Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Congruências Quadráticas, Reciprocidade e Aplicações em Sala de Aula [†]

por

Leonardo Rodrigues de Araújo

sob orientação

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2013
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Congruências Quadráticas, Reciprocidade e Aplicações em Sala de Aula

por

Leonardo Rodrigues de Araújo

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática.

Aprovada por:

Prof. Dr. Bruno Henrique Carvalho Ribeiro – UFPB (Orientador)

Profa. Dra. Miriam da Silva Pereira – UFPB

Prof. Dr. José Anderson Valença Cardoso – UFS

Agosto/2013

Agradecimentos

- A Deus por proporcionar força, poder e proteção nos momentos mais desafiadores da vida.

- Ao Prof. Dr. Bruno Henrique Carvalho Ribeiro não somente pela orientação extremamente competente, mas, principalmente, pela prova inesquecível de dedicação, incentivo e de incansável disposição em todas as etapas deste trabalho.

- À Profa. Dra. Miriam da Silva Pereira e ao Prof. Dr. José Anderson Valença Cardoso pelas excepcionais contribuições para a evolução deste trabalho.

- Ao Prof. Dr. João Marcos Bezerra do Ó e à Profa. Me. Flávia Jerônimo Barbosa pelo pulso firme em iniciar a coordenação deste curso proporcionando o encorajamento necessário para vencer as dificuldades.

- À minha família, em particular aos meus pais José Marcelino de Araújo e Flávia Rodrigues de Meneses Araújo, o eterno reconhecimento pelo apoio, conselhos, incentivos e afetividade.

- À Eneida Rodrigues de Araújo Coêlho e a Breno Rodrigues de Araújo pelo estímulo.

- Ao Rvmo. Pe. Marisaldo Barbosa de Lima pelo incentivo e oração nos momentos de tribulação.

- A todos os colegas do curso de Mestrado, pela amizade e companheirismo particularmente aos amigos e companheiros: Alex Cristophe Cruz da Silva, Gildeci José Justino, Márcio Alves Marinho e Salatiel Dias da Silva.

- Aos professores da Pós−Graduação, pelos conhecimentos matemáticos construídos durante o curso.

- À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro.

Dedicatória

A Deus, fonte de inesgotável inspiração.

A minha família, em especial a meus pais José Marcelino de Araújo e Flávia Rodrigues de Meneses Araújo.

Ao Prof. Dr. Bruno Henrique Carvalho Ribeiro.

Resumo

Neste estudo, vamos avaliar se a congruência $x^2 \equiv a \ (mod \ m)$, onde m é primo e $(a, m) = 1$, apresenta ou não solução, destacando a importância dos Resíduos Quadráticos e, consequentemente da cooperação do Símbolo de Legendre, do Critério de Euler e do Lema de Gauss. Também, demonstraremos a Lei de Reciprocidade Quadrática generalizando situações para números compostos, ou seja, o Símbolo de Jacobi e suas propriedades. Apresentamos algumas propostas de atividades para o Ensino Médio envolvendo o assunto abordado e suas possíveis aplicações, através de uma linguagem compreensível aos alunos deste nível de ensino.

Palavras−Chaves: Congruência − Resíduos Quadráticos − Lei de Reciprocidade Quadrática.

Abstract

In this study, we evaluate if the congruence $x^2 \equiv a \ (mod \ m)$, where m is prime and $(a, m) = 1$, has or not solutions, highlighting the importance of Quadratic Residues and consequently the cooperation of the Legendre's Symbol, the Euler's Criterion and the Gauss' Lemma. Also, we demonstrate the Law of Quadratic Reciprocity generalizing situations for composite numbers, that is, the Jacobi's Symbol and its properties. We present some proposals of activities for the High School involving the subject matter and its possible applications, through an understandable language for students of this level.

Keywords: Congruence − Quadratic Residues − Law of Quadratic Reciprocity.

Sumário

Notações

$\equiv$ Congruente

$\not\equiv$ Incongruente

$|$ Divide

$\nmid$ Não Divide

(a, p) Máximo Divisor Comum de a e p

$\#$ Cardinalidade

$\mathbb{Z}$ Conjunto dos Números Inteiros

$\mathbb{Z}_p$ Anel dos inteiros módulo p

$\left(\frac{a}{p}\right)$ Símbolo de Legendre para Reciprocidade Quadrática

$\lfloor a \rfloor$ Menor inteiro menor do que ou igual a a

$\left[\frac{a}{n}\right]$ Símbolo de Jacobi

Introdução

A Matemática é a rainha das Ciências, e a Teoria dos Números é a rainha da Matemática. (Carl Friedrich Gauss)

Muitos matemáticos desempenharam um papel de destaque no desenvolvimento da Teoria dos Números sendo que Euclides (cerca de 300 a.C), em Elementos de Geometria, preservou o conhecimento matemático dos antigos gregos e Diofanto (cerca de 250 a.C), em Arithmetica, representou o primeiro tratado sobre álgebra. O que os tornam os fundadores da Teoria dos Números clássica.

Os Elementos de Euclides, especialmente nos livros VII, VIII e IX, apresentaram uma riqueza de informações sobre as propriedades fundamentais da divisibilidade e conceitos teóricos de papel central no estudo da Teoria dos Números, enquanto que Diofanto desenvolveu métodos para obter soluções racionais para equações polinomiais simples que podemos hoje denominar de equações diofantinas.

A Matemática na Europa teve uma renovação vigorosa após a Idade Média, onde a Teoria dos Números por representar uma área particular da Matemática de grande desenvolvimento apresenta matemáticos de destaque, como Pierre de Fermat, Leonhard Euler, Adrien−Marie Legendre e Carl Friedrich Gauss que através de suas contribuições significativas aprimoraram a Teoria dos Números.

Sendo p um primo maior que 2, veremos que alguns elementos do conjunto $\{0, 1, \ldots, p-1\}$ possuem uma característica especial que abordaremos neste trabalho. Tais elementos são denominados resíduos quadráticos sendo, portanto, uma forte ferramenta para o estudo da representação de inteiros. Mais especificamente, dizemos que a é um resíduo quadrático módulo p se $x^2 \equiv a \ (mod\ p)$ para algum $x \in \{0, 1, \ldots, p-1\}$.

Assim, a será um resíduo quadrático módulo p se a congruência tiver $x^2 \equiv a \ (mod\ p)$ solução, com $(a, p) = 1$. Veremos que no conjunto supracitado, é possível verificar que metade são considerados resíduos quadráticos, outra metade não. Estudaremos métodos como o Símbolo de Legendre, Critério de Euler e Lema de Gauss como forma de caracterizá−los e assim procurar soluções para as congruências quadráticas.

O primeiro matemático a estudar reciprocidade quadrática foi Fermat, que tinha a Matemática como uma atividade de lazer em uma época em que não existiam revistas matemáticas. Fermat tinha um costume curioso de apresentar resultados matemáticos em margens de livros que ele leu e em cartas de correspondências com outros matemáticos. Ainda assim, esta forma peculiar de estudar matemática muito contribuiu na direção da demonstração da reciprocidade quadrática.

A Lei de Reciporicidade Quadrática pode ser enunciada, em palavras, da seguinte forma: se p e q são dois números primos distintos, de modo que $p \equiv q \equiv 3 \ (mod\ 4)$, temos q como resíduo quadrático módulo p, se, e somente se, p é não resíduos quadrático módulo q, como também se p e q são dois números primos distintos, tais que $p \equiv 1 \ (mod\ 4)$, ou $q \equiv 1 \ (mod\ 4)$, então q é resíduo quadrático módulo p, se, e somente se, p é resíduo quadrático módulo q.

Fermat foi crucial na dedução do caráter quadrático de -1, ± 2, ± 3, mas foi Euler que prosseguiu com o trabalho de provar as conjecturas de Fermat. Podemos perceber em [9] que o autor considera Euler como um matemático de notável destaque no desenvolvimento histórico da Reciprocidade Quadrática por ser responsável em provar e contestar grande parte das conjecturas de Fermat.

Devido ao grande interesse na Teoria dos Números e por começar a desenvolver os trabalhos de Fermat, tendo contato com Christian Goldbach, Euler percebeu a relação entre a Lei de Reciprocidade Quadrática e os estudos dos diversos binários de certas formas quadráticas. Em [16], encontramos a afirmação de que a primeira prova de Euler sobre a Lei de Reciprocidade Quadrática é conhecida hoje como Critério de Euler.

Joseph Lagrange teve participação fundamental em inspirar Euler a continuar a trabalhar na Teoria dos Números e especialmente na tentativa em provar a Lei de Reciprocidade Quadrática completa que, com sua morte, Euler não pode encontrar nenhuma prova concreta. Além disso, o Critério de Euler foi bastante útil para Legendre e Gauss aprofundarem o problema dos resíduos quadráticos em contexto geral dando um enfoque mais rigoroso.

Legendre não ficou satisfeito em estudar apenas os resultados descobertos por Fermat e Euler e por isso escreveu, em 1798, seu primeiro trabalho denominado "Essal sur la Theorie des nombres" que se preocupou em interligar a Teoria dos Números desde a Arithmetica de Diofanto ao Quadratorum Liber de Fibonacci. Dessa maneira, inúmeros trabalhos sobre a Lei de Reciprocidade Quadrática permitiram ao mundo conhecer uma notação ainda usada atualmente para simbolizar convenientemente a Lei de Reciprocidade Quadrática de forma moderna, a saber, o símbolo de Legendre.

Legendre não conseguiu colocar suas provas em um contexto teórico consistente, mas desenvolveu um símbolo que levou a uma série de maneiras de provar a Reciprocidade Quadrática. Em [4], encontramos a indicação de que isto foi essencial

nos estudos de leis superiores de reciprocidade tendo o símbolo de Legendre como origem para o desenvolvimento de Jacobi e símbolos de Hilbert.

Em 1801, Gauss, "o príncipe da Matemática", publicou seu trabalho inovador "Disquisitiones Arithmeticae" introduzindo de forma clara e concisa a notação moderna de congruência $a \equiv b \ (mod \ n)$ sendo a e b múltiplo de n e n chamado módulo de congruência. Nesta obra, Gauss trás uma demonstração do Teorema Fundamental da Aritmética e apresenta uma revisão de tudo que se conhecia em Teoria dos Números até aquele momento.

Na seção IV desta obra, Gauss contempla a primeira prova completa de reciprocidade quadrática, tesouro da Matemática do século XVIII e XIX, por meio de indução cuja prova seguiu o raciocínio da prova de Legendre sendo descoberta independentemente do trabalho de Legendre. Com isso, comprova−se que Euler descobriu a Lei de Reciprocidade Quadrática cabendo a Legendre continuar a tentar prová−la, mérito este atribuído a Gauss mesmo sendo uma primeira prova longa e deselegante. Tal teorema recebeu posteriormente a denominação de Theorema Aureum ("teorema de ouro").

Gauss definitivamente provou a Lei de Reciprocidade Quadrática, em 18 de Abril de 1796, no entanto só conseguiu publicá-la em 1801, através de sua obra "Disquisitiones Arithmeticae" e por se sentir atraído pela beleza do "Teorema de Ouro" ele encontrou oito demonstrações, sendo a quinta demonstração considerada pelos matemáticos como a mais elegante e direta.

Já na seção V de sua obra, Gauss destaca a teoria de formas quadráticas binárias que segundo [2] trata−se de polinômios homogêneos de grau dois em duas variáveis, sendo que esta seção representa mais da metade do livro tornando−se uma prova da Lei de Reciprocidade Quadrática.

Em [14], Mota afirma a existência de 2071 provas da Lei de Reciprocidade Quadrática das quais apresentaremos, no final deste trabalho, uma listagem com 221 demonstrações contento os autores e os métodos. Contudo, é conveniente ressaltar que a prova considerada mais elementar é dada por Eisenstein, por meio de argumentos geométricos.

Com a demonstração da Lei de Reciprocidade Quadrática, Gauss alcançou importantes conquistas que expandiram os horizontes da Teoria dos Números principalmente quando apresentou a primeira prova. Ele considerou que, a partir dessa lei, haveria reciprocidades com graus superiores. Mesmo sendo provada há mais de 200 anos ainda desperta grande interesse dos matemáticos. Em [4], estuda-se a utilização em criptografia e no algoritmo de fatoração de inteiros que fazem uso da lei da reciprocidade quadrática, além de os resíduos quadráticos serem bastante utilizados em acústica.

Estruturamos este trabalho em partes. A primeira consta−se desta introdução. Em seguida, a segunda parte compreende as congruências quadráticas estendendo−se

aos Resíduos Quadráticos, Símbolo de Legendre, Critério de Euler, Lema de Gauss para que possamos determinar as soluções destas congruências como também reunir subsídios para as demonstrações da Lei de Reciprocidade Quadrática e assim analisar o Símbolo de Jacobi e suas propriedades para números compostos. Logo depois, apresentamos atividades propostas para aperfeiçoar o conhecimento matemático dos alunos, na quarta parte, e finalmente na parte pós-texto, apresentamos os apêndices e as referências.

Capítulo 1

Congruências Quadráticas

Neste capítulo, vamos examinar se um inteiro é ou não um resíduo quadrático módulo p primo a partir das congruências quadráticas $x^2 \equiv a \ (mod \ p)$. Além disso, exploraremos procedimentos eficazes para alcançar esta finalidade, tais como o Critério de Euler, o Símbolo de Legendre com suas propriedades e o Lema de Gauss. As demonstrações foram inspiradas em [7],[11],[18],[19],[21],[23],[24] e [27].

1.1 Resíduos Quadráticos

Consideremos a equação

$$ax^2 + bx + c \equiv 0 \ (mod \ p) \tag{1.1}$$

de modo que $a, b, c \in \mathbb{Z}$, p é um primo ímpar e $a \not\equiv 0 \ (mod \ p)$. Podemos observar que $(a, p) = 1$ e como p é ímpar teremos $(4a, p) = 1$. Assim, (1.1) será equivalente a $4a(ax^2 + bx + c) \equiv 0 \ (mod \ p)$ que ao completarmos quadrados obtemos $(2ax + b)^2 - (b^2 - 4ac) \equiv 0 \ (mod \ p)$, e consequentemente ao fazermos $y = 2ax + b$ e $d = b^2 - 4ac$, teremos

$$y^2 \equiv d \ (mod \ p). \tag{1.2}$$

Com isso, para encontrarmos solução para (1.1) é suficiente descobrir a solução de equações na forma

$$x^2 \equiv a \ (mod\ p) \tag{1.3}$$

pelo fato de se $p \mid a$ obtemos a desinteressante equação $x^2 \equiv 0 \ (mod\ p)$, e por essa razão $x \equiv 0 \ (mod\ p)$ o que torna indispensável assumir que $p \nmid a$ para evitarmos soluções triviais.

Exemplo 1.1 *Resolva a congruência* $8x^2 + 5x + 1 \equiv 0 \ (mod\ 23)$.

Solução: Como $(8, 23) = 1$ e $p = 23$ é primo ímpar temos que $(4 \cdot 8, 23) = (32, 23) = 1$, no qual ao multiplicarmos a congruência em questão e completar quadrados obtemos $(16x + 5)^2 + 32 - 25 \equiv 0 \ (mod\ 23) \Rightarrow (16x + 5)^2 \equiv 16 \ (mod\ 23)$. Com isso, encontramos $16x + 5 \equiv \pm 4 \ (mod\ 23)$ onde ao resolvermos a congruência linear $16x \equiv -1 \ (mod\ 23)$ temos $x \equiv 10 \ (mod\ 23)$, enquanto que a partir da congruência linear $x \equiv -9 \ (mod\ 23)$ obteremos $x \equiv 21 \ (mod\ 23)$. Dessa maneira, 10 e 21 são as únicas soluções incongruentes de $8x^2 + 5x + 1 \equiv 0 \ (mod\ 23)$.

Então, caso a congruência (1.3) apresente solução terá exatamente duas soluções incongruentes. Isso é exatamente o que vamos provar no teorema seguinte.

Teorema 1.1 *Para p um primo ímpar e a um inteiro não divisível por p, a congruência (1.3), caso tenha solução, tem exatamente duas soluções incongruentes modulo p.*

Demonstração: Consideremos que a congruência (1.3) tenha x_1 como solução, então podemos escrever que $-x_1$ também será solução, pelo fato de

$$(-x_1)^2 = x_1^2 \equiv 0 \ (mod\ p).$$

Agora, mostremos que estas soluções x_1 e $-x_1$ são incongruentes módulo p. Supondo que $x_1 \equiv -x_1 \ (mod\ p)$ obtemos $2x_1 \equiv 0 \ (mod\ p)$. Uma vez que, por hipótese, p é primo e p não divide x_1 temos que $2x_1 \equiv 0 \ (mod\ p)$ é impossível, e x_1 é incongruente a $-x_1$ módulo p, sendo necessário mostrarmos que apenas existem duas soluções incongruentes. Suponha agora que y é uma solução de $x^2 \equiv a \ (mod\ p)$. Daí, temos $y^2 \equiv a \ (mod\ p)$ e como x_1 é solução podemos escrever $x_1^2 \equiv a \ (mod\ p)$. Como $x_1^2 \equiv y^2 \equiv a \ (mod\ p)$, obteremos $x_1^2 - y^2 = (x_1 + y)\ (x_1 - y) \equiv 0 \ (mod\ p)$ que

resultará em $p \mid (x_1 + y)$ ou $p \mid (x_1 - y)$, o que implicará em $y \equiv -x_1 \ (mod\ p)$ ou $y \equiv x_1 \ (mod\ p)$ e, por consequência, caso exista uma solução, existem exatamente duas soluções incongruentes módulo p, e as demais soluções serão congruentes a uma dessas duas. □

Exemplo 1.2 *Determine todas as soluções da congruência* $x^2 \equiv 1 \ (mod\ 3)$.

