ 2).$$

Consequentemente $\left[\frac{-1}{Q}\right] = (-1)^{\sum_{i=1}^{m}\frac{q_i-1}{2}} = (-1)^{\frac{Q-1}{2}}$. Analogamente, sendo a e b ímpares, temos que

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) = \frac{a^2b^2-a^2-b^2+1}{8} = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \ (mod\ 2)$$
$$\Rightarrow \frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} \ (mod\ 2).$$

Logo, $\sum_{i=1}^{m} \frac{q_i^2-1}{8} \equiv \frac{Q^2-1}{8} \ (mod\ 2)$ e, portanto

$$\left[\frac{2}{Q}\right] = \prod_{i=1}^{m}\left(\frac{2}{q_j}\right) = (-1)^{\sum_{i=1}^{m}\frac{q_i^2-1}{8}} = (-1)^{\frac{Q^2-1}{8}}.$$

□

Teorema 2.8. *Sejam P e Q inteiros positivos ímpares e $(P,Q)=1$, então*

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

Demonstração: Sejam $P = p_1 \cdots p_r$ e $Q = q_1 \cdots q_s$, pela Definição 2.4 e pelo Teorema 2.4 temos que

$$\begin{aligned}\left[\frac{P}{Q}\right] = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right) &= \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \\ &= \left[\frac{Q}{P}\right](-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2}}.\end{aligned}$$

Note que

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{(p_i-1)}{2}\cdot\frac{(q_j-1)}{2} = \sum_{i=1}^{r}\frac{(p_i-1)}{2}\sum_{j=1}^{s}\frac{(q_j-1)}{2}.$$

A partir da demonstração do Teorema 2.7 vimos que $\sum_{i=1}^{r}\frac{(p_i-1)}{2} \equiv \frac{P-1}{2} \ (mod\ 2)$ e $\sum_{j=1}^{s}\frac{(q_j-1)}{2} \equiv \frac{Q-1}{2} \ (mod\ 2)$. Portanto

$$\begin{aligned}\left[\frac{P}{Q}\right] = \left[\frac{Q}{P}\right](-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2}} &\Rightarrow \left[\frac{P}{Q}\right] = \left[\frac{Q}{P}\right](-1)^{\frac{P-1}{2}\frac{Q-1}{2}} \\ &\Rightarrow \left[\frac{P}{Q}\right]\left[\frac{Q}{P}\right] = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.\end{aligned}$$

□

2.4 Aplicações

Nesta seção apresentaremos duas aplicações da teoria vista.

2.4.1 Infinidade de Números Primos

Euclides (350 a. C.) foi o primeiro matemático a mostrar que o conjunto dos números primos é infinito, isto é, $P = \{2, 3, 5, 7, \cdots\}$. O resultado a seguir trata da infinidade de números primos da forma $3k+1$, com $k \in \mathbb{Z}$.

Teorema 2.9. *Existem infinitos primos da forma* $3k+1$*, com* $k \in \mathbb{N}$*.*

Demonstração: Suponhamos por contradição que o conjunto de primos da forma $3k+1$ é finito, ou seja, $P = \{p_1, p_2, \cdots, p_r\}$ para algum $r \in \mathbb{N}$. Inicialmente observemos que o primo 2 não pode ser escrito na forma $3k+1$, do contrário, $2 = 3\alpha+1$, assim $1 = 3\alpha$, isso implica que $3 \mid 1$, o que é um absurdo. Analogamente, $3 \neq p_i$ com $i = 1, \cdots, r$, pois $3 \neq 3k+1$ para todo $k \in \mathbb{N}$. Assim, tomemos o número

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

Consideremos p um divisor primo de n. Neste caso, $p \neq 2$, uma vez que n é ímpar. Além disso, p não pode ser nenhum dos primos $3, p_1, \cdots, p_r$. De fato, se $p = 3$ teríamos que $3|p_i$ para algum $i = 1, \cdots, r$. Caso $p = p_i$ isso implica que $p_i|3$, mas isso não é possível, pois $p_i \neq 3$ para todo $i = 1, \cdots, r$. Consequentemente p é da forma $3k+2$, logo $p \equiv -1$ $(mod\ 3)$ e como $p|n$, segue que

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

o que implica que $\left(\frac{-3}{p}\right) = 1$. Porém

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right). \tag{2.21}$$

No entanto, pela Lei da Reciprocidade Quadrática,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}. \tag{2.22}$$

A partir das igualdades 2.21 e 2.22 temos que

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

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

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

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

□

2.4.2 $\sqrt{2}$ é irracional

O primeiro matemático a demonstrar que $\sqrt{2}$ é um número irracional foi Euclides. Ele usou o método de redução ao absurdo junto com técnicas de aritmética. Aqui mostraremos a irracionalidade de 2 por meio do método de redução ao absurdo combinado com alguns resultados da Teoria de Resíduos Quadráticos.

Teorema 2.10. *$\sqrt{2}$ é irracional.*

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

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

Consequentemente,

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

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

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

Pelo símbolo de Legendre, $\left(\frac{a^2}{p}\right) = 1$ e $\left(\frac{b^2}{p}\right) = 1$, mas, como $a^2 \equiv 2b^2 \ (mod\ p)$, segue que

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

Pelo Corolário 2.1, temos que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Se $p \equiv 3 \ (mod\ 8)$, existe um inteiro k tal que $p = 8k + 3$, assim:

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

logo, $\frac{p^2-1}{8}$ é ímpar e, portanto, $\left(\frac{2}{p}\right) = -1$.

Se $p \equiv -3 \ (mod\ 8)$, existe k inteiro tal que $p = 8k - 3$, então

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

o que implica que $\frac{p^2-1}{8}$ é ímpar, portanto $\left(\frac{2}{p}\right) = -1$. Temos uma contradição! Portanto, $\sqrt{2}$ é irracional.

□

3 Problemas Olímpicos

Neste capítulo trabalharemos problemas de Olimpíadas de Matemática que podem ser resolvidos com os resultados apresentados nos capítulos anteriores. Falaremos um pouco sobre cada uma das olimpíadas das quais os problemas a seguir foram retirados. Além disso, apresentaremos um problema retirado de um portal dedicado à olimpíadas de matemática e outro de um periódico científico.

3.1 Olimpíada Internacional de Matemática

A Olimpíada Internacional de Matemática (IMO) é a maior competição de matemática do mundo. O evento é voltado para alunos do ensino médio cujos objetivos são encorajá-los e desafiá-los, além de criar oportunidades e trocas de experiências entre os participantes. Os problemas da IMO são organizados em quatro áreas: Álgebra, Combinatória, Geometria e Teoria dos Números.

Sua primeira edição aconteceu no ano de 1959, na Romênia, e contou com a participação de estudantes de outros seis países: Alemanha Oriental, Bulgária, Checoslóvaquia, Hungria, Polônia e URSS. Desde então o evento acontece todos os anos, sempre em um país diferente.

O Brasil participou da competição pela primeira vez no ano de 1979, chegando a sediar o evento em 2017. No ano de 2020, o país soma um total de 142 medalhas, sendo o país latino-americano mais premiado na competição.

Atualmente, o torneio possui a colaboração de mais de 100 países, sendo que cada país pode enviar uma equipe de até seis alunos (com menos de 20 anos) do ensino médio ou alunos que ainda não tenham ingressado no ensino superior para participarem da competição. Além disso, cada equipe possui um professor líder e um professor vice-líder. Tais equipes são formadas a partir de uma seleção específica em cada país. A delegação brasileira é formada a partir do desempenho na OBMEP.

3.1.1 IMO-1996

Problema 3.1. *Sejam a e b inteiros positivos tais que os números $15a+16b$ e $16a-15b$ são quadrados de inteiros positivos. Qual é o menor valor possível que pode ter o menor desses números?*

Demonstração: Sejam x e y inteiros positivos tais que $15a+16b = x^2$ e $16a-15b =$

y^2. Multiplicando a primeira equação por 16 e a segunda por 15 temos que

$$\begin{aligned} 240a + 256b &= 16x^2 \quad (3.1) \\ 240a - 225b &= 15y^2 \quad (3.2) \end{aligned}$$

Fazendo a subtração entre 3.1 e 3.2 temos que $481b = 16x^2 - 15y^2$. De modo análogo, multiplicando a primeira equação por 15 e a segunda por 16 obtemos

$$\begin{aligned} 225a + 240b &= 15x^2 \quad (3.3) \\ 256a - 240b &= 16y^2 \quad (3.4) \end{aligned}$$

Somando as equações 3.3 e 3.4 temos que $481a = 15x^2 + 16y^2$. Note que $481 = 13 \cdot 37$, então $37|[(16x^2 - 15y^2) - (15x^2 + 16y^2)] = x^2 - 31y^2$, o que equivale dizer que $x^2 \equiv 31y^2$ $(mod\ 37)$.

Suponha que y não é divisível por 37, então $37 \nmid x$. Como $31y^2$ é um resíduo quadrático módulo 37, note que

$$\begin{aligned} \left(\frac{31y^2}{37}\right) &= \left(\frac{31}{37}\right)\left(\frac{y^2}{37}\right) \\ &= \left(\frac{-6}{37}\right)\left(\frac{y^2}{37}\right) \\ &= \left(\frac{6}{37}\right)\left(\frac{-1}{37}\right) \\ &= \left(\frac{2}{37}\right)\left(\frac{3}{37}\right)(-1)^{\frac{37-1}{2}} \\ &= (-1)^{\frac{37^2-1}{8}}\left(\frac{3}{37}\right) \\ &= -\left(\frac{3}{37}\right). \end{aligned}$$

Pela Lei da Reciprocidade Quadrática, $\left(\frac{3}{37}\right)\left(\frac{37}{3}\right) = (-1)^{\frac{37-1}{2}\cdot\frac{3-1}{2}} = 1$. Mas $\left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1$, o que implica que $\left(\frac{3}{37}\right) = 1$. Portanto, $\left(\frac{31y^2}{37}\right) = -\left(\frac{3}{37}\right) = -1$. Temos uma contradição. Logo, $31y^2$ não é resíduo quadrático módulo 37. Assim, $37|x$ e $37|y$.

Como $13|(x^2 - 31y^2)$, isso equivale a $x^2 \equiv 31y^2 \equiv 5y^2$ $(mod\ 13)$. Suponha que y não é divisível por 13, portanto x também não é divisível por 13. Nesse caso, $5y^2$ é um resíduo quadrático módulo 13, então

$$\left(\frac{5y^2}{13}\right) = \left(\frac{5}{13}\right)\left(\frac{y^2}{13}\right) = \left(\frac{5}{13}\right).$$

Pela Lei da Reciprocidade Quadrática temos que $\left(\frac{5}{13}\right)\left(\frac{13}{5}\right) = (-1)^{\frac{5-1}{2}\frac{13-1}{2}} = 1$, portanto $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} \equiv -1 \ (mod\ 5)$. Logo, $\left(\frac{5y^2}{13}\right) = -1$.