Solução: Como 3 é um primo ímpar e 1 não é divisível por 3 poderá existir, pelo Teorema 1.1, apenas duas soluções incongruentes módulo 3. Assim, observemos que $x_1 = 2$ satisfaz a congruência e $-x_1 = -2$ também satisfaz essa congruência. Portanto, $x_1 = 2$ não é congruente a $-x_1 = -2$ módulo 3 o que implicará em as outras soluções são congruentes à $x_1 = 2$ ou à $x_1 = -2$ módulo 3, por existir apenas duas soluções incongruentes módulo 3 para a congruência em questão. Com isso, fazendo s uma solução diferente de x_1 e $-x_1$ obtemos $s \equiv 2 \ (mod\ 3)$ ou $s \equiv -2 \ (mod\ 3)$. Enfim, todas as soluções serão dadas por $s = 3k + 2$ ou $s = 3k - 2$, para $k \in \mathbb{Z}$.

Definição 1.1 *O conjunto dos inteiros* $\{r_1, r_2, r_3, \ldots, r_v\}$ *é um sistema completo de resíduos modulo p se:*

(i) r_t *não for congruente a* r_u *módulo p para* $t \neq u$;

(ii) para todo inteiro k, existe um r_t, *tal que* $k \equiv r_t \ (mod\ p)$.

Definição 1.2 *Sejam a e m inteiros com* $(a, m) = 1$. *Dizemos que a é um resíduo quadrático módulo m se a congruência* $x^2 \equiv a \ (mod\ m)$ *tiver solução. Caso* $x^2 \equiv a \ (mod\ m)$ *não tenha solução, dizemos que a não é um resíduo quadrático módulo m ou que a é um resíduo não−quadrático.*

Como $4^2 \equiv 6 \ (mod\ 10)$, então 6 é resíduo quadrado quadrático módulo 10, assim como $12^2 \equiv 1 \ (mod\ 13)$ e assim 1 é resíduo quadrático módulo 13. Agora, consideremos o primo 17 vamos obter os números que são resíduos quadráticos módulo 17. Para tanto, é suficiente considerar os quadrados dos números $1, 2, 3, 4, \ldots, 16$ pelo fato destes números formarem um sistema reduzido de resíduos módulo 17. Portanto,

$1^2 \equiv 1\ (mod\ 17)$ $\quad$ $9^2 \equiv 13\ (mod\ 17)$
$2^2 \equiv 4\ (mod\ 17)$ $\quad$ $10^2 \equiv 15\ (mod\ 17)$
$3^2 \equiv 9\ (mod\ 17)$ $\quad$ $11^2 \equiv 2\ (mod\ 17)$
$4^2 \equiv 16\ (mod\ 17)$ $\quad$ $12^2 \equiv 8\ (mod\ 17)$
$5^2 \equiv 8\ (mod\ 17)$ $\quad$ $13^2 \equiv 16\ (mod\ 17)$
$6^2 \equiv 2\ (mod\ 17)$ $\quad$ $14^2 \equiv 9\ (mod\ 17)$
$7^2 \equiv 15\ (mod\ 17)$ $\quad$ $15^2 \equiv 4\ (mod\ 17)$
$8^2 \equiv 13\ (mod\ 17)$ $\quad$ $16^2 \equiv 1\ (mod\ 17)$

Podemos observar que na coluna da esquerda das congruências acima temos os quadrados dos números 1 até 16 e na coluna da direita apenas 8 números $1, 2, 4, 8, 9$, 13,15 e 16. Portanto, estes números são todos os resíduos quadráticos módulo 17. Também, é possível notar que estes números aparecem na metade superior da tabela acima e que eles se repetem na metade inferior, cuja repetição ocorre a partir de 9^2. Tal curiosidade é proveniente da congruência $(17-k)^2 \equiv k^2\ (mod\ 17)$ de verificação imediata. Logo, ao termos um número primo ímpar qualquer podemos imaginar que, dentre os elementos, 1, 2, 3,..., $p-1$, que formam um sistema reduzido de resíduos módulos p, metade, ou seja,$\dfrac{(p-1)}{2}$ são resíduos quadráticos e $\dfrac{(p-1)}{2}$ restantes não são. Isso é exatamente o que iremos demonstrar em seguida.

Teorema 1.2 *Seja p um primo ímpar. No conjunto $\{1, 2, ..., p-1\}$, $\dfrac{p-1}{2}$ são resíduos quadráticos enquanto que $\dfrac{p-1}{2}$ não são.*

Demonstração: Consideremos a congruência $x^2 \equiv a_i\ (mod\, p)$, para $i = 1, 2, 3, ...,$ $p-1$ com p primo onde desejamos obter todos os $a_i's$ que são resíduos quadráticos módulo p. Então, vamos considerar os quadrados dos números de 1 a $p-1$ que ao escrevermos $1^2 \equiv 1\ (mod\ p)$ temos $a_1 = 1$ como resíduo quadrático módulo p, mas também -1 é solução pelo fato de $(-1) \equiv p-1\ (mod\ p)$. Agora, pelo Teorema 1.1, temos que 1 e $p-1$ são as únicas soluções incongruentes módulo p, e sendo os números $1, 2, 3, \ldots, p-1$ todos incongruentes módulo p, por formar um sistema reduzido de resíduos módulo p, tem−se que 1 e $p-1$ são as únicas soluções da congruência $x^2 \equiv 1\ (mod\ p)$ dentre os números $1, 2, 3, \ldots, p-1$.

Ao tomarmos 2^2, este será congruente a algum número r diferente de 1 e obvi-

amente $(-2)^2$ também será congruente a esse número r. Uma vez que $-2 \equiv p-2$ $(mod\ p)$, pelo teorema 1.1, verificamos que 2 e $p-2$ são as únicas soluções incongruentes de $x^2 \equiv r \pmod{p}$ dentre os números 1, 2, 3,..., $p-1$. Agora, ao tomarmos 3^2 que será congruente a algum número s diferente de 1 e de r percebe−se que $(-3)^2$ também será congruente a esse número s e como $-3 \equiv p-3$ $(mod\ p)$, pelo Teorema 1.1, tem−se que 3 e $p-3$ são as únicas soluções incongruentes de $x^2 \equiv s$ $(mod\ p)$ dentre os números $1, 2, 3, \ldots, p-1$ e assim observemos que temos 1,r e s como resíduos quadráticos das respectivas congruências:

(1) $x^2 \equiv 1$ $(mod\ p)$, que tem soluções (1, $p-1$);
(2) $x^2 \equiv r$ $(mod\ p)$, que tem soluções (2, $p-2$);
(3) $x^2 \equiv s$ $(mod\ p)$, que tem soluções (3, $p-3$).

Ao prosseguir desta maneira teremos $\frac{p-1}{2}$ pares de soluções

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

em que cada par é solução para uma dentre as $\frac{p-1}{2}$ congruências $x^2 \equiv a_i\ (mod\ p)$,

relacionadas exatamente a $\frac{p-1}{2}$ dos números 1, 2, 3,..., $p-1$ e, portanto os $\frac{p-1}{2}$ números $a'_i s$ são os $\frac{p-1}{2}$ resíduos quadráticos e os restantes $\frac{p-1}{2}$ não são resíduos quadráticos. □

Exemplo 1.3 *Sendo o primo 7, encontre, dentre os números {1,2,3,4,5,6}, os três números que são resíduos quadráticos e os outros três que não são resíduos quadráticos.*

Solução:

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

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

Assim, os números que são resíduos quadráticos são 1,4 e 2, enquanto os números que não que são resíduos quadráticos são 3,5 e 6.

Teorema 1.3 *A congruência $x^2 \equiv -1 \ (mod\ p)$, para p primo, tem solução se, e somente se, $p = 2$ ou $p \equiv 1 \ (mod\ 4)$.*

Demonstração: ($\Rightarrow$) Sendo $p = 2$, pode−se verificar que $x = 1$ é uma solução, pois $1^2 \equiv -1 \ (mod\ p)$. Assim, é necessário supor agora que a congruência $x^2 \equiv -1$ $(mod\ p)$ apresenta solução e que $p > 2$. Elevando ambos os membros a potência $\frac{(p-1)}{2}$ tem−se:

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

e como $x^{2\frac{(p-1)}{2}} \equiv x^{(p-1)} \ (mod\ p)$ podemos escrever, pelo Pequeno Teorema de Fermat, (Anexo B), que

$$x^{p-1} \equiv 1 \ (\text{mod}\ p) \Rightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$$

resultando no fato de $\frac{(p-1)}{2}$ ser par temos:

$$\frac{(p-1)}{2} = 2k \Rightarrow p - 1 = 4k \Rightarrow p = 4k + 1, \ \ k \in \mathbb{Z} \text{ e, então } p \equiv 1 \ (mod\ 4).$$

($\Leftarrow$) Agora, é preciso encontrar uma solução para a congruência $x^2 \equiv -1 \ (mod\ p)$ no momento em que $p \equiv 1 \ (mod\ 4)$, onde p é um número primo ímpar que, através do Teorema de Wilson, (Anexo B), podemos organizá−los como sendo

$$(\ 1 \cdot 2 \cdot 3 \cdots j \cdots \frac{p-1}{2}) \ (\frac{p+1}{2} \cdots (p-j) \ \cdots (p-2)(p-1)) \equiv -1 \ (mod\ p).$$

O produto $(p-1)!$ está dividido em duas partes, cada uma com a mesma quantidade de fatores, ou seja, cada uma tem $\frac{(p-1)}{2}$ fatores que ao reescrever este produto formando pares, cada fator j na primeira parte equivalerá ao fator $(p-j)$ na segunda parte podendo, pelo Teorema de Wilson, (Anexo B), ser escrito como:

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1 \ (mod\, p).$$

Como $j(p-j) \equiv -j^2 \ (mod\ p)$, pois $jp - j^2 \equiv -\ j^2 \ (mod\ p)$ obtemos:

$$-1 \equiv \prod_{j=1}^{(p-1)/2} -j^2 \equiv (-1)^{(p-1)/2} \left(\prod_{j=1}^{(p-1)/2} j \right)^2 (mod\, p).$$

Mas, sendo $p \equiv 1 \ (mod\ 4)$, então p é da forma $4k+1$, com $k \in \mathbb{Z}$, e como $\dfrac{(p-1)}{2}$ é par teremos

$$x = \prod_{j=1}^{(p-1)/2} j = \left(\frac{p-1}{2} \right)!,$$

que é uma solução de $x^2 \equiv -1 \ (mod\ p)$.

□

1.2 Símbolo de Legendre e o Critério de Euler

Adrien−Marie Legendre (1752−1833) desenvolveu um símbolo para verificar se uma congruência do tipo $x^2 \equiv a \ (mod\, p)$, com p primo possui solução simplificando os cálculos e sendo uma possibilidade de os termos resíduos quadráticos e não-resíduos possam ser denotados de modo muito conveniente, bem como útil.

Definição 1.3 *Seja p um inteiro primo ímpar. Para um inteiro a defini−se o Símbolo de Legendre de a módulo p e denotamos por $\left(\dfrac{a}{p} \right)$ como sendo*

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

É possível observar que na definição acima considera−se p ímpar uma vez que qualquer número inteiro é um quadrado módulo 2. O próximo resultado, descoberto por Euler possibilita o cálculo do Símbolo de Legendre.

Teorema 1.4 *(Critério de Euler) Seja $p > 2$ um primo e a um inteiro. Então*

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

Demonstração: Para $a \equiv 0\ (mod\ p)$ o resultado é evidente, de modo que devemos supor $p \nmid a$. Com isso, ao considerarmos primeiramente que $a = 1$ verifica−se que a congruência $x^2 \equiv a\ (mod\ p)$ apresenta solução, pelo Teorema 1.1, e consequentemente teremos $y^2 \equiv a\ (mod\ p)$ para algum $y \in \mathbb{Z}$ resultando em p divide $(y^2 - a)$. Mas, p não divide a, p não divide y^2 e portanto, p não divide y. Concluímos assim que $(y, p) = 1$ e assim, pelo Pequeno Teorema de Fermat, (Anexo B), $y^{p-1} \equiv 1\ (mod\ p)$, podemos escrever que

$$\begin{aligned} y^2 \equiv a\ (mod\ p) \Rightarrow (y^2)^{\frac{(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}}\ (mod\ p) \Rightarrow a^{\frac{(p-1)}{2}} \equiv y^{p-1}\ (mod\ p) \\ \Rightarrow a^{\frac{(p-1)}{2}} \equiv 1\ (mod\ p) \end{aligned}$$

o que comprova o teorema para o caso em que $\left(\frac{a}{p}\right) = 1$.

Agora, mostremos para o caso em que $\left(\frac{a}{p}\right) = -1$, ou seja, a não é um resíduo quadrático de p e se s é um dos inteiros de $\{1,2,3,\cdots,p-1\}$ podemos admitir que, pela Teoria das Congruências Lineares, existe uma solução s' de $sx \equiv a\ (mod\ p)$, com s' também no conjunto $\{1,2,3,\cdots,p-1\}$. Mas, s e s' devem ser distintos para evitarmos que $s^2 \equiv a\ (mod\ p)$, já que $\left(\frac{a}{p}\right) = -1$. Então, os inteiros entre a e $p-1$

podem ser divididos em $\frac{(p-1)}{2}$ pares, s e s', onde $ss' \equiv a \ (mod\ p)$ nos levará às congruências

$$s_1 s'_1 \equiv a \ (mod\ p)$$

$$s_2 s'_2 \equiv a \ (mod\ p)$$

$$\vdots \quad \vdots$$

$$s_{\frac{(p-1)}{2}} s'_{\frac{(p-1)}{2}} \equiv \ a \ (mod\ p).$$

Ao multiplicarmos as congruências acima obtemos

$$s_1 \cdot s'_2 \cdot s_2 \cdot s'_2 \cdot \ldots \cdot s_{\frac{(p-1)}{2}} \cdot s'_{\frac{(p-1)}{2}} \equiv \ a^{\frac{(p-1)}{2}} \ (mod\ p)$$

que representa um rearranjo de $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ resultando em $(p-1)! \equiv a^{\frac{(p-1)}{2}} \ (mod\ p)$ e, teremos, pelo Teorema de Wilson, (Anexo B), $a^{\frac{(p-1)}{2}} \equiv -1 \ (mod\ p)$ se referindo ao Critério de Euler quando a não é um resíduo quadrático, ou seja, $\left(\frac{a}{p}\right) = -1$.

□

Exemplo 1.4 *Verificar que $a = 3$ é um resíduo não quadrático módulo 7, mas é resíduo quadrático módulo 11.*

Solução: Pelo Critério de Euler é possível escrever que

$$\left(\frac{3}{7}\right) = 3^{\frac{(7-1)}{2}} \equiv -1 \ (mod\ 7);$$

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

Vamos introduzir algumas propriedades que permitem o cálculo do Símbolo de Legendre.

Teorema 1.5 *Seja p primo ímpar e $a, b, c \in \mathbb{Z}$. Então, pelo Critério de Euler e pela definição do Símbolo de Legendre, seguem as seguintes propriedades:*

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

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

3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *se* $p \nmid a$ *e* $p \nmid b$.

4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4 \\ -1 & \text{se } p \equiv 3 \pmod 4 \end{cases}$

Demonstração: Para a propriedade 1 é suficiente observar que

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

enquanto na propriedade 2 é evidente que a é resíduo quadrático de p pelo fato de, pelo Pequeno Teorema de Fermat, (Anexo B), $(a^2)^{\frac{(p-1)}{2}} \equiv a^{(p-1)} \equiv 1 \ (mod\ p)$. Já as propriedades 3 e 4 são consequências imediatas do Critério de Euler, pois

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

Mas como

$$(ab)^{\frac{(p-1)}{2}} = \mathrm{a}^{\frac{(p-1)}{2}} b^{\frac{(p-1)}{2}}$$

podemos escrever que

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

concluindo que

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

Já a propriedade 4 possibilita investigar todos os primos para os quais -1 são resíduos quadráticos, onde $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{(p-1)}{2}} \ (mod\, p)$ significando que $\left(\frac{-1}{p}\right)$ seria

igual a 1 quando $\frac{(p-1)}{2}$ for par e igual a -1, quando $\frac{(p-1)}{2}$ for ímpar. Então, se p é um primo ímpar, existem apenas duas possibilidades para p em termos de congruência módulo 4 ou $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$ e se $p \equiv 1 \pmod 4$ teremos $p-1$ divisível por 4 e $\frac{(p-1)}{2}$ será par. Agora, se $p \equiv 3 \pmod 4$, existe k tal que $p-3 = p-1-2 = 4k$ e, desse modo $p-1 = 4k+2 = 2(2k+1)$ implicando em $\frac{(p-1)}{2}$ ímpar. Então, para $p \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = 1$ e, para $p \equiv 3 \pmod 4$, $\left(\frac{-1}{p}\right) = -1$.

□

Assim, através da propriedade 3 do Teorema 1.5, [21] revela que o produto de dois resíduos quadráticos é um resíduo quadrático, que o produto de dois números que não são resíduos quadráticos é um resíduo quadrático e que o produto de um que não é resíduo quadrático por um que é resíduo quadrático não é resíduo quadrático.

1.3 Lema de Gauss

Nessa seção, analisaremos o resultado a seguir, conhecido como Lema de Gauss, que segundo [7], trata−se de um método capaz de determinar $\left(\frac{a}{p}\right)$ para todo primo ímpar p e todo número natural a, tal que $(a,p) = 1$.

Lema 1.1 *(Lema de Gauss) Sejam p um primo ímpar e a um inteiro não−divisível por p. Então*

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

onde r é a quantidade de resíduos positivos módulo p dos números

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a, \tag{1.4}$$

que são maiores que $\frac{p}{2}$.

Demonstração: Inicialmente observe que não podemos ter $ab \equiv 0 \ (mod\ p)$ para

$b \in \{1, 2, \cdots, \frac{p-1}{2}\}$ pois, caso contrário, teríamos $p|ab$, o que é uma contradição por $b < p$ e $p \nmid a$. Com isso os elementos de (1.4) serão incongruentes dois a dois módulo p, pois se $ab \equiv ac \ (mod\ p)$, para $b, c \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ obtemos $p \mid (b-c)a$, mas se $p \nmid a$ temos $p \mid (b-c)$, ou seja, $b \equiv c \ (mod\ p)$ o que é impossível.

Agora, ao analisar a reordenação de (1.4) temos

$$r_1, r_2, \ldots, r_i, s_1, s_2, \ldots, s_j, \text{ com } i+j = \frac{(p-1)}{2}, \tag{1.5}$$

formada por resíduos positivos módulo p, em que os inteiros r_k são menores que $\frac{(p-1)}{2}$ e os inteiros s_t maiores que $\frac{(p-1)}{2}$.

Sendo

$$\{r_1, r_2, \ldots, r_i, p-s_1, p-s_2 \ldots, p-s_j\} \tag{1.6}$$

obtemos um conjunto de elementos positivos menores que p, e então quaisquer dois elementos de (1.6) são incongruentes módulo p. Por outro lado, quando $k \neq t$, temos $p - s_k \not\equiv p - s_t \ (mod\ p)$ e $r_k \not\equiv \mathrm{r}_t \ (mod\ p)$ pelo fato de os elementos de (1.4) serem incongruentes módulo p. Por outro lado, temos $p - s_k \not\equiv r_t \ (mod\ p)$. Caso contrário, $s_t + r_k \equiv 0 \ (mod\ p)$ e como cada elemento de (1.5) é congruente módulo p com algum elemento de (1.4), obtemos

$$s_t + r_k \equiv ab + ac \equiv (b+c)a \equiv 0 \ (mod\ p),\ b, c \leq \frac{(p-1)}{2}.$$

Por hipótese, $p \nmid a$ e então

$$p \mid (b+c) \leq \frac{(p-1)}{2} + \frac{(p-1)}{2} = p - 1.$$

Isto é impossível, pois os elementos de (1.6) são incongruentes módulo p dois a dois. Note−se que (1.6) tem $p-1$ elementos positivos e menores que p. Isto implica que os elementos de (1.6) são forçosamente os elementos $1, 2, \ldots, \frac{(p-1)}{2}$.

Multiplicando todos os elementos de (1.6) obtemos

$$\prod_{k=1}^{j}(p - s_k) \cdot \prod_{t=1}^{i} r_t \equiv \left(\frac{p-1}{2}\right)!(\mathrm{mod}\, p).$$

Como $p-s_k \equiv -s_k \ (mod\ p)$, vem que

$$(-1)^r \prod_{k=1}^{j}(s_k) \cdot \prod_{t=1}^{i} r_t \equiv \left(\frac{p-1}{2}\right)! \ (\mathrm{mod}\, p),$$

e como cada elemento de (1.5) é congruente módulo p com algum elemento de (1.4), a congruência anterior é equivalente a

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

Com isso, da congruência anterior resulta que $(-1)^r a^{\frac{(p-1)}{2}} \equiv 1 \ (mod\ p)$ e, como $\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \ (mod\ p)$, (Critério de Euler), conclui− se que $\left(\frac{a}{p}\right) = (-1)^r$.

□

Vamos agora ilustrar a demonstração do Lema de Gauss. Portanto, ao considerarmos o caso particular em que $a = 5$ e $p = 17$ teremos que calcular os menores resíduos positivos módulo 17 dos seguintes múltiplos de 5, uma vez que $8 = \frac{(17-1)}{2}$:

$1 \cdot 5$, $2 \cdot 5$, $3 \cdot 5$, $4 \cdot 5$, $5 \cdot 5$, $6 \cdot 5$, $7 \cdot 5$ e $8 \cdot 5$. Então,

$1 \cdot 5 \equiv 5 \ (mod\ 17)$
$2 \cdot 5 \equiv 10 \ (mod\ 17)$
$3 \cdot 5 \equiv 15 \ (mod\ 17)$
$4 \cdot 5 \equiv 3 \ (mod\ 17)$
$5 \cdot 5 \equiv 8 \ (mod\ 17)$
$6 \cdot 5 \equiv 13 \ (mod\ 17)$
$7 \cdot 5 \equiv 1 \ (mod\ 17)$
$8 \cdot 5 \equiv 6 \ (mod\ 17)$

Podemos verificar que dentre estes resíduos, que são 1,3,5,6,8,10,13 e 15, apenas cinco, 1,3,5,6 e 8, são menores do que $\frac{17}{2}$, e consequentemente ao tomarmos os que são maiores, ou seja,10,13 e 15 e ao considerarmos os números $17-10, 17-13$ e $17-15$, obtemos 7,4 e 2, respectivamente que associando com 1,3,5,6 e 8 constituem todos os números de 1 a 8.

Desse modo, na demonstração do Lema de Gauss deveremos fazer o que foi feito acima com p primo ímpar qualquer para provarmos que $(-1)^r = \left(\frac{a}{p}\right)$, onde r

representa o número de resíduos positivos de $1\cdot$ a, $2\cdot a, 3\cdot a, \cdots, \frac{(p-1)}{2}\cdot a$ que são maiores que p. Partindo de caso particular $r = 5$ tem−se

$$\left(\frac{5}{17}\right) = (-1)^5 = -1$$

o que está coerente com o Critério de Euler, uma vez que

$$\left(\frac{5}{17}\right) = 5^{\frac{(17-1)}{2}} \equiv 5^8 \equiv 5^2\cdot 5^2\cdot 5^2\cdot 5^2 \equiv 8\cdot 8\cdot 8\cdot 8 \equiv 16 \equiv -1 \ (mod\ 17).$$

1.4 O Símbolo de Legendre $\left(\frac{2}{p}\right)$

Nesta seção, vamos determinar uma fórmula válida para $\left(\frac{2}{p}\right)$.

Teorema 1.6 *Para p um primo ímpar, temos*

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

Demonstração: Usando o Critério de Euler, vamos verificar que $2^{\frac{(p-1)}{2}} \equiv 1$ $(mod\ p)$ se, e somente se, $p \equiv \pm 1$ $(mod\ 8)$. Assim, observemos que

$$2^{\frac{(p-1)}{2}}\left(\frac{p-1}{2}\right)! = 2^{\frac{(p-1)}{2}}\left(1\cdot 2\cdot 3\cdot \ldots \cdot \frac{p-1}{2}\right) = 2\cdot 4\cdot \ldots \cdot (p-1).$$

Agora, consideremos, pelo Critério de Euler, que $\left(\frac{2}{p}\right) = 2^{\frac{(p-1)}{2}}$ $(mod\ p)$ e, portanto

$*$ Se $\frac{(p-1)}{2}$ é par.

$$2^{\frac{(p-1)}{2}}\left(\frac{p-1}{2}\right)! = 2\cdot 4\cdot \ldots \cdot (p-1)$$

$$= \underbrace{(2 \cdot \ldots \cdot \frac{p-1}{2})}_{\frac{p-1}{4} fatores} \underbrace{(\frac{p+3}{2} \cdot \ldots \cdot (p-3) \cdot (p-1))}_{\frac{p-1}{4} fatores}$$

$$\equiv \left(2 \cdot \ldots \cdot (\frac{p-1}{2})\right) \cdot ((-\frac{p-3}{2}) \cdot \ldots \cdot (-3) \cdot (-1)) \ (mod\ p)$$

$$\equiv (2 \cdot \ldots \cdot \frac{p-1}{2}) \cdot (1 \cdot 3 \cdot \ldots \cdot \frac{p-3}{2})(-1)^{\frac{(p-1)}{4}} \ (mod\ p)$$

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

$*$ Se $\dfrac{(p-1)}{2}$ é ímpar.

$$2^{\frac{(p-1)}{2}} \left(\frac{p-1}{2}\right)! = 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)$$

$$= \underbrace{(2 \cdot \ldots \cdot \frac{p-3}{2})}_{\frac{p-3}{4} fatores} \underbrace{(\frac{p+1}{2} \cdot \ldots \cdot (p-3) \cdot (p-1))}_{\frac{p+1}{4} fatores}$$

$$\equiv (2 \cdot \ldots \cdot \frac{p-3}{2}) \cdot ((-\frac{p-1}{2}) \cdot \ldots \cdot (-3) \cdot (-1)) \ \ (mod\ p)$$

$$\equiv (2 \cdot \ldots \cdot \frac{p-3}{2}) \cdot (1 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2})(-1)^{\frac{(p-1)}{4}} \ (mod\ p)$$

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

Logo,

$$2^{\frac{(p-1)}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{(p-1)}{4}} \left(\frac{p-1}{2}\right)! \ (mod\ p) \text{ se } \frac{(p-1)}{2} \text{ é par}$$

$$2^{\frac{(p-1)}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{(p-1)}{4}} \left(\frac{p-1}{2}\right)! \ (mod\ p) \text{ se } \frac{(p-1)}{2} \text{ é ímpar.}$$

Ao cancelarmos $\left(\dfrac{p-1}{2}\right)!$ nas congruências acima, temos

$$2^{\frac{(p-1)}{2}} = \begin{cases} (-1)^{\frac{(p-1)}{4}} (mod\ p) & \text{se } \dfrac{(p-1)}{2} \text{ é par} \\ (-1)^{\frac{(p-1)}{4}} (mod\ p) & \text{se } \dfrac{(p-1)}{2} \text{é ímpar} \end{cases}$$

$$= (-1)^{\frac{(p-1)(p+1)}{8}} \ (mod\ p).$$

Ao analisarmos os diversos casos possíveis para p módulo 8, obtemos

$$\left(\frac{2}{p}\right) = 2^{\frac{(p-1)}{2}} = \begin{cases} p \equiv 1\ (mod\ 8) \Rightarrow 2^{\frac{(p-1)}{2}} = 1 \text{ porque } \dfrac{(p-1)}{2} \text{ e } \dfrac{(p-1)}{4} \text{ são pares} \\ p \equiv 3\ (\text{mod } 8) \Rightarrow 2^{\frac{(p-1)}{2}} = -1 \text{ porque } \dfrac{(p-1)}{2} \text{ e } \dfrac{(p+1)}{4} \text{ são ímpares} \\ p \equiv 5\ (\text{mod } 8) \Rightarrow 2^{\frac{(p-1)}{2}} = -1 \text{ porque} \dfrac{(p-1)}{2} \text{ é par e } \dfrac{(p-1)}{4} \text{ é ímpar} \\ p \equiv 7\ (\text{mod } 8) \Rightarrow 2^{\frac{(p-1)}{2}} = 1 \text{ porque } \dfrac{(p-1)}{2} \text{ é ímpar e } \dfrac{(p+1)}{4} \text{ é par.} \end{cases}$$

□

Com o auxílio do Teorema 1.5 pode−se verificar que se p é um número primo ímpar teremos que

$$\left(\frac{-2}{p}\right) = 1 \Leftrightarrow p \equiv 1\ (mod\ 8) \text{ ou } p \equiv 3\ (mod\ 8).$$

Capítulo 2

Lei de Reciprocidade Quadrática

Neste capítulo, iniciaremos uma investigação da Lei de Reciprocidade Quadrática, um dos primeiros resultados da Teoria dos Números Moderna, conjecturada por Euler e por Legendre, na primeira metade do século XVIII. No entanto, Gauss forneceu a primeira demonstração e, ao longo de sua vida, encontrou outras demonstrações. Também o estudo dessa lei foi construído por meio de várias demonstrações inspiradas em [6],[7],[8],[10],[11],[15],[18],[20],[21],[22] e [25], atribuindo um destaque ao estudo do Símbolo de Jacobi para inteiros módulo de um número composto e, em particular, a resolução de raízes quadradas módulo n.

2.1 Provas da Lei de Reciprocidade Quadrática

Teorema 2.1 *Se p e a são números ímpares diferentes, em que p é primo e não divide a, então,*

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

onde

$$M = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \cdots + \left\lfloor \frac{p'a}{p} \right\rfloor \text{ e } p' = \frac{(p-1)}{2}.$$

Demonstração: O Algoritmo da Divisão permite determinar os menores resíduos positivos de $a, 2a, 3a, \ldots, p'a$ por meio das seguintes divisões:

$$
\begin{aligned}
a &= p\left\lfloor \frac{a}{p} \right\rfloor + r_1 \\
2a &= p\left\lfloor \frac{2a}{p} \right\rfloor + r_2 \\
3a &= p\left\lfloor \frac{3a}{p} \right\rfloor + r_3 \\
&\vdots \\
p'a &= p\left\lfloor \frac{p'a}{p} \right\rfloor + r_{p'}
\end{aligned}
$$

em que $r_1, r_2, ..., r_{p'}$ são, respectivamente, os restos da divisão por p dos números $a, 2a, 3a,\ldots,p'a$. Ao somarmos, membro a membro, as p' igualdades acima obtemos

$$(1+2+3+...+p')a = p\left(\left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \cdots + \left\lfloor \frac{p'a}{p} \right\rfloor\right) + r_1 + r_2 + ... + r_{p'}$$

ou ainda, ao colocarmos pelo Lema de Gauss (Lema 1.1), $B = b_1 + b_2 + \ldots + b_h$ e $C = c_1 + c_2 + \ldots + c_k$, teremos $r_1 + r_2 + ... + r_{p'} = B + C$; e, então,

$$\frac{(p^2-1)}{8}a = pM + B + C. \tag{2.1}$$

Mas, como os números $b_1, b_2, \ldots, b_h, p - c_1, p - c_2, \ldots, p - c_k$ são, a menos da ordem, os números $1, 2, 3, \ldots, p'$ pode−se escrever que

$$1 + 2 + \ldots + p' = \frac{(p^2-1)}{8} = b_1 + b_2 + \ldots + b_h + rp - (c_1 + c_2 + \ldots + c_k)$$

e consequentemente

$$\frac{(p^2-1)}{8} = -B + rp + C. \tag{2.2}$$

Ao subtrairmos, membro a membro, as equações (2.1) e (2.2) obtemos para $M \geq r$

$$\frac{(p^2-1)}{8}(a-1) = p(M-r) + 2B \tag{2.3}$$

e, para $r > M$

$$\frac{(p^2-1)}{8}(a-1) = p(r-M) + 2B. \tag{2.4}$$

Dessa maneira, como a e p são ímpares, por hipótese, o termo $\frac{(p^2-1)}{8}(a-1)$ será par o que resultará em $p(M-r)$ também será par pelo fato desta diferença ser par por serem ambos pares ou ambos ímpares. Logo, o Lema de Gauss permite escrever que

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

já que M e r apresentam a mesma paridade.

□

O Teorema 2.1 nos permite fornecer uma demonstração alternativa do Teorema 1.6 apresentado no Capítulo anterior.

Demonstração: Fazendo uso das notações da demonstração do Teorema 2.1, tomamos $a = 2$, temos $M = \left\lfloor \frac{2}{p} \right\rfloor + \left\lfloor \frac{4}{p} \right\rfloor + \ldots + \left\lfloor \frac{p-1}{p} \right\rfloor = 0$.

Da equação (2.3), obtemos

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

Logo, r será par ou ímpar de acordo com $\frac{p^2-1}{8}$ é par ou ímpar, respectivamente e assim, pelo Lema de Gauss, $\left(\frac{2}{p}\right) = (-1)^M = (-1)^{\frac{p^2-1}{8}}$.

□

Exemplo 2.1 *Mostre que a equação diofantina* $X^2 - 13Y = 5$ *apresenta soluções.*

Solução: Caso essa equação diofantina possua alguma solução 5 será resíduo quadrático módulo 13, e então

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

Portanto,

$$\left(\frac{5}{13}\right) = (-1)^M = (-1)^5 = -1,$$

resultando em que 5 não é resíduo quadrático módulo 13.

Agora, vamos provar a Lei de Reciprocidade Quadrática. O próprio Gauss proporcionou pelo menos 8 demonstrações e a literatura abrange várias dessas, atribuindo ao matemático alemão Ferdinand Gotthold Max Eisenstein (1823−1852) a origem da demonstração que apresentaremos a seguir.

Teorema 2.2 *(Lei de Reciprocidade Quadrática de Gauss) Sejam p e q dois números primos ímpares distintos, então*

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

Demonstração: Usando argumentos geométricos, consideremos um sistema retangular de coordenadas. Marquemos sobre o eixo das abscissas os pontos distantes $1, 2, \ldots, \frac{(p-1)}{2}$ unidades da origem A, e sobre o eixo das ordenadas, os pontos distantes $1, 2, \ldots, \frac{(q-1)}{2}$ unidades de A além de marcarmos os pontos de vértice $A = (0,0)$; $B = (\frac{p}{2}, 0)$; $C = (\frac{p}{2}, \frac{q}{2})$ e $D = (0, \frac{q}{2})$ e, em seu interior, os pontos pertencentes ao produto cartesiano dos conjuntos $\{1, 2, 3, \ldots, \frac{(p-1)}{2}\}$ e $\{1, 2, 3, \ldots, \frac{(q-1)}{2}\}$ de acordo com a figura (2.1).