Temos outra contradição. Assim, $13|x$ e $13|y$. Portanto, $481|x$ e $481|y$, além disso, $481^2|x^2$ e $481^2|y^2$, então x^2 e y^2 são, no mínimo, iguais a 481^2. Consequentemente

$$a = \frac{15 \cdot 481^2 + 16 \cdot 481^2}{481} = 481 \cdot 31$$

$$b = \frac{16 \cdot 481^2 - 15 \cdot 481^2}{481} = 481.$$

Logo, o menor desses números é, no mínimo, $b = 481$.

□

3.1.2 IMO-1998

Problema 3.2. *Determine todos os números inteiros positivos n para os quais existe um número inteiro m tal que $2^n - 1$ é um divisor de $m^2 + 9$.*

Demonstração: Suponha que $(2^n - 1)|(m^2 + 9)$, então $m^2 + 9 \equiv 0 \ (mod\ 2^n - 1)$, equivalentemente temos que

$$m^2 \equiv -9 \ (mod\ 2^n - 1).$$

Analisaremos n em dois casos:

Se $n > 1$ for um número ímpar temos que $2^n - 1 > 3$. Neste caso,

$$2^n \equiv 0 \ (mod\ 4) \Rightarrow 2^n - 1 \equiv -1 \ (mod\ 4).$$

Diante disso, o número $2^n - 1$ possui pelo menos um divisor primo p tal que $p \equiv 3$ $(mod\ 4)$. Assim, $\frac{p-1}{2}$ é ímpar e, pela Lei da Reciprocidade Quadrática, segue que:

$$\left(\frac{-9}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{9}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)^2 = (-1)^{\frac{p-1}{2}} = -1.$$

Portanto, $p \nmid (m^2 + 9)$ o que implica que -9 não é um resíduo quadrático módulo $2^n - 1$. Logo, n não pode ser ímpar.

Se n for par temos que

$$2 \equiv -1 \ (mod\ 3) \Rightarrow 2^n \equiv 1 \ (mod\ 3),$$

isso implica que $3|(2^n-1)$. Suponha que $n=2^kq$ com $k,q\in\mathbb{N}$ e $q>1$, então

$$2^n-1=2^{2^kq}-1=(2^{2^{k-1}q}+1)(2^{2^{k-2}q}+1)\cdots(2^q-1).$$

Sendo q ímpar temos que $2^q-1\equiv 3\ (mod\ 4)$, pelo mesmo argumento utilizado acima, temos que $(2^q-1)\nmid(m^2+9)$. Absurdo! Portanto, $q=1$, assim $n=2^k$.

□

O problema a seguir esteve em uma das provas de seleção de equipes do Vietnã. Tal seleção tinha o objetivo de escolher estudantes para participarem da Olimpíada Internacional de Matemática (IMO).

3.1.3 Olimpíada de Matemática do Vietnã-2004

Problema 3.3. *Prove que 2^n+1 não possui fatores primos da forma $8k+7$.*

Demonstração: Suponha que existe p primo tal que $p|(2^n+1)$ e $p\equiv 7\ (mod\ 8)$. Isso implica que $2^n\equiv -1\ (mod\ p)$.

Se n for par, então

$$2^n\equiv -1\ (mod\ p)\Rightarrow 2^n=(2^k)^2\equiv -1\ (mod\ p).$$

Neste caso, $\left(\frac{-1}{p}\right)=1$, ou seja, -1 é um resíduo quadrático módulo p.

Porém, como $p\equiv 7\ (mod\ 8)$ temos que $p=8k+7=4(2k+1)+3$. Sendo $p=4t+3$, com $t\in\mathbb{Z}$, pela Proposição 2.4, -1 não é resíduo quadrático módulo p. Portanto, $\left(\frac{-1}{p}\right)=-1$. Temos uma contradição!

Caso n seja ímpar, note que

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

Logo, $\left(\frac{-2}{p}\right)=1$, isto é, -2 é um resíduo quadrático módulo p. Mas, pelo Teorema 2.2 e pelo Corolário 2.1, temos que

$$\begin{aligned}\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}\\ &= (-1)^{\frac{8k+6}{2}}(-1)^{\frac{(8k+7)^2-1}{8}}\\ &= (-1)^{4k+3}(-1)^{\frac{64k^2+56k+48}{8}}\\ &= -(-1)^{8k^2+7k+6}\\ &= -(-1)^{(8k+6)(8k+3)}=-1.\end{aligned}$$

Temos outra contradição. Portanto, $2^n + 1$ não possui fatores primos da forma $8k + 7$.

□

O próximo problema esteve na prova da Olimpíada Nacional de Matemática de Taiwan, no ano de 1997. Esta competição também tem como um dos objetivos selecionar estudantes para participarem da IMO.

3.1.4 Olimpíada de Matemática de Taiwan-1997

Problema 3.4. *Seja n um inteiro positivo tal que $k = 2^{2^n} + 1$. Mostre que k é primo se, e somente se, $k \mid (3^{\frac{k-1}{2}} + 1)$.*

Demonstração: Suponha que $k \mid (3^{\frac{k-1}{2}} + 1)$, então $3^{\frac{k-1}{2}} \equiv -1 \ (mod\ k)$. Assim, $3^{k-1} \equiv 1 \ (mod\ k)$.