É possível verificar que o número de pontos de coordenadas naturais no interior do retângulo (dentro do retângulo, mas não na fronteira) apresenta coordenadas de números inteiros equivalentes a $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

Agora, a reta que passa por O e B tem por equação $py = qx \Rightarrow y = \frac{q}{p}\, x$, enquanto

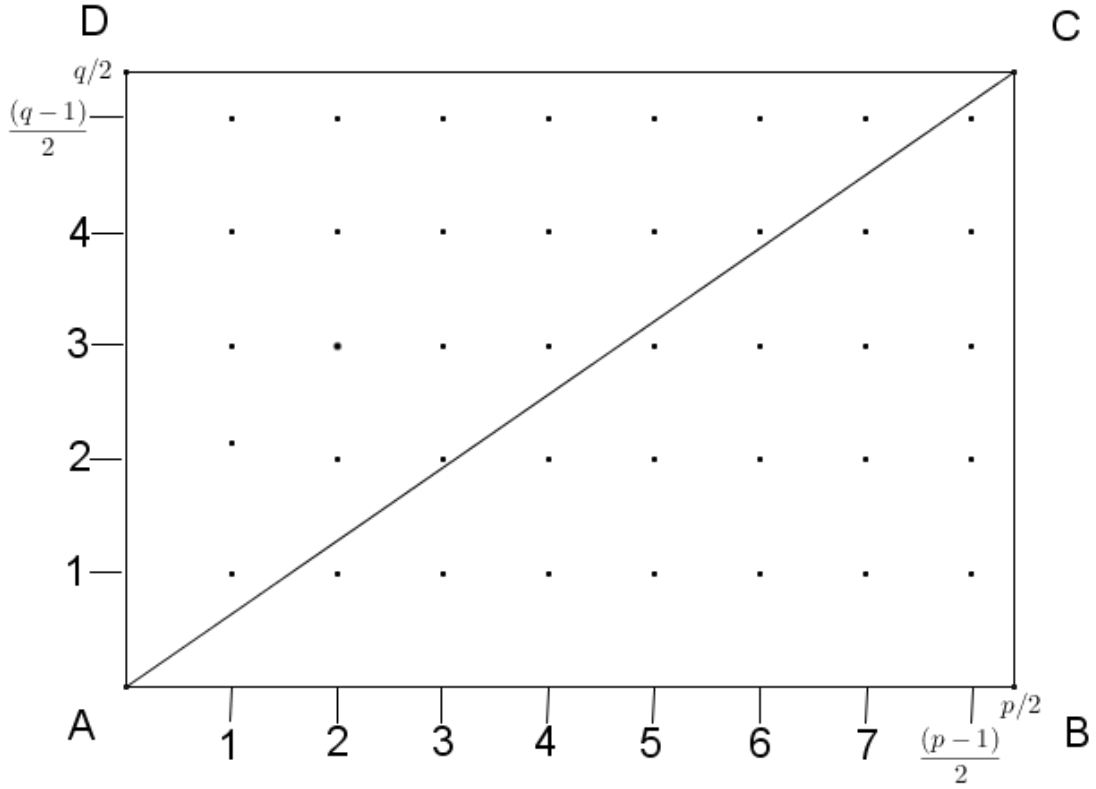

Figura 2.1: $y = \frac{q}{p}\, x$

que o fato de os números 1,2,..., $\frac{(p-1)}{2}$ serem todos primos com p acarreta em essa reta não possuir nenhum dos pontos interiores contados acima e, por consequência esta reta, $y = \frac{q}{p}\, x$, intercepta as retas $x = k$, paralelas ao eixo y, nos pontos de coordenadas $(k, \frac{kq}{p})$.

Como $\frac{kq}{p}$ não é inteiro e $1 \leq k \leq p-1$ obtemos que o número de pontos de coordenadas naturais sobre a reta $x = k$, acima do eixo x e abaixo da reta $y = \frac{q}{p}\, x$ é representado por $\left\lfloor \frac{kq}{p} \right\rfloor$ e, dessa maneira a quantidade de pontos de coordenadas naturais no interior do triângulo ABC é dado por

$$M = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{3q}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2} \cdot \frac{q}{p} \right\rfloor .$$

De forma análoga, as interseções das retas $y = k$, paralelas ao eixo x, com a reta $y = \left(\frac{q}{p}\right) x$ resulta que o número de pontos de coordenadas naturais no interior do triângulo ACD é igual a

$$N = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \left\lfloor \frac{3p}{q} \right\rfloor + \cdots + \left\lfloor \frac{q-1}{2} \cdot \frac{p}{q} \right\rfloor .$$

Então, $M + N$ é igual ao total

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

de pontos no interior do retângulo ABCD.

Dessa maneira, podemos escrever que

$$\left(\frac{q}{p}\right) = (-1)^M \text{ e } \left(\frac{p}{q}\right) = (-1)^N,$$

e consequentemente, pelo Teorema 1.6, temos

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

□

O Teorema da Lei de Reciprocidade Quadrática pode ser reenunciado das seguintes maneiras:

Corolário 1: *Se p e q são dois números distintos, tais que $p \equiv 1 \pmod 4$, ou $q \equiv 1 \pmod 4$, então q é resíduo quadrático módulo p, se, e somente se, p é resíduo quadrático módulo q;*

Corolário 2: *Se p e q são dois números distintos, tais que $p \equiv q \equiv 3 \pmod 4$, então q é resíduo quadrático módulo p, se, e somente se, p é não resíduo quadrático módulo q.*

Apresentaremos a seguir três demonstrações distintas da Lei de Reciprocidade

Quadrática. A primeira e a segunda demonstração, inspirada em [25]. Para efetuar a terceira demonstração, [8] aponta a utilização da definição de um conjunto. Para alcançar este propósito, vamos ressaltar a prova de dois lemas úteis a esta demonstração.

Primeira Demonstração: Inicialmente, consideremos a figura (2.2) em que

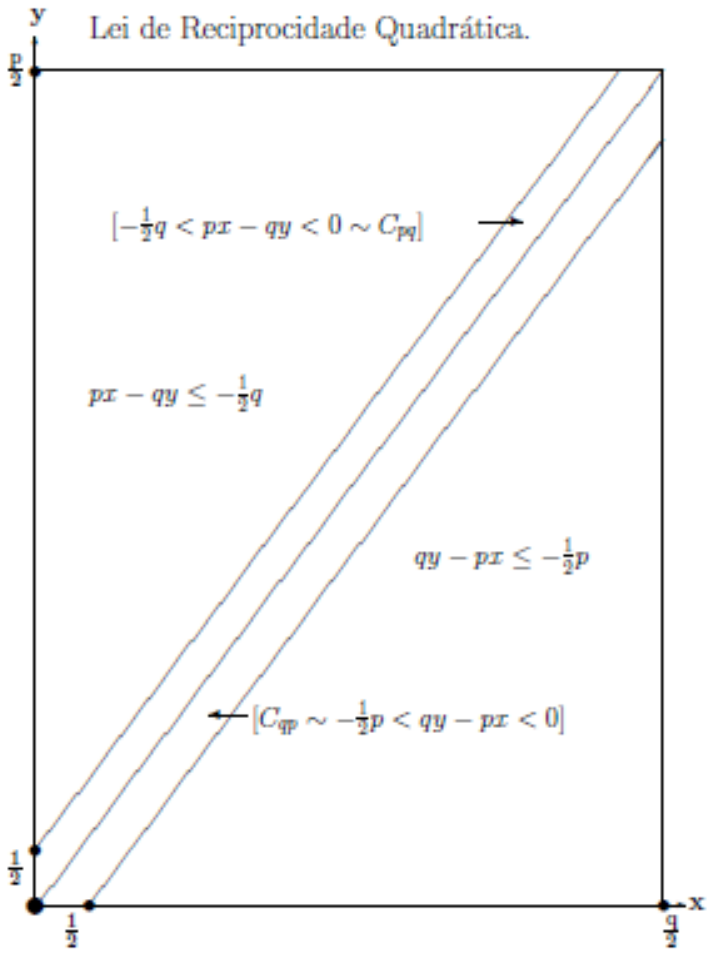

Figura 2.2: O Retângulo R

$$C_{pq} = \{x \in \mathbb{Z} \mid 1 \leq x \leq \frac{q-1}{2} \text{ e } -\frac{q-1}{2} \leq px \leq 0 \ (mod\ q)\}$$
$$C_{qp} = \{y \in \mathbb{Z} \mid 1 \leq y \leq \frac{p-1}{2} \text{ e } -\frac{p-1}{2} \leq qy \leq 0 \ (mod\ p)\}$$

$$M = \#\ \mathrm{C}_{pq}$$

$$N = \#C_{qp}$$

Então, pelo Lema de Gauss (Lema 1.1), temos

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

e, assim mostraremos que $M+N$ e $\frac{p-1}{2}\cdot\frac{q-1}{2}$ apresentam a mesma paridade.

Para cada $x \in C_{pq}$ existe um e apenas um $y \in \mathbb{Z}$ de modo que $-\frac{q-1}{2} \leq px - qy < 0$ e, simultaneamente $0 < y < \frac{p}{2}$. Ao observar que p é ímpar, temos

$$C_{pq} = \{(x,y) \in \mathbb{Z}^2 \mid 0 < x < \frac{1}{2}q \text{ e } 0 < y < \frac{1}{2}p \text{ e } -\frac{1}{2}q < px - qy < 0\}.$$

De forma análoga,

$$C_{qp} = \{(x,y) \in \mathbb{Z}^2 \mid 0 < x < \frac{1}{2}q \text{ e } 0 < y < \frac{1}{2}p \text{ e } -\frac{1}{2}p < qy - px < 0\}.$$

Caso,

$$R = \{(x,y) \in \mathbb{Z}^2 \mid 0 < x < \frac{1}{2}q \text{ e } 0 < y < \frac{1}{2}p\},$$

obtemos

$$\#R = \frac{p-1}{2}\cdot\frac{q-1}{2} \text{ e } \#R = (M+N)$$

representando o número de pares $(x,y) \in R$ de forma que

$$-\frac{1}{2}q < px - qy < 0 \quad ou \quad -\frac{1}{2}p < qy - px < 0,$$

sendo estas condições definitivas na construção de dois conjuntos disjuntos equipotentes pelo fato de

$$(x, y) \mapsto \frac{1}{2}\,(q+1, p+1) - (x', y')$$

definir uma bijeção entre ambas e portanto valida a condição de $M+N$ e $\frac{p-1}{2}\cdot\frac{q-1}{2}$ tem a mesma paridade.

□

Segunda Demonstração: Na notação do Teorema 2.2, com $p = q$, para cada $j \in P$, onde $P = \{1, 2, \ldots, \frac{p-1}{2}\}$, temos que $\varepsilon_j = -1$ se, e somemte se, existe $y \in \mathbb{Z}$ de forma que $-\frac{p-1}{2} \leq qj - py < 0$, além de y deve pertencer a Q, sendo $Q = \{1, 2, \ldots, \frac{q-1}{2}\}$.

Desse modo,

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

onde $M = |R|$ e $R = \{(x, y) \in P \times Q \mid -\frac{(p-1)}{2} \leq qx - py < 0\ \}$. Observemos que $qx - py$ nunca assume valores 0 e, assim

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

em que $N = |S|$ e $S = \{(x, y) \in P \times Q \mid 0 < qx - py \leq -\frac{(q-1)}{2}\ \}$.

Logo,

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

onde $K = M + N = |T|$, e $T = \{(x, y) \in P \times Q \mid -\frac{(p-1)}{2} \leq qx - py \leq -\frac{(q-1)}{2}\ \}$ porque $qx - py$ nunca assume o valor 0. Então, $k = |G| - |E| - |F|$ onde $G = P \times Q$ e

$$E = \{(x, y) \in G \mid qx - py < -\frac{(p-1)}{2}\ \};$$
$$F = \{(x, y) \in G \mid qx - py > -\frac{(q-1)}{2}\ \}.$$

Como $|G| = \frac{p-1}{2}\cdot\frac{q-1}{2}$, mostremos que $|E| = |F|$. Mas $\Omega : G \to G$ é definida

por $\Omega\ (x,y) = \left(\frac{(p+1)}{2} - x, \frac{(q+1)}{2} - y\right)$ o que representa uma bijeção entre E e F.

□

Terceira Demonstração: Consideremos o conjunto C definido por $C = \{a : 1 \leq a \leq \frac{p-1}{2}\}$, sendo $(a, pq) = 1$ e, em seguida o conjunto $A = \prod_{a \in C} a$. Com isso, temos

Lema 2.1 $A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)\ (mod\ p)$ *e* $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)\ (mod\ q)$.

Demonstração: Sendo conjunto

$D = \{a : 1 \leq a \leq \frac{p-1}{2}\}$, onde $(a, p) = 1$, e $E = \{q \cdot 1, q \cdot 2, \ldots, q \cdot \frac{p-1}{2}\}$

podemos admitir que E é um subconjunto de D porque

$$\frac{pq-1}{2} = \frac{p-1}{2}q + \frac{q-1}{2}. \tag{2.5}$$

Ao observar que $C = D - E$ onde, pelo Critério de Euler, temos

$$\prod_{a \in D} a = \prod_{a \in E} a \cdot \prod_{a \in C} a = q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \cdot A \equiv \left(\tfrac{q}{p}\right) \left(\frac{p-1}{2}\right)! \cdot A\ (mod\ p).$$

Podemos também escrever a expressão (2.5) de seguinte forma:

$$\frac{pq-1}{2} = \frac{q-1}{2}p + \frac{p-1}{2}. \tag{2.6}$$

Portanto,

$$\prod_{a \in D} a = ((p-1)!)^{\frac{q-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \cdot A\ (mod\ p)$$

onde, pelo Teorema de Wilson, (Anexo B), temos

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

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

As outras declarações do Lema 2.1 seguem por simetria e, dessa maneira segue-se consecutivamente que $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \Leftrightarrow A \equiv 1\ ou - 1\ (mod\ pq)$.

Lema 2.2 *$A \equiv 1$ ou -1 $(mod\ pq)$ se, e somente se, $p \equiv q \equiv 1$ $(mod\ 4)$.*

Demonstração: Ao determinarmos $z = pq$, pelo teorema Chinês do Resto, (Anexo B), a congruência $x^2 \equiv 1\ (mod\ z)$ tem precisamente 4 soluções: $x \equiv 1, -1, n, -n\ (mod\ z)$. Já a congruência $x^2 \equiv -1\ (mod\ z)$ apresenta uma solução, $x \equiv I\ (mod\ z)$, apenas se $p \equiv q \equiv 1\ (mod\ 4)$ e dessa forma haverá precisamente 4 soluções, isto é, $x \equiv 1, - 1, n_1, - n_1\ (mod\ z)$.

Agora, para cada "a" em G , existe um único a em G e $8a$ em $\{-1, 1\}$ tal que $a \cdot a' \equiv 8a\ (mod\ z)$ cuja correspondência $a \to a'$ é uma permutação de Ψ. Ao escrevermos $G = \{a \in \text{C: a = a'}\} = \{\text{a} \in C : a^2 \equiv \pm 1\ (mod\ z)\}$ observemos que $G = \prod_{a \in C} a \equiv \pm \prod_{a \in G} a\ (mod\ z)$, se $p \equiv q \equiv 1\ (mod\ 4)$, e então $\prod_{a \in G} a \equiv \pm (1 \cdot n \cdot I \cdot I \cdot n)(n^2 \cdot I^2) \equiv \pm 1\ (mod\ d)$. Caso contrário, teríamos $\prod_{a \in G} a \equiv \pm (1 \cdot n^2) \neq \pm 1\ (mod\ d)$.

Ao combinarmos os Lemas 2.1 e 2.2 conclui−se 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, $p \equiv q \equiv 1\ (mod\ 4)$. O teorema agora segue pela consideração dos 4 casos: $(p, q) \equiv (1, 1), (1, -1), (-1, 1), (-1, -1)\ (mod\ 4)$ ou através de fórmulas uma vez que $p \equiv q \equiv 1\ (mod\ 4)$ se, e somente se, $(-1)^{\frac{p+1}{2}\frac{q+1}{2}} = -1$. Logo,

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

Contudo,

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

o que resultará em

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

□

Exemplo 2.2 *Calcule* $\left(\frac{402}{991}\right)$.

Solução: Como 991 é um número primo e que $402 = 2 \cdot 3 \cdot 67$, teremos que

$$\left(\frac{2}{991}\right) = 1 \qquad (991 \equiv -1 \ (mod\ 8))$$

$$\begin{aligned}\left(\frac{3}{991}\right) &= -\left(\frac{991}{3}\right) && (991 \equiv -3 \ (mod\ 4))\\ &= -\left(\frac{1}{3}\right) && (991 \equiv -1 \ (mod\ 3))\\ &= -1.\end{aligned}$$

$$\begin{aligned}\left(\frac{67}{991}\right) &= -\left(\frac{991}{67}\right) && (991 \equiv 67 \equiv 3 \ (mod\ 4))\\ &= -\left(\frac{-14}{67}\right) && (991 \equiv -14 \ (mod\ 67))\\ &= -\left(\frac{-1}{67}\right)\left(\frac{2}{67}\right)\left(\frac{7}{67}\right) && (-14 = (-1)\cdot 2 \cdot 7)\\ &= -(-1)\cdot(-1)\cdot\left(-\left(\frac{67}{7}\right)\right) && (67 \equiv 3 \ (mod\ 8) \text{ e } 7 \equiv 3 \ (mod\ 4))\\ &= \left(\frac{4}{7}\right) && (67 \equiv 4 \ (mod\ 7))\\ &= 1.\end{aligned}$$

Portanto, $\left(\frac{402}{991}\right) = \left(\frac{2}{991}\right)\left(\frac{3}{991}\right)\left(\frac{67}{991}\right) = 1\cdot(-1)\cdot 1 = -1.$

Logo, a Lei de Reciprocidade Quadrática e o fato de já termos visto que

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \ (mod\ 4) \\ -1 & \text{se } p \equiv 3 \ (mod\ 4) \end{cases} \textit{(Propriedade 3 do Teorema 1.5)}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \ (mod\ 8) \\ -1 & \text{se } p \equiv \pm 3 \ (mod\ 8) \end{cases} \quad \textit{(Teorema 1.6)}$$

nos permite acrescentar mais alguns resultados parecidos para os seguntes Símbolos de Legendre.

Exemplo 2.3 *Mostre que se p é um primo ímpar, então,*

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

Solução: Usando a Lei de Reciprocidade Quadrática temos

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

Enquanto que o Teorema 1.5 (1) permite escrever

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

Por outro lado,

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \ (mod\ 4) \\ -1 & \text{se } p \equiv 2 \ (mod\ 4) \end{cases}$$

Assim,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \text{ ou p} \equiv 11 \ (mod\ 12) \\ -1 & \text{se } p \equiv 5 \text{ ou p} \equiv 7 \ (mod\ 12) \end{cases}$$

Exemplo 2.4 *Calcule* $\left(\frac{5}{p}\right)$ *, onde p é um número primo maior do que 5.*

Solução: Com o auxílio da Lei de Reciprocidade Quadrática temos

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

Pelo Teorema 1.5 (1), temos

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

Teorema 2.3 *Para todo primo p existem inteiros a, b e c, não todos nulos, tais que se verifica a seguinte congruência:*

$$a^2 + b^2 + c^2 \equiv 0 \ (mod\ p).$$

Demonstração: Quando fizermos $p = 2$ e tomando $a = b = 1$ e $c = 0$ obtemos $1^2 + 1^2 + 0^2 \equiv 0 \ (mod\ 2)$. Agora, pelo Teorema 1.3, ao admitir que se $p \equiv 1 \ (mod\ 4)$ tomaremos a como uma solução de $x^2 \equiv 1 \ (mod\ p)$, $b = 1$ e $c = 0$ enquanto que para $p \equiv 3 \ (mod\ 4)$ adotaremos $c = 1$ para mostrar a existência de solução para a congruência $a^2 + b^2 \equiv -1 \ (mod\ p)$. Então, o Teorema 1.2 nos garante que sendo p um primo ímpar teremos que $\frac{p-1}{2}$ serão os resíduos quadráticos e $\frac{p-1}{2}$ não serão, dentre os números $1, 2, \ldots, p-1$, mas se k for resíduo quadrático encontramos a congruência $x^2 \equiv k \ (mod\ p)$ que apresenta solução, quando p é primo. Consideremos dentre os números 1, 2,..., $p-1$ que d seja o menor resíduo positivo não−quadrático módulo p em que 1 é resíduo quadrático para $d \geqslant 2$, o Teorema 1.5 (3) possibilita observar que se $p \equiv 3 \ (mod\ 4)$ teremos $\left(\frac{-1}{p}\right) = -1$. E se d não é resíduo quadrático obtemos que $\left(\frac{d}{p}\right) = -1$. Então, pelo Teorema 1.5 (4), podemos escrever que

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

o que permite afirmar que $-d$ é um resíduo quadrático módulo p, ou seja, a congruên-

cia $x^2 \equiv -d \ (mod\ p)$ apresenta solução. Sendo b de maneira que $b^2 \equiv -d \ (mod\ p)$ precisaremos encontrar um "a" em que $a^2 \equiv d-1 \ (mod\ p)$ e assim resulta em

$$\begin{cases} a^2 \equiv d-1 \ (mod\ p) \\ b^2 \equiv -d \ (mod\ p) \end{cases} \Rightarrow a^2 + b^2 \equiv -1 (mod\ p).$$

No entanto, a congruência $a^2 \equiv d-1 \ (mod\ p)$ possui claramente solução por $d \geqslant 2$, $d-1 < d$ e d ser o menor resíduo não−quadrático positivo módulo p. Por isso, $d-1$ será resíduo quadrático módulo p e a congruência $a^2 + b^2 \equiv -1 \ (mod\ p)$ apresentará solução, resultando na demostração da congruência $a^2 + b^2 + c^2 \equiv 0 \ (mod\ p)$.

□

2.2 Símbolo de Jacobi

O Símbolo de Jacobi apresenta várias propriedades similares ao Símbolo de Legendre. A generalização desta simbologia foi desenvolvida para valores não primos por Carl Gustav Jakob Jacobi (1804-1851), em 1837, tendo como principal utilidade na Teoria dos Números Computacional, especialmente no teste de primalidade e fatoração de inteiros e com grande importância na criptografia.

Definição 2.1 *Seja n um número positivo com respectiva fatoração em componentes primos ${p_1}^{e_1}\ {p_2}^{e_2} \cdots {p_k}^{e_k}$. Para qualquer valor $a \geq 0$, o Símbolo de Jacobi é definido como o produto dos Símbolos de Legendre relativamente aos componentes primos de n, na forma da expressão*

$$\left[\frac{a}{n}\right] = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i},$$

onde $\left(\frac{a}{p_i}\right)$ é o Símbolo de Legendre.

Exemplo 2.5 *Calcule* $\left[\frac{3}{539}\right]$ *e* $\left[\frac{81}{385}\right]$.

Solução:

$$\left[\frac{3}{539}\right] = \left[\frac{3}{7^2.11}\right] = \left(\frac{3}{7}\right)^2 \cdot \left(\frac{3}{11}\right) = (-1)^2(-1) = -1;$$

$$\left[\frac{81}{385}\right] = \left[\frac{81}{5.7.11}\right] = \left(\frac{81}{5}\right) \cdot \left(\frac{196}{7}\right) \cdot \left(\frac{81}{11}\right)$$

$$= \left(\frac{1}{5}\right) \cdot \left(\frac{4}{7}\right) \cdot \left(\frac{4}{11}\right) = \left(\frac{1}{5}\right) \cdot \left(\frac{2}{7}\right)^2 \cdot \left(\frac{2}{11}\right)^2 = 1.$$

Em [21], Santos ressalta que o símbolode Legendre $\left(\frac{a}{p}\right)$ nos informa sobre a existência de soluções para a congruência $x^2 \equiv a \ (mod\ p)$, enquanto que o Símbolo de Jacobi $\left[\frac{a}{n}\right]$ não fornece nenhuma informação a respeito da existência de soluções para a congruência $x^2 \equiv a \ (mod\ n)$. Caso n seja primo o Símbolo de Jacobi será idêntico ao Símbolo de Legendre. Agora, se p é um fator primo de n e se $x^2 \equiv a \ (mod\ n)$ possui solução concluímos que a congruência $x^2 \equiv a \ (mod\ p)$ também terá solução, ou seja, $\left(\frac{a}{p}\right) = 1$. Portanto,

$$\left[\frac{a}{n}\right] = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i} = 1.$$

Exemplo 2.6 *Sendo $a = 2$ e $n = 35$, mostre a existência de $\left[\frac{a}{n}\right] = 1$ pode ocorrer sem que a congruência $x^2 \equiv a \ (mod\ n)$ apresente solução.*

Solução: Seja

$$\left[\frac{2}{35}\right] = \left[\frac{2}{5.7}\right] = \left(\frac{2}{5}\right) \cdot \left(\frac{2}{7}\right) = (-1)(-1) = 1.$$

As congruências $x^2 \equiv 2 \ (mod\ 5)$ e $x^2 \equiv 2 \ (mod\ 7)$ não possuem nenhuma solução e, por consequência a congruência $x^2 \equiv 2 \ (mod\ 35)$ não terá solução alguma. Entretanto, o Símbolo de Jacobi cumpre as mesmas regras computacionais que o Símbolo de Legendre, incluindo a demonstração da Lei de Reciprocidade Quadrática.

Teorema 2.4 *Sejam a e n inteiros positivos ímpares e primos entre si. Pelas propriedades do Símbolo de Legendre e pela definição de Jacobi, seguem as seguintes propriedades:*

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

(2) $\left[\frac{a^2}{n}\right] = 1$;

(3) $\left[\frac{a}{n}\right]\left[\frac{b}{n}\right] = \left[\frac{ab}{n}\right]$;

(4) $\left[\frac{a}{m}\right]\left[\frac{a}{n}\right] = \left[\frac{a}{mn}\right]$;

(5) $\left[\frac{-1}{n}\right] = (-1)^{\frac{n-1}{2}}$;

(6) $\left[\frac{2}{n}\right] = (-1)^{\frac{p^2-1}{8}}$;

(7) $\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$. *(Lei de Reciprocidade Quadrática)*

Demostração: As propriedades *(1)* a *(3)* são consequências imediatas da definição do Símbolo de Jacobi e do fato destas propriedades se aplicarem ao Símbolo de Legendre. Já a propriedade *(4)* segue da definição do Símbolo de Jacobi em que se $m = p_1, \cdots, p_j$ e $n = q_1, \cdots, q_k$ representam as decomposições em fatores primos de m e n permitindo que os primos p_i e q_j possam aparecer repetidos. Portanto,

$$\left[\frac{a}{m}\right]\left[\frac{a}{n}\right] = \left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_j}\right)\left(\frac{a}{q_1}\right)\cdots\left(\frac{a}{q_k}\right) = \left(\frac{a}{p_1\cdots p_j q_1\cdots q_k}\right) = \left[\frac{a}{mn}\right].$$

Agora, para verificarmos as propriedades *(5)*, *(6)* e *(7)* precisaremos do Lema a seguir.

Lema 2.3 *Se* x *e* y *são números inteiros ímpares, então*

$$\frac{x-1}{2} + \frac{y-1}{2} \equiv \frac{xy-1}{2} \ (mod\ 2) \tag{2.7}$$

e

$$\frac{x^2-1}{8} + \frac{y^2-1}{8} \equiv \frac{x^2y^2-1}{8} \ (mod\ 2). \tag{2.8}$$

Demonstração: Como x e y são números ímpares, os números $(x-1)$ e $(y-1)$ são pares, e assim $\dfrac{(x-1)(y-1)}{2}$ continuará sendo par, além de

$$0 \equiv \frac{(x-1)(y-1)}{2} \equiv \frac{xy-x-y+1}{2} \equiv \frac{xy-1-x+1-y+1}{2} \ (mod\ 2)$$

provando dessa maneira $\dfrac{x-1}{2} + \dfrac{y-1}{2} \equiv \dfrac{xy-1}{2}\ (mod\ 2)$.

Em contrapartida, $(x-1)$ e $(x+1)$ são pares e consequentemente $x^2-1 = (x-1)(x+1)$ possui pelo menos dois fatores 2 e, por analogia, para y^2-1 podemos admitir que $(x^2-1)(y^2-1)$ tem pelo menos 4 fatores 2 o resultará em $\dfrac{(x^2-1)(y^2-1)}{8}$ ser par e

$$0 \equiv \frac{(x^2-1)(y^2-1)}{8} \equiv \frac{x^2y^2-x^2-y^2+1}{8} \equiv \frac{x^2y^2-1-x^2+1-y^2+1}{8} \ (mod\ 2)$$

provando dessa maneira que $\dfrac{x^2-1}{8} + \dfrac{y^2-1}{8} \equiv \dfrac{x^2y^2-1}{8}\ (mod\ 2)$.

Vamos supor que $m = p_1, \cdots, p_j$ e $n = q_1, \cdots, q_k$ são decomposições em fatores primos de m e n em que os primos p_j e q_k podem aparecer repetidos. Então,

$$\left[\frac{-1}{n}\right] = \left(\frac{-1}{n}\right) = \left(\frac{-1}{q_1}\right) \cdots \left(\frac{-1}{q_j}\right) = (-1)^{\sum_{h=1}^{j} \frac{q_h-1}{2}} = (-1)^{\frac{n-1}{2}}.$$

Pela congruência (2.7) obtemos $\sum_{h=1}^{j} \frac{q_h-1}{2} = \frac{(\prod_{h=1}^{j} q_h)-1}{2}\ (mod\ 2)$.

De forma similar, é possível demonstrar, pela congruência (2.8), que $\left[\dfrac{2}{n}\right] = (-1)^{\frac{p^2-1}{8}}$ sendo possível constatar que, para h fixo, a congruência (2.7) resultará em $\sum_{i=1}^{k} \frac{p_h-1}{2}\frac{q_i-1}{2} \equiv \frac{p_h-1}{2}\sum_{i=1}^{k}\frac{q_i-1}{2} \equiv \frac{p_h-1}{2}\ \frac{(\prod_{i=1}^{k} q_i)-1}{2}\ (mod\ 2)$. Então, pelas propriedades 3 e 4 podemos escrever

$$\left[\frac{a}{n}\right]\left[\frac{n}{a}\right] = \left(\prod_{h=1}^{j}\prod_{i=1}^{k}\left(\frac{q_i}{p_h}\right)\right)\left(\prod_{h=1}^{j}\prod_{i=1}^{k}\left(\frac{p_h}{q_i}\right)\right) = \prod_{h=1}^{j}\prod_{i=1}^{k}\left(\frac{q_i}{p_h}\right)\left(\frac{p_h}{q_i}\right)$$

$$= \prod_{h=1}^{j}\prod_{i=1}^{k}(-1)^{\frac{p_h-1}{2}\frac{q_i-1}{2}} = (-1)^{\sum_{h=1}^{j}\sum_{i=1}^{k}\frac{p_h-1}{2}\frac{q_i-1}{2}}$$

$$= (-1)^{\sum_{h=1}^{j} \frac{p_h-1}{2}\frac{n-1}{2}} = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

□

Provamos assim a propriedade *(7)* que se refere à Lei da Reciprocidade Quadrática por meio do Símbolo de jacobi.

Exemplo 2.7 *Avalie os Símbolos de Jacobi* $\left[\frac{429}{563}\right]$ e $\left[\frac{181}{991}\right]$.

Solução: Vamos analisar os Símbolos de Jacobi $\left[\frac{429}{563}\right]$ e $\left[\frac{181}{991}\right]$, no qual faremos uso da Lei da Reciprocidade Quadrática. Então,

$$\begin{aligned}
\left[\frac{429}{563}\right] &= (-1)^{\frac{429-1}{2}\frac{563-1}{2}}\left[\frac{563}{429}\right] = \left[\frac{563}{429}\right] \\
&= \left[\frac{134}{429}\right] = \left[\frac{2}{429}\right]\left[\frac{67}{429}\right] \\
&= (-1)^{\frac{67-1}{2}\frac{429-1}{2}}\left[\frac{429}{67}\right] = \left[\frac{429}{67}\right] \\
&= \left[\frac{27}{67}\right] = (-1)^{\frac{27-1}{2}\frac{67-1}{2}}\left[\frac{67}{27}\right] = -\left[\frac{13}{27}\right] \\
&= -(-1)^{\frac{13-1}{2}\frac{27-1}{2}}\left[\frac{27}{13}\right] = -1.
\end{aligned}$$

$$\begin{aligned}
\left[\frac{181}{991}\right] &= (-1)^{\frac{181-1}{2}\frac{991-1}{2}}\left[\frac{991}{181}\right] = \left[\frac{991}{181}\right] \\
&= \left[\frac{86}{181}\right] = \left[\frac{2}{181}\right]\left[\frac{43}{181}\right] \\
&= (-1)^{\frac{181^2-1}{8}}\left[\frac{43}{81}\right] = -\left[\frac{43}{81}\right] \\
&= -(-1)^{\frac{43-1}{2}\frac{181-1}{2}}\left[\frac{181}{43}\right] = -\left[\frac{181}{43}\right] \\
&= -\left[\frac{9}{43}\right] = -\left[\frac{3}{43}\right]^2 = -1.
\end{aligned}$$

2.3 Extraindo Raízes Quadradas módulo n

Vamos desenvolver as ferramentas para encontrar as raízes quadradas modulares. Sendo a uma função quadrática resíduo módulo p, com p primo ímpar, a congruência $x^2 \equiv a \ (mod\ p)$ terá exatamente duas soluções dadas por $[\pm\ x_0]$, para qualquer solução particular x_0. Então, descobriremos o valor de x_0.

Teorema 2.4 *Se* $\left(\frac{a}{p}\right) = 1$ *e* $p \equiv 5 \ (mod\ 8)$ *em que* $s = a^{\frac{(p+3)}{8}}$ *teremos que a congruência* $x^2 \equiv a \ (mod\ p)$ *apresentará como soluções* s *ou* $2^{\frac{(p-1)}{4}} \cdot s$.

Demostração: Sendo $\left(\frac{2}{p}\right) = -1$, Teorema 2.7, podemos escrever, pelo Critério de Euler, que $2^{\frac{(p-1)}{2}} \equiv -1 \ (mod\ p)$. Assim, a congruência $s^4 = a^{\frac{(p-1)}{2}} a^2 \equiv a^2 \ (mod\ p)$ resultará em $s^2 \equiv \pm a \ (mod\ p)$ se $s^2 \equiv -a \ (mod\ p)$. Consequentemente $2^{\frac{(p-1)}{4}} \cdot s$ será solução para $x^2 \equiv a \ (mod\ p)$.

□

Exemplo 2.8 *Resolva a congruência* $x^2 \equiv 5 \ (mod\ 29)$.

Solução: É possível verificar que $29 \equiv 5 \ (mod\ 8)$ e, dessa maneira $s = 5^{\frac{(29+3)}{8}} = 5^4 = 625 \equiv 16 \ (mod\ 29)$. Mas também $16^2 = 256 \equiv 24 \equiv -5 \ (mod\ 29)$ que ao fazermos $2^7 = 128 \equiv 12 \ (mod\ 29)$ teremos $x_0 = 12 \cdot 16 = 192$ e, portanto a solução particular será $x_0 \equiv 192 \equiv 11 \ (mod\ 29)$ e $-x_0 \equiv -11 \equiv 18 \ (mod\ 29)$.

Teorema 2.5 *Se* $\left(\frac{a}{p}\right) = 1$ *e* $p \equiv 3 \ (mod\ 4)$, *então existe exatamente duas soluções para a congruência* $x^2 \equiv a \ (mod\ p)$, *onde* $x \equiv \pm a^{\frac{(p+1)}{4}} \ (mod\ p)$.

Demonstração: O Critério de Euler nos fornece que $(a^{\frac{(p+1)}{4}})^2 = a^{\frac{(p+1)}{2}} = a^{\frac{(p-1)}{2}} a \equiv a \ (mod\ p)$.

□

Uma aplicação bastante útil é o cálculo de raízes quadradas onde, através da tecla de raiz quadrada, a maioria das calculadoras manuais a informam de maneira instantânea como, por exemplo, podemos observar que $\sqrt{29} \approx 5{,}38516480$. No entanto,

o resultado de $\sqrt{29}$ em $\mathbb{Z}_{71}$ é impossível de se obter na maiorias das calculadoras e assim quando expressamos que 7 é raiz quadrada de 49 queremos afirmar que 7 é raiz da equação $x^2 - 49 = 0$ sendo que 49 tem duas raízes quadradas diferentes: $+7$ e -7.