Seja $d = ord_k 3$, pela Proposição 1.7, temos que $d|(k-1)$ e $d \nmid (k-1)/2$. Como $k - 1 = 2^{2^n}$, segue que $d|2^{2^n}$, mas $d \nmid 2^{2^n-1}$. Isso implica que $d = 2^{2^n} = k - 1$. Além disso, pelo Corolário 1.2, $d|\phi(k)$. Como $1 \leq \phi(k) \leq k - 1$, temos que $\phi(k) = k - 1$, então k é primo.

De modo análogo, suponha que k é primo. Além disso, note que

$$2^{2^n} \equiv 1 \ \ (mod\ 3) \Rightarrow 2^{2^n} + 1 \equiv 2 \ \ (mod\ 3),$$

portanto $k \equiv 2 \ (mod\ 3)$. Pela Lei da Reciprocidade Quadrática, temos que

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

Consequentemente, $\left(\frac{3}{k}\right) = \left(\frac{k}{3}\right)$. Daí $\left(\frac{k}{3}\right) = \left(\frac{2}{3}\right) = -1$. Isso implica que $-1 = \left(\frac{3}{k}\right) \equiv 3^{\frac{k-1}{2}} \ (mod\ k)$, isto é, $k|(3^{\frac{k-1}{2}} + 1)$.

□

3.2 Eötvös-Kürschák Competition

A Eötvös-Kürschák Competition é um campeonato de matemática realizado na Hungria. Esta competição foi fundada em 1894, sendo a mais antiga do mundo e foi chamada de Eötvös Mathematical Competition até 1938. Seu nome mudou de Eötvös para Kürschák a partir da Segunda Guerra Mundial. O torneio consiste na resolução de 3 problemas destinados a alunos que cursaram até o primeiro ano do ensino superior.

Problema 3.5. *Dado $n \in \mathbb{Z}$, se $2 + 2\sqrt{28n^2 + 1}$ é um inteiro, então é um quadrado perfeito.*

Demonstração: Se $2 + 2\sqrt{28n^2 + 1}$ é um inteiro, então $\sqrt{28n^2 + 1}$ é inteiro. Suponha que $28n^2 + 1$ seja um quadrado perfeito. Observe que $28n^2 + 1$ é um número ímpar, então

$$\begin{aligned} 28n^2 + 1 &= (2k + 1)^2 \\ 28n^2 + 1 &= 4k^2 + 4k + 1 \\ 28n^2 &= 4k^2 + 4k \\ 7n^2 &= k(k + 1). \end{aligned}$$

Logo $7|k$ ou $7|(k + 1)$. Como $(k, k + 1) = 1$, pela Proposição 1.4, temos dois casos. O primeiro deles é: $k = x^2$ e $(k + 1)/7 = y^2$. Assim, $1 = (k + 1) - k = 7y^2 - x^2$, ou seja, $x^2 \equiv -1 \ (mod\ 7)$. Porém, pela Proposição 2.4, -1 não é resíduo quadrático módulo 7. Diante disso, temos uma contradição.

O outro caso é: $k/7 = x^2$ e $k + 1 = y^2$, então $1 = (k + 1) - k = y^2 - 7x^2$, o que implica que $y^2 \equiv 1 \ (mod\ 7)$. Como 1 é resíduo quadrático módulo 7, essa condição é válda. Logo

$$\begin{aligned} 2 + 2\sqrt{28n^2 + 1} &= 2 + 2\sqrt{(2k + 1)^2} \\ &= 2 + 2(2k + 1) \\ &= 2 + 4k + 2 \\ &= 4(k + 1) \\ &= 4y^2 \\ &= (2y)^2. \end{aligned}$$

Fica provado que $2 + 2\sqrt{28n^2 + 1}$ é um quadrado perfeito.

□

3.3 AwesomeMath

Nesta seção apresentaremos um problema do portal AwesomeMath [21]. Seu objetivo é proporcionar experiências enriquecedoras em matemática para alunos e professores por meio de acampamentos de verão, publicações, currículo e competições. Este portal foi criado em 2006 pelo Dr. Titu Andreescu que dedicou sua carreira a desafios e competições matemáticas. O problema foi publicado no ano de 2009. Antes de apresentá-lo, demonstraremos duas proposições que servirão como base para a demonstração do problema.

Proposição 3.1. *Seja p um primo ímpar. O número -3 é um resíduo quadrático módulo p se, e somente se, $p \equiv 1$ $(mod\ 6)$.*

Demonstração: Seja p um primo ímpar, então

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

Pela Lei da Reciprocidade Quadrática

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

Consequentemente

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

Como p é um primo ímpar podemos escrevê-lo em uma das formas: $6k_1+1, 6k_2+3$ ou $6k_3+5$ com $k_i \in \mathbb{Z}$, $i = 1, 2, 3$.

Se $p = 6k_1 + 1$, temos que $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.

Se $p = 6k_2 + 3$, segue que $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 0$.

Se $p = 6k_3 + 5$, temos que $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Portanto, -3 é um resíduo quadrático módulo p se, e somente se, $p \equiv 1$ $(mod\ 6)$.