A raiz positiva apresenta um tratamento preferencial, pois quando pesquisamos as raízes quadradas de 29 mentalizamos que x $\in \mathbb{Z}_{71}$ e o resultado apresentado pela calculadora não nos ajuda em nada. Podemos, então, utilizar a Lei de Reciprocidade Quadrática para solucionar esse problema uma vez que existe apenas 71 elementos distintos em $\mathbb{Z}_{71}$ e por meio do Teorema 2.5 podemos enfim declarar as raízes quadradas de 29 em $\mathbb{Z}_{71}$, ou seja, obter as soluções da congruência $x^2 \equiv 29 \ (mod\ 71)$. De modo inicial, temos $\left(\frac{29}{71}\right) = (-1)^{\frac{29-1}{2}\frac{71-1}{2}}\left(\frac{71}{29}\right) = \left(\frac{71}{29}\right) = \left(\frac{13}{29}\right) = (-1)^{\frac{13-1}{2}\frac{29-1}{2}}\left(\frac{29}{13}\right) = \left(\frac{29}{13}\right) = \left(\frac{3}{13}\right) = (-1)^{\frac{3-1}{2}\frac{13-1}{2}}\left(\frac{13}{3}\right) = \left(\frac{13}{3}\right) = 1$ e como $71 \equiv 3 \ (mod\ 4)$ obtemos como solução particular $x_0 = 29^{\frac{(71+1)}{4}} = 29^{18} \equiv 10 \ (mod\ 71)$. Logo, as soluções são dadas por $x_0 = 10 \ (mod\ 71)$ e $-x_0 = -10 \equiv 61 \ (mod\ 71)$.

Essa aplicação é válida para $\mathbb{Z}_p$ em que p é primo, mas também podemos obter a raiz quadrada para um certo n de forma que $n = pq$. Então, para encontrar $\sqrt{500}$ em $\mathbb{Z}_{589}$ é preciso visualizar que $n = 589 = 19 \cdot 31$ onde podemos escrever as seguintes congruências $x^2 \equiv 500 \ (mod\ 19)$, ou seja, $x^2 \equiv 6 \ (mod\ 19)$ e $x^2 \equiv 500 \ (mod\ 31)$, isto é, $x^2 \equiv 4 \ (mod\ 31)$. O fato de termos, pelo teorema 1.11, $19 \equiv 3 \ (mod\ 4)$ e $31 \equiv 3 \ (mod\ 4)$ nos permite concluir que $\left(\frac{6}{19}\right) = 1$ e $\left(\frac{4}{31}\right) = 1$. Portanto,

$$x_0 = 6^{\frac{(19+1)}{4}} = 6^5 \equiv 5 \ (mod\ 19) \Rightarrow x_0 = 5 \text{ e } -x_0 = 14;$$
$$x_1 = 4^{\frac{(31+1)}{4}} = 4^8 \equiv 2 \ (mod\ 31) \Rightarrow x_1 = 2 \text{ e } -x_1 = 29.$$

Com essa redução, caso x seja uma raiz quadrada de 500 em $\mathbb{Z}_{589}$ também será uma raiz quadrada de 500 em $\mathbb{Z}_{19}$ e em $\mathbb{Z}_{31}$ de maneira que x satisfaça $x \equiv 5, 14 \ (mod\ 19)$ e $x \equiv 2, 29 \ (mod\ 31)$ o que resulta nos quatro problemas a resolver:

$$\begin{array}{ll} x \equiv 5 \ (mod\ 19) & (i) \\ x \equiv 2 \ (mod\ 31) & \end{array} \qquad \begin{array}{ll} x \equiv 5 \ (mod\ 19) & (ii) \\ x \equiv 29 \ (mod\ 31) & \end{array}$$

$$x \equiv 14 \ (mod\ 19) \qquad (iii) \qquad\qquad x \equiv 14 \ (mod\ 19) \qquad (iv)$$

$$x \equiv 2 \ (mod\ 31) \qquad\qquad x \equiv 29 \ (mod\ 31)$$

Para solucionar esses quatro problemas será preciso fazer uso do Teorema do Resto Chinês, (Anexo B). Com isso, é posível verificar de imediado a presença de quatro raízes quadradas de 500 em $\mathbb{Z}_{589}$, ou seja, ao resolver cada sistema de congruência por esse teorema obtemos as quatro raízes quadradas de 500, em $\mathbb{Z}_{589}$, como sendo 157,556,33 e 432, nessa ordem. Agora, de forma semelhante, vamos determinar todos os valores de $\sqrt{17985}$ em $\mathbb{Z}_{34751}$ em que $n = 34751 = 19 \cdot 31 \cdot 59$. Isto implicará nas seguintes congruências:

$$x^2 \equiv 17895 \ (mod\ 19) \Rightarrow x^2 \equiv 11 \ (mod\ 19);$$
$$x^2 \equiv 17895 \ (mod\ 31) \Rightarrow x^2 \equiv 5 \ (mod\ 31);$$
$$x^2 \equiv 17895 \ (mod\ 59) \Rightarrow x^2 \equiv 49 \ (mod\ 59).$$

Como $19 \equiv 3 \ (mod\ 4)$, $31 \equiv 3 \ (mod\ 31)$ e $59 \equiv 3 \ (mod\ 4)$ podemos escrever que

$$x_0 = 11^{\frac{(19+1)}{4}} = 11^5 \equiv 7 \ (mod\ 19) \Rightarrow x_0 = 7 \text{ e } -x_0 = 12;$$
$$x_1 = 5^{\frac{(31+1)}{4}} = 5^8 \equiv 25 \pmod{31} \Rightarrow x_1 = 25 \text{ e } -x_1 = 6;$$
$$x_2 = 49^{\frac{(59+1)}{4}} = 49^{15} \equiv 7 \ (mod\ 59) \Rightarrow x_2 = 7 \text{ e } -x_2 = 52;$$

o que equivale dizer que como x é uma raiz quadrada de 17985 em $\mathbb{Z}_{34751}$ também será uma raiz quadrada de 17985 em $\mathbb{Z}_{19}$, em $\mathbb{Z}_{31}$ e em $\mathbb{Z}_{59}$. Nesse caso, x coresponderá a $x \equiv 7, 12 \ (mod\ 19)$, $x \equiv 25, 6 \ (mod\ 31)$, e $x \equiv 7, 52 \ (mod\ 59)$ decorrendo em oito problemas a resolver:

$$\begin{array}{ll} x \equiv 12 \ (mod\ 19) & \\ x \equiv 25 \ (mod\ 31) & (i) \\ x \equiv 7 \ (mod\ 59) & \end{array} \qquad \begin{array}{ll} x \equiv 12 \ (mod\ 19) & \\ x \equiv 6 \ (mod\ 31) & (ii) \\ x \equiv 52 \ (mod\ 59) & \end{array}$$

$$\begin{array}{ll} x \equiv 12 \ (mod\ 19) & \\ x \equiv 25 \ (mod\ 31) & (iii) \\ x \equiv 52 \ (mod\ 59) & \end{array} \qquad \begin{array}{ll} x \equiv 12 \ (mod\ 19) & \\ x \equiv 6 \ (mod\ 31) & (iv) \\ x \equiv 7 \ (mod\ 59) & \end{array}$$

$$\begin{array}{ll} x \equiv 7 \ (mod\ 19) & \\ x \equiv 25 \ (mod\ 31) & (v) \\ x \equiv 7 \ (mod\ 59) & \end{array} \qquad \begin{array}{ll} x \equiv 7 \ (mod\ 19) & \\ x \equiv 6 \ (mod\ 31) & (vi) \\ x \equiv 7 \ (mod\ 59) & \end{array}$$

$$\begin{array}{l} x \equiv 7 \ \ (mod\ 19) \\ x \equiv 25 \ (mod\, 31) \\ x \equiv 52 \ \ (mod\ 59) \end{array} \quad (vii) \qquad \begin{array}{l} x \equiv 7 \ \ (mod\ 19) \\ x \equiv 6 \ \ (mod\, 31) \\ x \equiv 52 \ \ (mod\ 59) \end{array} \quad (viii)$$

Então, para resolvermos esses oito problemas também será preciso fazer uso do Teorema do Resto Chinês, (Anexo B). Observa−se de imediado a existência de oito raízes quadradas de 17985 em $\mathbb{Z}_{34751}$, isto é, solucionando cada sistema de congruência por esse teorema é possível especificar as oito raízes quadradas de 17985,em $\mathbb{Z}_{34751}$ como sendo 19772, 16808, 28018, 8562, 17943, 6733, 26189 e 14979, respectivamente. No entanto, é possível obter, de forma semelhante, raízes cúbicas e biquadradas módulo n.

Dessa maneira, para determinarmos a raiz quadrada módulo n devemos usar a fatoração, o cálculo da raiz quadrada em $\mathbb{Z}_p$ e o Teorema do Resto Chinês, (Anexo B). Já em uma visão computacional a fatoração é a etapa mais complicada enquanto que as outras fases são desenvolvidas de forma eficiente pelo computador. Portanto, o processo de obtenção das raízes quadradas de números em $\mathbb{Z}_n$ torna−se viável quando n é um inteiro da forma $n = pq$ com p e q primos de modo que $p \equiv q \equiv 3\ (mod\ 4)$. Mas, se p e q forem primos com 100 algarismos a etapa da fatoração torna o processo totalmente impraticável.

Capítulo 3

Aplicações em Sala de Aula

A Teoria dos Números abrange os fundamentos em Matemática sendo estes necessários para construir e para aprender mais Matemática. A resolução de certos tipos de problemas aplicáveis à vida cotidiana necessita de estratégias que não se resumem a simples cálculos mesmo que Teoria dos Números aparenta ser uma área da Matemática que lida com problemas que são aparentemente simples. Dessa maneira, [17] aponta a Teoria dos Números como uma ferramenta para outros campos da Matemática assim como os conhecimentos e ferramentas desses campos são utilizados na resolução de seus problemas ao mesmo tempo em que tem como foco resolver os mistérios dos números e, para isso são utilizados métodos algébricos, métodos analíticos ou também métodos geométricos.

Neste capítulo, vamos propor algumas atividades aplicáveis aos Ensinos Fundamental e Médio de modo a construir uma compreensão da simbologia de congruência e, consequentemente analisar os resíduos quadráticos, além de fazer uma associação com a Criptografia, em particular ao Método de Rabin, através da orientação de [1].

3.1 Atividade 1 – A Utilização da Simbologia de Congruência e os Resíduos Quadráticos

Neste trabalho, estudamos que a congruência $x^2 \equiv a \ (mod\ m)$ apresentará solução se a for um resíduo quadrático módulo m, com $(a, m) = 1$. Caso contrário, ela não possuirá solução. Então, vamos desenvolver uma linguagem acessível aos alunos

do Ensino Médio para que possa realizar um ensino de Matemática mais dinâmico e que os educandos participem ativamente de sua aprendizagem.

Atividade

(i) Encontre os restos da divisão de 10^2 por 7, 89^2 por 11 e 125^2 por 19.

(ii) Agora, se escrevermos $10^2 \equiv 2 \ (mod\ 7)$, $89^2 \equiv 1 \ (mod\ 11)$ e $125^2 \equiv 7 \ (mod\ 19)$. Qual seria a semelhança com o item anterior?

(iii) Podemos obter o conjunto dos possíveis restos de cada divisão do item (i)?

(iv) Mas, se agora escrevermos $x^2 \equiv a \ (mod\ m)$. Qual será a compreensão?

(v) Qual regularidade podemos observar do item (v)?

(vi) Agora, podemos explicar o porquê de $4^2 \equiv 3 \ (mod\ 13)$ e $9^2 \equiv 3 \ (mod\ 13)$ apresentar como resultado o mesmo resíduo quadrático, ou seja, o valor de 3 como resposta?

(vii) Já com todos esses conhecimentos abordados, pode−se verificar os casos em que há solução para a congruência $x^2 \equiv a \ (mod\ 7)$?

Objetivo Geral

$*$ Desenvolver a linguagem de congruência e a noção de resíduos quadráticos, no Ensino Médio, como forma de contribuir para a expansão dos conhecimentos matemáticos dos educandos.

Objetivos Específicos

$*$ Obter o resto de uma divisão, envolvendo potências quadradas, em que identificaremos o conjunto dos possíveis restos;

$*$ Associar que a congruência $x^2 \equiv a \ (mod\ n)$ descreve uma nova possibilidade de escrita em que a é o resto da divisão de x^2 por n;

$*$ Conceituar a congruência $x^2 \equiv a \ (mod\ n)$;

$*$ Detectar as regularidades no sistema reduzido de resíduos quadrados;

$*$ Verificar se a congruência $x^2 \equiv a \ (mod\ n)$ possui ou não solução, ou seja, se é ou não resíduo quadrático.

Público−Alvo e Materiais

Esta atividade possui como público alvo os discentes do Ensino Médio onde

consideraremos seus conhecimentos prévios sendo preciso saber das propriedades de números inteiros, em particular a divisão e a potenciação. Com relação aos materiais utilizados podemos destacar lápis, borracha, papel e cartolina para confecção de cartazes.

Comentários

Com essa atividade o professor conseguirá completamente atribuir um significado a esse conhecimento matemático aperfeiçoando a aprendizagem de seus alunos. A seguir, propomos a interpretação das questões abordadas.

(i) O aluno que possui uma percepção das propriedades dos números inteiros, particularmente na divisão interligada à potenciação observará facilmente que as divisões de 10^2 por 7, 89^2 por 11 e 125^2 por 19 apresentam como restos 3,1 e 11, respectivamente tendo que efetuar primeiramente a potenciação e, em seguida a divisão.

(ii) Nesta fase, é fundamental que o professor enfatize que a escrita de congruência do tipo $x^2 \equiv a \ (mod \ n)$ representa uma alternativa mais elaborada. Também, deve−se expressar que mesmo com a escrita diferenciada do item (i) exibe o mesmo significado.

(iii) Agora, ao entrarmos na Classe de Restos, ramo de estudo muito importante da Matemática pura chamado Teoria dos Números, que trata do estudo dos números inteiros, os alunos deverão perceber que ao efetuar uma divisão entre dois números (inteiros) poderão acontecer duas possibilidades:

* se a divisão for exata, o resto será igual a zero;

ou

* se a divisão não for exata, o resto será diferente de zero.

Com a divisão exata, o resultado é evidente. Mas, caso a divisão não seja exata, deveremos refletir nas possibilidades de valores (inteiros) para o resto. Então, se dividirmos qualquer número (inteiro) por 2 tem−se os seguintes restos: zero (divisão exata) ou 1. Isto, porque se o resto (r) for um número maior ou igual a 2 ($r \geq 2$) podemos continuar com a divisão. Assim, o conjunto dos possíveis restos da divisão por 2 será $r(2) = 0, 1$.

Já quando dividirmos qualquer número (inteiro) por 3 poderemos ter os seguintes

restos: zero (a divisão é exata), 1 ou 2. Por essa mesma razão, se o resto for maior ou igual a 3 ($r > 3$) podemos continuar com a divisão. Então, o conjunto dos possíveis restos da divisão por 3 será: $r(3) = 0, 1, 2$.

E a partir destes resultados podemos conjecturar n como um inteiro não−nulo, em que o conjunto dos possíveis restos de uma divisão por n será: $r(n) = \{0, 1, 2, 3, \ldots, n-1\}$. Dessa maneira, o aluno conseguirá perceber que a divisão por 7 possui como restos possíveis o conjunto $r(7) = \{0, 1, 2, 3, 4, 5, 6\}$, a divisão por 11 terá $r(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ e por 19 o conjunto $r(19) = \{0, 1, 2, 3, 4, 5, 6, \ldots, 16, 17, 18\}$.

(iv) Os estudantes já poderão ter a consciência que se trata de um valor x^2, com $x \in \mathbb{Z}$, que ao ser dividido por m obteremos o resto a. No entanto, a será a classe residual de m, ou seja, $r(a) = \{0, 1, 2, 3, 4, \ldots, n-1\}$.

(v) O aluno já sabe que $r(13) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ e portanto terá elevar ao quadrado cada resto e, em seguida efetuar a divisão por 13. Logo,

$$1^2 \equiv 1 \ (mod\ 13) \qquad 7^2 \equiv 10 \ (mod\ 13)$$
$$2^2 \equiv 4 \ (mod\ 13) \qquad 8^2 \equiv 12 \ (mod\ 13)$$
$$3^2 \equiv 9 \ (mod\ 13) \qquad 9^2 \equiv 3 \ (mod\ 13)$$
$$4^2 \equiv 3 \ (mod\ 13) \qquad 10^2 \equiv 9 \ (mod\ 13)$$
$$5^2 \equiv 12 \ (mod\ 13) \qquad 11^2 \equiv 4 \ (mod\ 13)$$
$$6^2 \equiv 10 \ (mod\ 13) \qquad 12^2 \equiv 1 \ (mod\ 13)$$

Ao colocar os quadrados dos números de 1 até 12 obtemos apenas 6 números 1,3,4,9,10, e 12. Estes serão todos resíduos quadráticos módulo 13 em que os números na metade superior se repetem na metade inferior, se referindo ao Teorema 1.2.

(vi) O aluno deverá observar que $4^2 \equiv (13-4)^2 = 9^2 \equiv 3 \ (mod\ 13)$. Dessa maneira já terá condições de verificar a veracidade do Teorema 1.1 em que para n um primo ímpar e a um inteiro não divisível por n, a congruência $x^2 \equiv a \ (mod\ n)$, caso tenha solução, tem exatamente duas soluções incongruentes modulo n.

(vii) Com a congruência $x^2 \equiv a \ (mod\ n)$, em que $(a, n) = 1$ e $x^2 - a$ é divisível por n, teremos consequentemente, pelo Pequeno Teorema de Fermat, (Anexo B), que $a^{n-1} - 1$ é divisível por n. Então, podemos afirmar que $(a^{\frac{n-1}{2}})^2 - 1$ também será divisível por n e como $(a^{\frac{n-1}{2}})^2 - 1 = (\mathrm{a}^{\frac{n-1}{2}} - 1)(a^{\frac{n-1}{2}} + 1)$ temos que ou $(a^{\frac{n-1}{2}} - 1)$ será divisível por n ou $(a^{\frac{n-1}{2}} + 1)$ será divisível por n. Essa descoberta permite

concluir que se ocorrer a primeira situação a será resíduo quadrático de n, enquanto na segunda a não será resíduo quadrático de n.

Agora, para a congruência $x^2 \equiv a \ (mod\ 7)$ usaremos a consequência do Teorema 1.4, o Critério de Euler, como justificativa para verificar se há solução. Sendo $n = 7$ e $\frac{p-1}{2} = 3$, poderemos admitir que

$$1^3 \equiv 1 \ (mod\ 7) \qquad 4^3 \equiv 1 \ (mod\ 7)$$
$$2^3 \equiv 1 \ (mod\ 7) \qquad 5^3 \equiv -1 \ (mod\ 7)$$
$$3^3 \equiv -1 \ (mod\ 7) \qquad 6^3 \equiv -1 \ (mod\ 7)$$

As congruências $x^2 \equiv 1 \ (mod\ 7)$, $x^2 \equiv 2 \ (mod\ 7)$ e $x^2 \equiv 4 \ (mod\ 7)$ possuem solução por serem resíduos quadráticos à medida que $x^2 \equiv 3 \ (mod\ 7)$, $x^2 \equiv 5 \ (mod\ 7)$ e $x^2 \equiv 6 \ (mod\ 7)$ não terão solução. Com essa abordagem, o aluno saberá o procedimento de como obter resíduos quadráticos sem se tornar um ensino voltado a memorização de fórmulas em que o aluno será apenas reproduz o conhecimento e passará a ser sujeito de sua própria aprendizagem podendo notar que uma metade será resíduo quadrático já a outra não, Teorema 1.2. Por outro lado, empregaremos o Símbolo de Legendre, Definição 1.3, de uma maneira mais simplificada, ou seja, estamos adequando esta simbologia para alcançar uma aprendizagem mais expressiva no Ensino Médio.

3.2 Atividade 2 – A Congruência $x^2 \equiv a \ (mod\ n)$ e a Criptografia: Método de Rabin

Desde a antiguidade, os egípcios, gregos e romanos utilizavam técnicas tão inteligentes quanto criativas para enviar mensagens. Neste envio, eles as protegiam com códigos para prevenir que a informação possa ser interpretada por todos.

A evolução das tecnologias torna constante a preocupação de que o envio de mensagens seja cercado de meios capazes de codificar o conteúdo a fim de aumentar a segurança dos usuários. Para manter a proteção das informações temos a criptografia definida, segundo [13], como o estudo de técnicas matemáticas relacionadas aos aspectos da segurança da informação, como confidencialidade, integridade e autenticação. Também pode ser visto como a transformação de um conjunto de

informações inteligíveis, como os e-mails, por exemplo, em um emaranhado de caracteres impossíveis de ser compreendido, texto cifrado.

Assim, apenas quem tem a chave de decriptação é capaz de recuperar a mensagem em formato legível mesmo que a pessoa não autorizada conheça todo o processo para esconder e recuperar os dados não conseguirá descobrir a informação sem a chave de decriptação. Enfatizaremos, a seguir, os processos de Criptografia e Decifração.

(i) Amanda deseja mandar uma mensagem M para Bernardo;

(ii) Bernardo acha dois números primos grandes (100 algarismos cada um) p e q, em que a divisão deles por 4 apresenta 3 como resto;

(iii) Bernardo calcula $n = pq$ e envia o inteiro n para Amanda;

(iv) Cássio, que consideraremos como o invasor, também conhece n, mas em virtude do processo de fatoração ser custoso, nem Alice e nem Cássio conhecem os fatores p e q;

(v) Amanda forma o inteiro M convertendo e unindo suas palavras em representações numéricas pelo Método de Rabin;

(vi) Amanda calcula um valor a que compreende o resto da divisão de M^2 por n, e o envia para Bernardo. Cássio também consegue ver a;

(vii) Para decriptograr, Bernardo calcula as quatro raízes quadradas de N no intervalo $[0, 1, \ldots, n-1]$;

($viii$) O fato de Bernardo conhecer os fatores p e q de n permite calcular facilmente as raízes quadradas, gerando quatro raízes possíveis, em que apenas uma é a mensagem M, enviada por Amanda.

(ix) Das quatro mensagens geradas, três delas não terão sentido, então Bernardo terá que reconhecer a correta;

(x) Cássio não consegue decriptografar pelo motivo de não saber como descobrir as raízes quadradas.

Agora, vamos apresentar uma atividade com a intenção de descrever um criptossistema famoso que consagrou a história da criptografia, o método de Rabin, que é um dos criptossistemas de chave pública de mais fácil compreensão. Este sistema criptográfico, denotado por $E(M) = M^2 \ (mod\ n)$, foi proposto pelo israelense Michael Oser Rabin, em Janeiro de 1979, consiste em criptografar as mensagens mediante a elevação ao quadrado e decodificadar através da extração de raízes qua-

dradas. Os cálculos presentes nesse processo se verificam em p e q, números primos inteiros, em que a divisão por 4 deixa 3 como resto.

Atividade

Suponhamos que Amanda e Bernardo querem compartilhar uma mensagem sem que Cássio a desvende para conseguir isto, faremos uso do Método de Rabin. Então, Amanda deseja enviar a mensagem **MATEMÁTICA É VIDA** para ser criptografada (cifrada). Com isso, Bernardo deverá escolher os primos $p = 179$ e $q = 43$ de forma que $n = p \cdot q = 7697$ e a envia para Amanda. Como n é a chave pública e $(179, 43)$ a chave privada, criptografe a letra **M** do vocábulo **MATEMÁTICA**, com o auxílio da tabela abaixo.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

s	t	u	v	w	x	y	z	_	0	1	2	3	4	5	6	7	8	9
28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46

Figura 3.1: Tabela de Conversão

Objetivo Geral

∗ Compreender a Criptografia, particularmente o Método de Rabin, como uma estratégia capaz de transformar uma mensagem de sua forma original para outra ilegível.

Objetivos Específicos

∗ Constatar que, na Criptografia, apenas o destinatário conhece a informação enviada, mantendo a sua segurança;

∗ Criptografar uma mensagem pelo Método de Rabin;

∗ Verificar que quem calcula o valor a é o remetente e envia para o destinatário, enquanto que o invasor também consegue ver a;

∗ Definir Sistema Binário e Sistema Decimal;

∗ Transformar um valor numérico em base binária para base decimal e vice−versa;

∗ Representar a congruência $x^2 \equiv a \ (mod \ n)$ como um $x \in \mathbb{Z}$ em que a será o resto da divisão de x^2 por n.

Público−Alvo e Materiais

Esta atividade contempla os números primos, as operações com números inteiros: adição, multiplicação, divisão e potenciação, sistema base 2 e decimal. Também foi desenvolvida para educando do Ensino Médio, envolvendo materiais como papel, lápis, borracha, calculadora e computador.

Comentários

É possível que o alunado tenha alguma dificuldade de identificar um número primo e de operar com os números inteiros o que vai exigir do professor aperfeiçoar estes conhecimentos matemáticos para, em seguida investir no sistema binário e no decimal. Dessa maneira, deverá perceber, pela tabela 3.1, que **M** corresponde ao $m = 22$. Ele ao escrever 22 na representação binário obterá $0\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2 + 0\cdot 2^3 + 1\cdot 2^4$, ou seja, $(10110)_2$. Como $m = (10110)_2$, deveremos repetir os quatro últimos dígitos o que resultará em $m = (101100110)_2$ e, consequentemente m? será equivalente a 358 na forma decimal, ou seja, $m = (358)_{10}$ pois $358 = 2^8 + 2^6 + 2^5 + 2^2 + 2^1$. Portanto, Amanda ao elevar ao quadrado m e dividir 128164 por $n = 7697$ descobre como resto 5012, isto é, $a = 5012$, que corresponde ao valor enviado a Bernardo em que é conveniente ressaltar que Cássio, o invasor, conhece n e a. O mesmo não podemos dizer dos primos p e q que são do conhecimento apenas de Bernardo. De maneira análoga poderemos obter todas as letras do vocábulo em questão.

Apêndice A

Coletânea: Provas da Lei de Reciprocidade Quadrática

Trazemos aqui a coletânea de autores que contribuiram para a evolução da **Lei de Reciprocidade Quadrática** contendo 221 demonstrações, o ano e o método utilizado. A inspiração foi obtida por intermédio de [26].

AUTOR	ANO	MÉTODO
1. Legendre	1788	Formas Quadráticas; incompleto
2. Gauss 1	1801	Indução; 8 de Abril de 1796
3. Gauss 2	1801	Formas Quadráticas; 27 de Junho de 1796
4. Gauss 3	1808	Lema de Gauss; 6 de Maio de 1807
5. Gauss 4	1811	Ciclotomia; Maio de 1801
6. Gauss 5	1818	Lema de Gauss; 08/1807
7. Gauss 6	1818	Somas de Gauss; 08/1807
8. Cauchy	1829	Gauss 6
9. Jacobi	1830	Gauss 6
10. Dirichlet 1	1835	Gauss 4
11. Lebesgue 1	1838	$N(x_1^2 + \ldots + x_q^2 = 1 \ (mod\ p)$
12. Schönemann	1839	Equação Periódica Quadrática
13. Cauchy	1840	Gauss 4
14. Eisenstein 1	1844	Generalização da Soma de Jacobi

15. Eisenstein 2	1844	Gauss 6
16. Eisenstein 3	1844	Lema de Gauss
17. Eisenstein 4	1845	Seno
18. Eisenstein 5	1845	Produtos Infinitos
19. Liouville	1847	Ciclotomia
20. Lebesgue 2	1847	Lebesgue 1
21. Schaar	1847	Lema de Gauss
22. Plana 1	1852	
23. Genocchi 1	1852	Lema de Gauss
24. Schaar 2 2	1854	Gauss 4
25. Dirichlet 2	1854	Gauss 1
26. Genocchi 2	1854	Liouville
27. Schaar 3 3	1860	Gauss 4
28. Lebesgue 3	1860	Gauss 7, 8
29. Kummer 1	1862	Formas Quadráticas
30. Kummer 2	1862	Formas Quadráticas
31. Dedekind 1	1863	Formas Quadráticas
32. Gauss 7	1863	Formas Quadráticas; Set. 1796
33. Gauss 8	1863	Formas Quadráticas; Set. 1796
34. Mathieu	1867	Ciclotomia
35. Von Staudt	1867	Ciclotomia
36. Bouniakowski	1869	Lema de Gauss
37. Stern	1870	Lema de Gauss
38. Zeller	1872	Lema de Gauss
39. Zolotarev	1872	Permutações
40. Kronecker 1	1872	Zeller
41. Schering 1	1875	Gauss 3
42. Kronecker 2	1876	Indução
43. Mansion 1	1876	Lema de Gauss
44. Dedekind 2	1877	Gaus 6
45. Dedekind 3	1877	Soma de Dedekind
46. Pellet 1	1878	Stickelberger-Voronoi

47. Pepin 1	1878	Ciclotomia
48. Sochocki	1878	Funções Theta
49. Schering 2	1879	Lema de Gauss
50. Petersen	1879	Lema de Gauss
51. Genocchi 2	1880	Lema de Gauss
52. Kronecker 3	1880	Gauss 4
53. Kronecker 4	1880	Períodos Quadráticos
54. Voigt	1881	Lema de Gauss
55. Pellet 2	1882	Mathieu 1867
56. Busche 1	1883	Lema de Gauss
57. Gegenbauer	1 1884	Lema de Gauss
58. Kronecker 5	1884	Lema de Gauss
59. Kronecker 6	1885	Gauss 3
60. Kronecker 7	1885	Lema de Gauss
61. Bock	1886	Lema de Gauss
62. Lerch 1	1887	Gauss 3
63. Busche 2	1888	Lema de Gauss
64. Hacks	1889	Schering
65. Hermes	1889	Indução
66. Kronecker 8	1889	Lema de Gauss
67. Tafelmacher 1	1889	Stern
68. Tafelmacher 2	1889	Stern/Schering
69. Tafelmacher 3	1889	Schering
70. Busche 3	1890	Lema de Gauss
71. Franklin	1890	Lema de Gauss
72. Lucas	1890	Lema de Gauss
73. Pepin 2	1890	Gauss 2
74. Fields	1891	Lema de Gauss
75. Gegenbauer 2	1891	Lema de Gauss
76. Gegenbauer 3	1893	Lema de Gauss
77. Schmidt 1	1893	Lema de Gauss
78. Schmidt 2	1893	Lema de Gauss

79. Schmidt 3	1893	Indução
80. Gegenbauer 4	1894	Lema de Gauss
81. Bang	1894	Indução
82. Mertens 1	1894	Lema de Gauss
83. Mertens 2	1894	Somas de Gauss
84. Busche 4	1896	Lema de Gauss
85. Lange 1	1896	Lema de Gauss
86. Mansion 2	1896	Gauss 2
87. De la Vallee Poussin	1896	Gaus 2
88. Lange 2	1897	Lema de Gauss
89. Hilbert	1897	Ciclotomia
90. Alexejewsky	1898	Schering
91. Pepin 3	1898	Legendre
92. Pepin 4	1898	Gauss 5
93. Konig	1899	Indução
94. Fischer	1900	Resultantes
95. Takagi	1903	Zeller
96. Lerch 2	1903	Gauss 5
97. Mertens 3	1904	Eisenstein 4
98. Mirimanoff e Hensel	1905	Stickelberger-Voronoi
99. Cornacchia 5	1909	
100. Busche 5	1909	Zeller
101. Busche 6	1909	Eisenstein
102. Aubry	1910	Eisenstein 3
103. Aubry	1910	Voigt
104. Aubry	1910	Kronecker
105. Pepin 5	1911	Gauss 2
106. Petr 1	1911	Mertens 3
107. Pocklington	1911	Gauss 3
108. Dedekind 3	1912	Zeller
109. Heawood	1913	Geometria
110. Frobenius 1	1914	Zeller

111. Frobenius 2	1914	Geometria (Eisenstein)
112. Lasker	1916	Stickelberger-Voronoi
113. Cerone	1917	Eisenstein 4
114. Bartelds e Schuh	1918	Lema de Gauss
115. Stieltjes	1918	Pontos Reticulares
116. Teege 1	1920	Legendre
117. Teege 2	1921	Ciclotomia
118. Arwin	1924	Formas Quadráticas
119. Rédei 1	1925	Lema de Gauss
120. Rédei 2	1926	Lema de Gauss
121. Whitehead	1927	Teoria da Classe (Kummer)
122. Petr 2	1927	Funções Theta
123. Skolem 1	1928	Teoria da Classe
124. Petr 3	1934	Kronecker (sinais)
125. van Veen	1934	Geometria (Eisenstein)
126. Fueter	1935	Álgebras de Quatérnios
127. Whiteman	1935	Lema de Gauss
128. Dockeray	1938	Eisenstein 3
129. Dörge	1942	Lema de Gauss
130. Rédei 3	1944	Gauss 5
131. Lewy	1946	Ciclotomia
132. Petr 4	1946	Ciclotomia
133. Skolem 2	1948	Gauss 2
134. Barbilian	1950	Eisenstein 1
135. Rédei 4	1951	Gauss 3
136. Brandt 1	1951	Gauss 2
137. Brandt 2	1951	Somas de Gauss
138. Brewer	1951	Mathieu, Pellet
139. Furquim de Almeida	1951	Corpos Finitos
140. Zassenhaus	1952	Corpos Finitos
141. Riesz	1953	Permutações
142. Fröhlich	1954	Teoria do Campo de Classe

143. Ankeny	1955	Ciclotomia
144. D.H. Lehmer	1957	Lema de Gauss
145. C. Meyer	1957	Somas de Dedekind
146. Holzer	1958	Somas de Gauss
147. Rédei 5	1958	Ciclotomia Polinomial
148. Reichardt	1958	Gauss 3
149. Carlitz	1960	Gauss 1
150. Kubota 1	1961	Ciclotomia
151. Kubota 2	1961	Somas de Gauss (seno)
152. Skolem 3	1961	Ciclotomia
153. Skolem 4	1961	Corpos Finitos
154. Hausner	1961	Somas de Gauss
155. Swan 1	1962	Stickelberger-Voronoi
156. Gerstenhaber	1963	Eisenstein, seno
157. Koschmieder	1963	Eisenstein, seno
158. Rademacher	1964	Análise de Fourier Finita
159. Weil	1964	Funções Theta
160. Kloosterman	1965	Holzer
161. Chowla	1966	Corpos Finitos
162. Burde	1967	Lema de Gauss
163. Kaplan 1	1969	Eisenstein
164. Kaplan 2	1969	Congruências Quadráticas
165. Birch	1971	K-grupos (Tate)
166. Reshetukha	1971	Somas de Gauss
167. Agou	1972	Corpos Finitos
168. Brenner	1973	Zolotarev
169. Honda	1973	Somas de Gauss
170. Milnor e Husemöller	1973	Weil 1964
171. Allander	1974	Lema de Gauss
172. Berndt e Evans	1974	Lema de Gauss
173. Hirzebruch e Zagier	1974	Somas de Dedekind
174. Rogers	1974	Legendre

175. Castaldo	1976	Lema de Gauss
176. Springer	1976	Lema de Gauss
177. Frame	1978	Kronecker (sinais)
178. Hurrelbrink	1978	K-teoria
179. Auslander e Tolimieri	1979	Transformação de Fourier
180. Corro	1980	Somas de Gauss
181. Brown	1981	Gauss 1
182. Goldschmidt	1981	Ciclotomia
183. Kac	1981	Eisenstein, seno
184. Barcanescu	1981	Zolotarev
185. Zantema	1983	Grupos de Brauer
186. Ely	1984	Lebesgue 1
187. Eichler	1985	Funções Theta
188. Barrucand e Laubie	1987	Stickelberger-Voronoi
189. Peklar	1989	Lema de Gauss
190. Barnes	1990	Zolotarev
191. Swan 2	1990	Ciclotomia
192. Rousseau 1	1990	Álgebras Exterior
193. Rousseau 2	1991	Permutações
194. Keune	1991	Corpos Finitos
195. Kubota 3	1992	Geometria
196. Russinoff	1992	Lema de Gauss
197. Garrett	1992	Weil 1964
198. Motose	1993	Álgebras de Grupo
199. Rousseau 3	1994	Zolotarev
200. Young	1995	Somas de Gauss
201. Brylinski	1997	Açoes de Grupos
202. Merindol	1997	Eisenstein, seno
203. Watanabe	1997	Zolotarev
204. Ishii	1998	Gauss 4
205. Motose	1999	Álgebras de Grupo
206. Zahidi	2000	Stickelberger-Voronoi

207. Lemmermeyer	2000	Lebesgue 1, Ely
208. Meyer	2000	Somas de Dedekind
209. Tangedal	2000	Eisenstein, Geometria
210. Chapman	2001	Sequências Recorrentes
211. Hammick	2001	Rousseau 2
212. Girstmair	2001	Eichler
213. Murty	2001	Schur
214. Luo	2003	Rousseau
215. Motose 2	2003	Schur
216. Motose 3	2003	Schur
217. Sey Yoon Kim	2004	Rousseau 2
218. Sun	2004	Lema de Gauss
219. Duke e Spears	2005	Grupos
220. Murty e Pacelli	2005	Funções Theta
221. Szyjewski	2005	Zolotarev

Apêndice B

Pequeno Teorema de Fermat, Teorema de Wilson e Teorema do Resto Chinês

Apresentaremos a seguir demonstrações e exemplificações de teoremas bastante úteis para o estudo das Congruências Quadráticas e para a Lei de Reciprocidade Quadrática. Estas demonstrações foram inspiradas em [3],[5],[7], [21] e [22].