□

Proposição 3.2. *Seja p um primo ímpar. O número 5 é um resíduo quadrático módulo p se, e somente se, $p \equiv \pm 1$ $(mod\ 10)$.*

Demonstração: Seja p um primo ímpar, pela Lei da Reciprocidade Quadrática

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

Isso implica que $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Sendo p um primo ímpar, podemos escrevê-lo em uma das formas: $10\mathrm{k}_1 \pm 1$ e $10k_2 \pm 3$ com $k_i \in \mathbb{Z}$ e $i = 1, 2$. Diante disso, temos que:

Se $10k_1 + 1$, segue que $\left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$. De modo análogo, se $p = 10k_1 - 1$, temos que $\left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) = 1$.

Se $10k_2+3$, temos que $\left(\frac{p}{5}\right)=\left(\frac{3}{5}\right)=-1$. Analogamente, sendo $p=10k_2-3$, isso implica que $\left(\frac{p}{5}\right)=\left(\frac{-3}{5}\right)=-1$.

Portanto, 5 é um resíduo quadrático módulo p se, e somente se, para $p\equiv\pm1$ $(mod$ 10).

□

Problema 3.6. *(MR-2009) Se m for um número inteiro positivo, mostre que 5^m+3 não tem um divisor primo da forma $p=30k+11$ ou $p=30k-1$.*

Demonstração: Analisaremos os dois casos. Se $p=30k+11$, suponhamos que m é par. Neste caso

$$5^m\equiv-3\ (mod\ p)\Rightarrow 5^m=(5^k)^2\equiv-3\ (mod\ p).$$

Assim, $\left(\frac{-3}{p}\right)=1$, isto é, -3 é um resíduo quadrático módulo p.

Como $p\equiv 11$ $(mod$ 30) temos que $p=30k+11=6(5k+1)+5=6t+5$, isto implica que $p\equiv 5$ $(mod$ 6), mas, pela Proposição 3.1, segue que $\left(\frac{-3}{p}\right)=-1$. Temos uma contradição.

Se m é ímpar, temos que

$$5^m\equiv-3\ (mod\ p)\Rightarrow 5^{2k-1}\equiv-3\ (mod\ p)\Rightarrow 5^{2k}\equiv-15\ (mod\ p).$$

Logo $\left(\frac{-15}{p}\right)=1$, isto é, -15 é um resíduo quadrático módulo p. Sabemos que $\left(\frac{-15}{p}\right)=\left(\frac{-3}{p}\right)\left(\frac{5}{p}\right)$.

Sendo $p\equiv 11$ $(mod$ 30) temos que $p=30k+11=10(3k+1)+1$, o que implica que $p\equiv 1$ $(mod$ 10). Pela Proposição 3.2, temos que $\left(\frac{5}{p}\right)=1$. No entanto, $\left(\frac{-3}{p}\right)=-1$, logo

$$\left(\frac{-15}{p}\right)=\left(\frac{-3}{p}\right)\left(\frac{5}{p}\right)=-1.$$

Temos outra contradição.

Se $p=30k-1$, suponhamos que m é par. Então

$$5^m\equiv-3\ (mod\ p)\Rightarrow 5^m=(5^k)^2\equiv-3\ (mod\ p).$$

Assim, $\left(\frac{-3}{p}\right)=1$, isto é, -3 é um resíduo quadrático módulo p.

Agora, como $p \equiv -1 \equiv 29 \ (mod\ 30)$ temos que $p = 30k + 29 = 6(5k + 4) + 5$, o que implica que $p \equiv 5 \ (mod\ 6)$. Novamente temos uma contradição, pois $\left(\frac{-3}{p}\right) = -1$.

Quando m é ímpar, temos que

$$5^m \equiv -3 \ (mod\ p) \Rightarrow 5^{2k-1} \equiv -3 \ (mod\ p) \Rightarrow 5^{2k} \equiv -15 \ (mod\ p).$$

De modo análogo, $p \equiv 29 \ (mod\ 30)$, assim $p = 30k + 29 = 10(3k + 2) + 9$, o que implica que $p \equiv -1 \ (mod\ 10)$. Novamente, pela Proposição 3.2, temos que $\left(\frac{5}{p}\right) = 1$. No entanto, $\left(\frac{-3}{p}\right) = -1$, logo

$$\left(\frac{-15}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{5}{p}\right) = -1.$$

Temos outra contradição. Portanto nenhum divisor do número $5^m + 3$ é da forma $p = 30k + 11$ ou $p = 30k - 1$.

□

3.4 American Mathematical Monthly

Nesta seção abordaremos um problema da referência [11]. Este problema foi publicado no periódico científico The American Mathematical Monthly. Tal jornal foi fundado em 1894 e atualmente é publicado dez vezes por ano pela Mathematical Association of America. O periódico é destinado, de modo geral, a estudantes da graduação e profissionais de pesquisa.

Problema 3.7. *Encontre todos os inteiros positivos n de modo que* $(2^n - 1)|(3^n - 1)$.

Demonstração: Mostraremos que $n = 1$ é a única solução para o problema.

Suponhamos que existe $n > 1$ sendo solução.

Como $3^n - 1$ não é um múltiplo de 3, então $2^n - 1$ não pode ser múltiplo de 3, isto é, $3 \nmid (2^n - 1)$. Portanto n não pode ser um número par.

Sendo n ímpar, temos que $2^n \equiv 8 \ (mod\ 12)$, daí $2^n - 1 \equiv 7 \ (mod\ 12)$.

Qualquer número primo ímpar maior que 3 pode ser escrito em uma das formas: $12k_1 \pm 1$ ou $12k_2 \pm 5$ com $k_1, k_2 \in \mathbb{Z}$. Neste caso, $2^n - 1$ possui pelo menos um divisor primo p da forma $12k \pm 5$, com $k \in \mathbb{Z}$. Além disso, temos que

$$\begin{aligned} 3^n - 1 \equiv 0 \ (mod\ 2^n - 1) &\Rightarrow 3^n \equiv 1 \ (mod\ 2^n - 1) \\ &\Rightarrow 3^{2t+1} \equiv 1 \ (mod\ 2^n - 1) \\ &\Rightarrow (3^{t+1})^2 \equiv 3 \ (mod\ 2^n - 1). \end{aligned}$$

Logo, 3 é um resíduo quadrático módulo $2^n - 1$. Sendo p um divisor primo de $2^n - 1$ devemos ter $\left(\frac{3}{p}\right) = 1$. Pela Lei da Reciprocidade Quadrática tem-se

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

Se $p \equiv 5 \ (mod\ 12)$ segue que $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Se $p \equiv -5 \ (mod\ 12)$ temos que $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = -\left(\frac{-2}{3}\right) = -\left(\frac{1}{3}\right) = -1$.

Portanto, 3 não é resíduo quadrático módulo p se $p = 12k \pm 5$. Consequentemente a única solução para o problema é dada quando $n = 1$.

□

4 Aplicação em sala de aula

A BNCC e o Novo Ensino Médio são as mais recentes mudanças na educação básica do Brasil. A Base Nacional Comum Curricular é um documento que norteará a elaboração dos currículos das escolas brasileiras, além de trazer habilidades e competências que devem ser desenvolvidas pelos estudantes ao longo da educação básica. O Novo Ensino Médio traz uma ampliação da carga horária desta etapa da educação básica e a elaboração de currículos baseados na BNCC.

Uma das propostas do Novo Ensino Médio é desenvolver o protagonismo e a autonomia de cada estudante. Além disso, outro diferencial é a inserção dos itinerários formativos que são o conjunto de disciplinas ou projetos disponíveis para que os alunos possam escolher de acordo com a sua preferência. Os itinerários formativos também podem ser organizados por área de conhecimento ou numa formação técnica e profissional. Neste caso, os estudantes poderão aprofundar os seus conhecimentos em determinadas áreas a partir das ofertas feitas pela escola.

Diante disso e considerando a proposta deste trabalho, neste capítulo apresentaremos uma breve sugestão de abordagem do conteúdo em sala de aula. Esta atividade é destinada aos alunos do ensino médio dentro do itinerário formativo direcionado para a área de matemática. O quadro abaixo traz um cronograma para o desenvolvimento da proposta.

Cronograma

1º aula	2 aulas de 50 minutos	Resíduos Quadráticos e Símbolo de Legendre
2º aula	2 aulas de 50 minutos	Apresentação dos Resultados e Exemplos
3º aula	1 aula de 50 minutos	Problemas de Olimpíadas Internacionais de Matemática
4º aula	1 aula de 50 minutos	Problemas de Olimpíadas Internacionais de Matemática

Objetivos

- Representar por meio da notação $x^2 \equiv a \ (mod\ p)$ a divisão cujo dividendo é o x^2, p é o divisor e a é o resto.
- Verificar quando a equação $x^2 \equiv a \ (mod\ p)$ admite solução, ou seja, se a é ou não um resíduo quadrático módulo p.

- Associar o número 1 ao fato de a ser resíduo quadrático módulo p e -1 o caso contrário.
- Aplicar os resultados apresentados no texto.
- Compreender os problemas de olimpíadas presentes no trabalho.

Desenvolvimento

- Na primeira aula, o professor introduzirá o conceito de resíduo quadrático por meio de uma análise feita a partir de determinados exemplos. Em seguida será apresentado o símbolo de Legendre.
- Na segunda aula, serão apresentados alguns dos teoremas e os exemplos presentes no capítulo 2 deste trabalho.
- Nas aulas 3 e 4, o professor apresentará as soluções de alguns problemas de olimpíadas trazidos no texto.

1º Aula: Resíduos Quadráticos e Símbolo de Legendre

Nesta etapa, o professor irá propor as seguintes questões aos alunos. A partir da resolução de cada uma delas o professor fará questionamentos e análises. No tópico seguinte citamos alguns comentários que o professor pode fazer durante a aplicação.

1- Divida os números $10, 12, 21, 33$ e 54 por 5.

2- Divida os números $10, 12, 21, 30, 39, 43$ e 55 por 7.

3- Escreva as divisões acima utilizando a notação $a \equiv b \ (mod\ p)$ onde a é o dividendo, p é o divisor e b é o resto.

4- Divida os números $10^2, 12^2, 21^2, 33^2$ e 54^2 por 5.

5- De maneira análoga ao item 3, escreva as divisões do item anterior utilizando a notação de congruência.

6- Determine todos os possíveis restos numa divisão de x^2 por 7.

7- Quais as congruências $x^2 \equiv a \ (mod\ 7)$ possuem solução e quais não possuem?

8- Considerando $p = 7$, determine $\left(\frac{a}{p}\right)$.