B.1 Pequeno Teorema de Fermat

Este teorema já era conhecido desde a antiguidade em que os chineses, por exemplo, sabiam que se p é primo então p divide $2^{p-1}-1$. [3] afirma que foi Fermat quem desvendou o resultado geral e o propagou na matemática européia do século XVII aplicando a linguagem de congruências à maneira moderna de enunciar o teorema.

Teorema de Fermat: Seja p um número primo. Se $p \nmid a$, então $a^{p-1} \equiv 1 \ (mod\ p)$.

Demonstração: Como o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ compõe um sistema completo de resíduos módulo p teremos que qualquer conjunto compreendendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjuntos de $\{0, 1, 2, \ldots, p-1\}$. Vamos, agora, considerar os $p-1$ números múltiplos de a, isto é, os inteiros $a, 2a, 3a, \ldots, (p-$

$1)a$. Sabendo que, pelo fato de que p não divide a, $(a,p) = 1$ e, portanto nenhum dos números deste conjunto é divisível por p. Além disso, dois quaisquer deles são incongruentes módulo p, pois se fosse

$$ra \equiv sa \ (mod\ p), 1 \leq r < s \leq p-1$$

poderemos cancelar o fator comum a e teríamos $r \equiv s \ (mod\ p)$. Isto só é possível se $r = s$, já que ambos r e s são positivos e menores do que p. Temos, portanto, um conjunto de $p-1$ incongruentes módulo p e não−divisíveis por p. Então, cada um deles é congruente a exatamente um dentre os elementos $1, 2, \ldots, p-1$, e por conseguinte multiplicando ordenadamente todas essas $p-1$ congruências, teremos

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

ou seja,

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

Mas, como p é primo e p não divide $(p-1)!$, ou seja, $((p-1)!, p) = 1$, podemos cancelar o fator comum (p-1)!, o que resulta na congruência de Fermat:

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

□

Corolário: *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \ (mod\ p)$.*

Demontração: Temos que analisar dois casos, se $p \mid a$ e $p \nmid a$. Se $p \mid a$, então $a \equiv 0 \ (mod\ p)$ e $a^p \equiv 0 \ (mod\ p)$ o que implicará em $a^p \equiv a \ (mod\ p)$. Se, ao invés, $p \nmid a$ então, pelo Teorema de Fermat, $a^{p-1} \equiv 1 \ (mod\ p)$. Logo,

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

Portanto, em ambos os casos, $a^p \equiv a \ (mod\ p)$.

□

Exemplo: *Verificar o Teorema de Fermat com $a = 3$ e $p = 17$.*

Solução: O inteiro 17 é primo e 17 não divide 3. Então, $3^{17-1} = 3^{16}$ em que não é necessário calcular o número muito grande 3^{16}, pois teremos

$$3^3 = 27 \equiv 10 \ (mod\ 17)$$

o que resultará em

$$3^6 \equiv 100 \equiv -2 \ (mod\ 17) \text{ e } 3^{12} \equiv 4 \ (mod\ 17).$$

Então,

$$3^{17-1} = 3^{16} = 3^{12} \cdot 3^3 \cdot 3 \equiv 4 \cdot 10 \cdot 3 \equiv 120 \equiv 1 \ (mod\ 17).$$

O leitor pode encontrar em [22] outras provas distintas para o Pequeno Teorema de Fermat.

B.2 Teorema de Wilson

Vamos provar um teorema atribuído a Wilson (1741−1793), mas que, na verdade, foi provado, pela primeira vez, por Joseph Louis Lagrange (1736−1813).

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

Demonstração: O teorema é verdadeiro para $p = 2$ e $p = 3$, pois

$$(2-1)! = 1! = 1 \equiv -1 \ (mod\ 2)$$
$$(3-1)! = 2! = 2 \equiv -1 \ (mod\ 3).$$

Vamos, agora, supor para $p \geq 5$. Consideremos que a congruência $ax \equiv 1 \ (mod\, p)$ apresenta uma única solução para todo a no conjunto $\{1, 2, 3, \ldots, p-1\}$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, 4, \ldots, p-2$ em $\dfrac{p-3}{2}$ pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos $2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \ (mod\ p)$. Multiplicando ambos os lados desta congruência por $p-1$ obtemos

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

Então, $(p-1)! \equiv -1 \ (mod \ p)$ já que $p - 1 \equiv -1 \ (mod \ p)$.

□

O teorema a seguir nos fornece que se um número satisfaz a relação do teorema de Wilson, ele deve ser primo.

Teorema: *Se n é um inteiro tal que $(n-1)! \equiv -1 \ (mod \ n)$, então n é primo.*

Demonstração: Suponhamos que o inteiro n é composto. Então, n apresenta um divisor d de forma que $1 < d < n$. Também, como $d \leq n - 1$, segue−se que d é um dos fatores de $(n-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1)$. Portanto, $d \mid (n-1)!$. No entanto, por hipótese, $n \mid (n-1)! + 1$ de maneira que $d \mid (n-1)! + 1$. Portanto, $d \mid 1$, o que é um absurdo. Então, n é primo.

□

Exemplo: *Reconhecer se o inteiro 11 é primo.*

Solução:

$$(11-1)! + 1 = 10! + 1 = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 10 + 1 = 3628801 = 11329891$$

e, assim $(11-1)! \equiv -1 \ (mod \ 11)$. Logo, 11 é primo.

B.3 Teorema do Resto Chinês

O Teorema do Resto Chinês é um algoritmo para solucionar sistemas de congruências lineares. Este algoritmo é muito antigo e foi descoberto pelos chineses e pelos gregos com o intuito de resolver problemas de astronomia. Também, [3] afirma que o algoritmo do resto chinês apresenta este nome porque apareceu inicialmente no livro Manual de aritmética do mestre Sun, escrito entre 287 d.C. e 473 d.C e, posteriormente o mesmo resultado é mencionado na Aritmética de Nicômaco de Gerasa.

Teorema do Resto Chinês: *Se $(a_i, m_i) = 1, (m_i, m_j) = 1$ para $i \neq j$ e c_i*

inteiro, então o sistema

$$\begin{aligned} a_1x &\equiv c_1 \ (mod\ m_1) \\ a_2x &\equiv c_2 \ (mod\ m_2) \\ a_3x &\equiv c_3 \ (mod\ m_3) \\ &\vdots \\ a_rx &\equiv c_r \ (mod\ m_r) \end{aligned}$$

possui solução e a solução é única módulo m, onde $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.

Demonstração: O fato $(a_i, m_i) = 1$ nos afirma que $a_1x \equiv c_1 \ (mod\ m_1)$ contém uma única solução que denotamos por b_i. Se estabelecermos $y_i = \dfrac{m}{m_i}$ em que, $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$, teremos $(y_i, m_i) = 1$, pois $(m_i, m_j) = 1$ para $i \neq j$.Assim, cada uma das congruências $a_rx \equiv c_i \ (mod\ m_i)$ apresenta uma única solução que denotaremos por $\overline{y_i}$ e, então $y_i\overline{y_i} \equiv 1 \ (mod\ m_i), i = 1, 2, \ldots, r$. Ao afirmarmos que o número x dado por

$$x = b_1y_1\overline{y_1} + b_2y_2\overline{y_2} + \cdots + b_ry_r\overline{y_r}$$

é uma solução simultãnea para o nosso sistema de congruência. Consequentemente,

$$\begin{aligned} a_ix &= a_ib_1y_1\overline{y_1} + a_ib_2y_2\overline{y_2} + \cdots + a_ib_iy_i\overline{y_1} + \cdots + a_ib_ry_r\overline{y_r} \\ &\equiv a_ib_iy_i\overline{y_i} \ (mod\ m_i) \equiv a_ib_i \equiv c_i \ (mod\ m_i) \end{aligned}$$

já que y_i é divisível por m_i para $i \neq j$, $y_i\overline{y_i} \equiv 1(modm_i)$ e b_i é solução de $a_ix \equiv c_i \ (mod\ m_i)$.

Em seguida, vamos demonstrar que esta solução é única módulo m. Caso $\overline{x}$ é uma outra solução para o sistema em questão, então $a_i\overline{x} \equiv c_i \equiv a_ix \ (mod\ m_i)$ e, como $(a_i, m_i) = 1$ obtemos $\overline{x} \equiv x \ (mod\ m_i)$. Portanto $m_i \mid (\overline{x} - x), i = 1, 2, \ldots, r$. No entanto, como $(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, \ldots, m_r].$$

Assim, $m_1, m_2, \ldots, m_r \mid (\overline{x} - x)$, ou seja, $\overline{x} \equiv x \ (mod\ m)$.

□

Exemplo: *Três satélites passarão sobre o Rio de Janeiro esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã.*

Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo 15 horas e o terceiro 19 horas. Determine quantas horas decorrerão, a partir da meia−noite, até que os três satélites passem ao mesmo tempo sobre o Rio.

Solução: Vamos formular este problema de maneira matemática. Chamaremos de x o número de horas, contadas a partir da meia−noite de hoje, quando os tês passarão juntos sobre o Rio. O primeiro satélite passa sobre o Rio a cada 13 horas, a contar da 1 da madrugada. Isto é equivalente a dizer $x \equiv 1 \ (mod\ 13)$. Aplicando para os outros satélites obtemos

$$x \equiv 4 \ (mod\ 15) \text{ e } x \equiv 8 \ (mod\ 19).$$

Para saber qual o horário exato de passagem dos três satélites, devemos encontrar o valor de x que satisfaça as três equações simultaneamente. Isto é, precisamos resolver o sistema

$$\begin{aligned} x &\equiv 1 \ (mod\ 13) \\ x &\equiv 4 \ (mod\ 15) \\ x &\equiv 8 \ (mod\ 19) \end{aligned}$$

Os módulos 13,15 e 19 das congruências do sistema dado são primos entre si dois a dois, de maneira que o sistema tem uma única solução módulo $m = 13 \cdot 15 \cdot 19 = 3705$. Então,

$$M_1 = \frac{m}{13} = 285,\ M_2 = \frac{m}{115} = 247\ ,\ M_3 = \frac{m}{19} = 195.$$

As congruências lineares

$$\begin{aligned} 285x &\equiv 1 \ (mod\ 13) \Rightarrow 12x \equiv 1 \ (mod\ 13) \\ 247x &\equiv 1 \ (mod\ 15) \Rightarrow 7x \equiv 1 \ (mod\ 15) \\ 195x &\equiv 1 \ (mod\ 19) \Rightarrow 5x \equiv 1 \ (mod\ 19) \end{aligned}$$

tem como soluções $x_1 = 12, x_2 = 13, x_3 = 4$. Logo,

$$X = 1 \cdot 285 \cdot 12 + 4 \cdot 247 \cdot 13 + 8 \cdot 195 \cdot 4 = 22504.$$

Como $22504 \equiv 274 \ (mod\ 3705)$, segue−se que $X \equiv 274 \ (mod\ 3705)$ é a única solução do sistema de congruências lineares dado.

Referências Bibliográficas

[1] BIASE, Adriele Giareta and AGUSTINI, Edson.*Criptografias El-Gamal, Rabin e algumas técnicas de ciframento*. Disponível em http://www.portal.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/famat.revista.13.artigo4.0.pdf. Acesso em 28 de Junho de 2013.

[2] BOYER, C. B. and MERZBACH U. C. *A History of Mathematics*. John Wiley Sons, Inc., San Francisco, CA, 1991.

[3] COUTINHO, S.C. *Números inteiros e Criptografia RSA*. Coleção Matemática e Aplicações. 2. ed. Rio de Janeiro: IMPA, 2005.

[4] ELVIDGE, Sean. *The History of the Law of Quadratic Reciprocity*. The University of Birmingham School of Mathematics. Disponível em http://seanelvidge.com/wp-content/uploads/2011/04/HistoryQR.pdf. Acesso em 27 de Fevereiro de 2013.

[5] FILHO, Edgar de Alencar. *Teoria Elementar dos Números*. 3. ed. São Paulo: Nobel, 1992.

[6] FLOSE, Vania Batista Schunck. *Criptografia e Curvas Elípticas*. Dissertação de Mestrado. Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas. Rio Claro: Novembro de 2011.

[7] HEFEZ, Abramo. *Elementos de Aritmética*. Textos Universitários. 2. ed. Rio de Janeiro: IMPA, 2011.

[8] KIM, S.Y. *An Elementary Proof of the Quadratic Reciprocity Law Amer*. Math. M onthly 1 11 (2004), no. 1, 48-50.

[9] LEMMERMEYER, Franz. *Reciprocity Laws: From Euler to Eisenstein*, chapter 1, pages 1−27. Springer, Berlin, Germany, 2000.

[10] LINDAHL, Lars-Ake. Lectures on Number Theory. Disponível em http://www2.math.uu.se/ lal/kompendier/Talteori.pdf. Acesso em 12 de Março de 2013.

[11] MARTINEZ, Fabio Brochero Martinez; et al. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro: IMPA, 2010.

[12] MELQUIADES, José A. Rodriguez NOLE, Teresa Bracamonte. *Álgebra universal para la Ciencia de la Computación: Aplicación a la Criptofrafía*. Universidad Nacional de La Libertad. Facultad de Ciencias Fisicas y Matemáticas. Departamento de Informática. Trujillo, Peru: 2009.

[13] MENEZES, Alfred J.; et al. *Handbook of Applied Cryptography*.119.CRC Press, 1997.

[14] MOTA, Marcelo Lisboa. *Lei da Reciprocidade Quadrática*. Disponível emhttp://www.ime.unicamp.br/ ftorres/ENSINO/MONOGRAFIAS/LRQMM.pdf. Acesso em 04 de Março de 2013.

[15] NETO, Afonso Comba de Araújo. *Um algoritmo de Criptografia de Chave Pública semanticamente Seguro Baseado em Curvas Elípticas*. Dissertação de Mestrado em Ciência da Computação. Universidade Federal do Rio Grande do Sul. Instituto de Informática. Porto Alegre: Abril de 2006.

[16] POTTER, Harrison. *The Historical Development of the Law of Quadratic Reciprocity*. History of Mathematics. April of 2007. Disponível em http://people.duke.edu/ hdp2/MathHistory2.pdf. Acesso em 12 de Fevereiro de 2013.

[17] RESENDE, Marilene Ribeiro. *Buscando significados para a Teoria dos Números como saber a ensinar na Licenciatura em Matemática*. Disponí-

vel em www.sbem.com.br/files/ix-enem/...Cientifica/.../CC16109783668T.doc. Acesso em 20 de Maio de 2013.

[18] ROSEN, Kenneth H. *Elementary Number Theory and lts Applications*. 5. ed. Estados Unidos da América: Addison Wesley, 1986.

[19] SAID, Sidki. *Introdução à Teoria dos Números*. Coloquio Brasileiro de Matematica, IMPA, 1975.

[20] SANTOS, Jorge Manuel Lopes. *O uso de cifragem para proteção de canais abertos*. Dissertação de Mestrado em Ensino da Matemática. Departamento de Matemática Pura, Faculdade de Ciências da Universidade do Porto. Porto: Setembro de 2002.

[21] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. Coleção Matemática Universitária. 3. ed. Rio de Janeiro: IMPA, 2011.

[22] SCHEINERMAN, Edward R. *Matemática Discreta:* Uma Introdução. São Paulo: Cengage Learning, 2011.

[23] SILVA, Otoniel Nogueira da CÂMARA, Marcos Antônio da. *O Problema de Waring e o Teorema de Lagrange*. Famat em Revista. Faculdade de Matemática−FAMAT. Universidade Federal de Uberlândia−UFU. v. 11. Uberlândia: Outubro de 2008.

[24] http://w3.math.uminho.pt/site/files/historicooutros/1597Capitulo4(congruencias quadraticas).pdf?PHPSESSID=ec35bfc49dbcb46d7e1cde4f29ed73a7. *Congruências Quadráticas*. Acesso em 16 de Março de 2013.

[25] http://www.ime.unicamp.br/ ftorres/ENSINO/MONOGRAFIAS/LRQRoberta.pdf. *Lei da Reciprocidade Quadrática*. Acesso em 09 de Março de 2013.

[26] http://www.rzuser.uni-heidelberg.de/ hb3/rchrono.html. *Proofs of the Quadratic Reciprocity Law*. Acesso em 20 de Fevereiro de 2013.

[27] http://www.witno.com/numbers/chap6.pdf. *Quadratic Residues*. Acesso em 10 de Março de 2013.