Comentários

- Nas etapas 1 e 2 o professor chamará a atenção dos alunos para os restos encontrados. Neste momento, o objetivo é mostrar para o aluno que numa divisão por p os restos possíveis compõem o conjunto $R = \{0, 1, 2, \cdots, p-1\}$.

- No item 3 o professor explicará para a turma a representação de uma divisão por meio da notação de congruência e, em seguida, eles representarão por meio da notação de congruência as divisões feitas nos itens 1 e 2.

- Neste momento será feito algo parecido com os itens 1 e 2. Novamente chamando a atenção para os restos, pois, no caso dos resíduos quadráticos, temos $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ resíduos não quadráticos. O intuito é fazer os alunos perceberem esse fato.

- Neste item o professor pode chamar atenção para fatos como $1^2 \equiv 1 \ (mod\ 7)$ e $6^2 \equiv 1 \ (mod\ 7)$. Além disso, $7 - 1 = 6$, isto é, dada a congruência $x^2 \equiv a \ (mod\ p)$, se b é solução, $p - b$ também é.

- No item 7 o aluno associará a solubilidade da congruência $x^2 \equiv a \ (mod\ 7)$ ao fato de a ser ou não um resíduo quadrático módulo 7.

- Antes da situação 8, o professor apresentará a definição do Símbolo de Legendre.

2º Aula: Apresentação dos Resultados e Exemplos

Neste momento, o professor apresentará alguns dos resultados presentes no capítulo 2. Esta etapa tem como objetivo oferecer novas ferramentas para que os alunos possam determinar quando um número é ou não resíduo quadrático módulo p. Ao longo disso, sugerimos a aplicação das seguintes questões.

1- Verifique se 9 é um resíduo quadrático módulo 13.

2- Calcule:

a) $\left(\frac{6}{13}\right)$

b) $\left(\frac{19}{13}\right)$

3- Verifique se 7 é um resíduo quadrático módulo 11.

4- Resolva a questão anterior utilizando o Teorema 2.3.

5- Determine $\left(\frac{11}{43}\right)$.

Comentários

- Neste momento, o professor pode começar pedindo para que os alunos tentem resolver a questão 1. Diante das respostas obtidas ele pode apresentar o Teorema 2.1 e o Exemplo 2.8 e, em seguida, pedir que os alunos tentem fazer a mesma análise, no entanto, utilizando o Critério de Euler.

- Nesta etapa, o professor apresentará as propriedades referentes ao símbolo de Legendre contidas no Teorema 2.2 e solicitará que os alunos apliquem algumas delas na questão 2.

- Antes de resolver o problema 3, o professor apresentará o Lema de Gauss e o Exemplo 2.9. Em seguida, deve propor que os alunos resolvam o problema 3.

- Dando continuidade ao estudo, antes da resolução da questão 4, o professor pode apresentar o Teorema 2.3, sua aplicação no Exemplo 2.10 e o Corolário 2.1.

- Neste momento, o professor apresentará a Lei da Reciprocidade Quadrática e o Exemplo 2.12. Ele pode chamar a atenção dos alunos para o fato deste teorema ser muito útil quando relacionamos números relativamente grandes. Em seguida, os alunos podem aplicar este resultado no problema 5.

3º e 4º Aulas: Problemas de Olimpíadas Internacionais de Matemática

Neste momento, o professor pode falar sobre as olimpíadas de matemática e a presença da Teoria dos Números nesse tipo de competição, em especial, a aplicação da Teoria de Resíduos Quadráticos. Diante disso, o professor pode apresentar alguns dos problemas presentes no capítulo 3 deste trabalho.

A sugestão é de apresentar 1 problema em cada aula. Levando em consideração a aplicação dos resultados estudados e o nível de dificuldade dos problemas, sugerimos:

- 3º aula: IMO-1996.

- 4º aula: AwesomeMath.

Antes de apresentar os problemas, sugerimos que o professor fale um pouco sobre a IMO e o portal AwesomeMath (neste caso).

ANEXO A- Coletânea de Provas da Lei da Reciprocidade Quadrática

Segue abaixo uma lista com 314 demonstrações da Lei da Reciprocidade Quadrática, feita com base na referência [18] . Esta lista está organizada em ordem cronológica, na qual especificamos o autor e o método utilizado.

Tabela 1: Lista de provas da Lei da Reciprocidade Quadrática.

Posição	Prova	Ano	Método
1	Legendre	1788	Formas quadráticas; incompleto
2	Gauss 1	1801	Indução; 8 de abril de 1876
3	Gauss 2	1801	Formas Quadráticas; 27 de junho de 1796
4	Gauss 3	1808	Lema de Gauss; 6 de maio de 1807
5	Gauss 4	1811	Cicolotomia; maio de 1801
6	Gauss 5	1818	Lema de Gauss; 08/1807
7	Gauss 6	1818	Soma de Gauss; 08/1807
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
16	Eisenstein 2	1844	Gauss 6
17	Eisenstein 3	1844	Lema de Gauss
18	Eisenstein 4	1845	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	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	1869	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
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
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
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	Gauss 1; incorreta
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
135	Mirimanoff e Hensel	1905	Stickelberger-Voronoiertens
136	Cornacchia	1909	Períodos Quadráticos
137	Busche 5	1909	Zeller
138	Busche 6	1909	Eisenstein
139	Busche 7	1909	Eisenstein
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	Zeller

147	Dedekind 5	1912	Zeller
148	Dedekind 6	1912	Zeller
149	Dedekind	1912	Zeller
150	Heawood	1913	Eisenstein 3
151	McDonnell	1913	Ciclotomia
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 Gaus
165	Rédei 2	1926	Lema de Gaus
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 (sinais)
170	van Veen	1934	Eisenstein 3
171	Fueter	1935	Álgebra dos 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	Soma 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	Soma 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
202	Kubota 2	1961	Soma 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	Soma de Gauss
208	Swan 1	1962	Stickelberger-Voronoi
209	Koschmieder	1963	Eisenstein, seno
210	Gerstenhaber	1963	Eisenstein, seno
211	Rademacher	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 2	1969	Congruências Quadráticas
218	Kubota 4	1970	Funções teta
219	Birch	1971	K-teoria (Tate; Gauss 1)
220	Reshetukha	1971	Soma de Gauss
221	Agou	1972	Corpos Finitos
222	Brenner	1973	Zolotarev
223	Honda	1973	Soma de Gauss
224	Milnor e Husemöller	1973	Weil 1964

225	Zagier	1973	Somas de Dedekind
226	Allander	1974	Lema de Gauss
227	Berndt e Evans	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	Soma de Gauss
233	Burde	1977	Ciclotomia
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	Soma 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

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 de Dedekind
271	Motose 2	1999	Álgebras de Grupos
272	Zahidi	1999	Stickelberger-Voronoi
273	Lemmermeyer	2000	Lebesgue 1, Ely
274	Meyer	2000	Somas de 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
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 de Pell
308	Karlsson	2012	Somas 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	Períodoso Quadráticos
314	Brunyate e Clark	2014	Zolotarev

Referências Bibliográficas

[1] HEFEZ, Abramo. Aritmética. Rio de Janeiro: SBM, 2016.

[2] NIVEN, Ivan; ZUCKERMAN, Herbert S; MONTGOMERY, Hugh L. An Introduction to the Theory of Numbers. EUA: 5ª edição, 1991.

[3] FEITOSA, Samuel. Resíduos Quadráticos. Curso de Teoria dos Números-Nível 2. Disponível em: *https : //poti.impa.br/uploads/material*$_t$*eorico/*82*phy*0*g*0*my*8*sg.pdf*. Acesso em: 09 jul. 2020.

[4] MAIER, Rudolf R. Teoria dos números (Notas de aula). Brasília: Universidade de Brasília, 2005.

[5] ISNERI, Renan Jackson Soares. Resíduos Quadráticos. Campina Grande: Universidade Estadual da Paraíba, 2017.

[6] MARTINEZ, Fabio E. Brochero; MOREIRA, Carlos Gustavo T. de A.; SALDANHA, Nicolau C.; TENGAN, Eduardo. Introdução à Teoria dos Números: Funções Aritméticas, 2011.

[7] SANTOS, Djair Paulino dos; JÚNIOR, Fernando Vieira Costa; SILVA, Lindinês Coleta da; OLIVEIRA, Ornan Felipe de Araújo. Teoria dos Números e a Lei de Reciprocidade Quadrática. SBM, Rio de Janeiro-RJ, 2014.

[8] LINARES, Juán Lopez. Problemas Resolvidos sobre Sequências no Treinamento de Estudantes do Ensino Médio para Olimpíadas Internacionais de Matemática. São Carlos: Universidade Federal de São Carlos, 2019.

[9] ARAÚJO, Joselito Elias de. Divisibilidade, Congruência e Aritmética Modular em Problemas Olímpicos. Campina Grande: Universidade Federal de Campina Grande, 2018.

[10] BRASIL CONQUISTA SEIS MEDALHAS NA IMO 2019, NA INGLATERRA. IMPA, 2019. Diponível em: <https://impa.br/noticias/brasil-conquista-seis-medalhas-na-imo-2019-na-inglaterra/>. Acesso em: 09 jan. 2021.

[11] ANDRICA, Dorin; ANDREESCU, Titu. Number Theory. 2008.

[12] SUPPA, Ercole. Eötvös-Kürschák Competitions. Mathematical and Physical Society: 2007.

[13] TEODISTA, José Cláudio da Silva. Os teoremas de Fermat, Euler e Wilson. Campina Grande: Universidade Estadual da Paraíba, 2013.

[14] SECCO, Matheus. Resíduos Quadráticos. Olimpíada Brasileira de Matemática.

[15] WRIGHT, Steve. Quadratic Residues and Non-Residues, 2016.

[16] BAGATINI, Alessandro. Olimpíadas de Matemática, Altas Habilidades e Resolução de Problemas. Porto Alegre: Universidade Federal do Rio GRande do Sul, 2010.

[17] BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília, 2018.

[18] BAUMGART, Oswald. The Quadratic Reciprocity Law. Birkhäuser, Dordrecht Heidelberg Londres, New York, 2015.

[19] KIM, Sey Y. An Elementary Proof of the Quadratic Reciprocity Law Amer. Math. Monthly 111 (2004), no. 1, 48-50.

[20] SANTOS, José Plínio de Oliveira. Introdução à teoria dos Números. Rio de Janeiro: IMPA, 2007.

[21] MUNARO, Andrea; Srinath, R. Olympiad problems. AwesomeMath, 2009. Disponível em: https://www.awesomemath.org/what-is-awesomemath/. Acesso em: 10 out. 2020.