Universidade Estadual de Campinas

Instituto de Matemática, Estatística e Computação Científica

Departamento de Matemática

Dissertação de Mestrado

FATORAÇÃO DE INTEIROS E GRUPOS SOBRE CÔNICAS

por

Vera Lucia Graciani de Souza

Mestrado Profissional em Matemática - Campinas - SP

Orientador: Prof. Dr. Martinho da Costa Araújo

Março de 2009

FATORAÇÃO DE INTEIROS E GRUPOS SOBRE CÔNICAS

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Vera Lucia Graciani de Souza
e aprovada pela comissão julgadora.

Campinas, 06 de março de 2009.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca Examinadora:

1. Prof. Dr. Martinho da Costa Araújo
2. Prof. Dr. José Plínio de Oliveira Santos
3. Prof. Dr. Trajano Pires da Nóbrega Neto

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues CRB8a / 2116

Souza, Vera Lucia Graciani de
So89f Fatoração de inteiros e grupos sobre cônicas / Vera Lucia Graciani de Souza -- Campinas, [S.P. :s.n.], 2009.

Orientador : Martinho da Costa Araujo
Trabalho final (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Corpos algébricos. 2. Teoria da reciprocidade. 3. Teoria dos números. 4. Fatoração (Matemática). 5. Algoritmos. I. Araújo, Martinho da Costa. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Interger fatorization and groups on conics.

Palavras-chave em inglês (Keywords): 1. Algebraic fields. 2. Reciprocity theorems. 3. Number theory. 4. Fatorization. 5. Algorithms (Mathematics).

Área de concentração: Matemática

Titulação: Mestre em Matemática

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo (UFMT)
Prof. Dr. José Plinio de Oliveira Santos (IMECC/UNICAMP)
Prof. Dr. Trajano Pires da Nóbrega Neto (UNESP/SJRP)

Data da defesa: 06/03/2009

Programa de pós-graduação: Mestrado Profissional em Matemática

Dissertação de Mestrado Profissional defendida em 06 de março de 2009 e Aprovada pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). MARTINHO DA COSTA ARAÚJO

Prof. (a). Dr (a). TRAJANO PIRES DA NÓBREGA NETO

Prof. (a). Dr (a). JOSÉ PLINIO DE OLIVEIRA SANTOS

Àqueles que enxergam nas ciências a possibilidade de um mundo melhor.

"Os ideais que iluminaram meu caminho e sempre me deram coragem para enfrentar a vida com alegria foram a Verdade, a Bondade e a Beleza."
(Albert Einstein)

Agradecimentos

- A Deus, o maior de todos os mestres pelos ensinamentos da vida, pela presença e força em todos os momentos em que precisei.
- À professora Sueli, pela paciência, pelo apoio e principalmente pelo profissionalismo com que conduziu a coordenação desse curso.
- Ao professor Martinho, meu orientador e amigo. Pela dedicação que tem me dispensado, pelos estímulos e paciência.
- À professora Zoraide, pela imensa colaboração durante todo o curso. Pela amizade, incentivo e apoio.
- Aos professores Edson, José Plinio,Luiz Mariano, às professoras Sandra,Rosane, Vera.
- Aos idealizadores desse projeto, professores, orientadores, monitores e colaboradores por terem acreditado e realizado esse curso.
- A todos meus amigos e parentes, muitos dos quais torceram bastante para que este momento se concretizasse. Em especial às minhas filhas Tarcila e Oriane e meu companheiro Barbosa.
- Aos amigos do mestrado, em especial Joseane, Donizete, Giseli, Luciana, Vera, Anderson, Cristiano, Fernando, Ludio. A amizade de cada um de vocês é muito importante.
- Aos amigos Aquiles, Itiho, José Luiz Marcio, Provenzano, William, Aurélia, Edina, Herice, dentre outros igualmente amados.

Resumo

SOUZA, Vera Lucia Graciani. *Fatoração de inteiros e grupos sobre cônicas*. Campinas - SP: Universidade Estadual de Campinas, 2009. Dissertação apresentada como requisito parcial para obtenção do Título de Mestre em Matemática.

Este trabalho tem por objetivo fatorar número inteiro utilizando pontos racionais sobre o círculo unitário. Igualmente pretende determinar alguns grupos sobre cônicas. A pesquisa inicia com os conceitos básicos de Álgebra e Teoria dos Números, que fundamentam que o conjunto de pontos racionais sobre o círculo unitário tem uma estrutura de grupo. Desse conjunto é possível estender a idéia de grupo de pontos racionais sobre o círculo para pontos racionais sobre cônicas. Para encontrar os pontos racionais sobre o círculo foi usada uma parametrização do círculo por funções trigonométricas. Para cada ponto sobre o círculo unitário está associado um ângulo com o eixo positivo das abscissas, portanto adicionar pontos sobre o círculo equivale adicionar seus ângulos correspondentes. Com a operação "adição" de pontos sobre o círculo é possível definir uma estrutura de grupo que é utilizada para fatorar números inteiros. Para a cônica, a operação "adição" é determinada algebricamente ao calcular o coeficiente angular da reta que passa por dois pontos dados e o elemento neutro dessa cônica, também justificada geometricamente. No trabalho foram determinados os grupos de pontos racionais sobre cônicas e demonstrado alguns resultados sobre esses grupos usando os resíduos quadráticos e finalizando com a dedução de alguns resultados sobre a soma das coordenadas dos pontos sobre uma cônica.

Palavras-Chave: Reciprocidade quadrática, Fatoração de número inteiro, Grupo de pontos racionais sobre cônicas.

Abstract

SOUZA , Vera Lucia Graciani. *Interger factoration and groups on conics*. Campinas - SP: Universidade Estadual de Campinas, 2009. Dissertation presented as partial requisite for the Mathematic tittle of Master obtention.

The objective of this paper is to factorize integer number using rational points on the unitary circle. Also, it intends to determinate some groups on the conics. The research begins with the basic concepts of Algebra and Number Theory ensuring that the rational points set on the unitary circle has a structure of group. From this set is possible to extend the idea of rational points on the circle toward rational points on conics. In order to find the rational points on the circle a parametrization by trigonometric function on it was used. For each point on the unitary circle it is associated an angle with abscissa positive axis, therefore adding points on the circle equals to add its corresponding angles. With the operation of "addition" points on the circle it is possible to define a group structure that is used to factorize integer numbers. For the conic, the "addition" operation is algebraically determinated when the angle coefficient of the line is calculated that joins two given points and the neutral element of that conic, which is geometrically justified. In the research the rational points groups on the conics were determined, and some result on these groups using quadratic residues were demonstrated, and it was finalized with the deduction of some results concerning the coordinates sum of points on a conics.

Keywords: Quadratic Reciprocity, Fatorization of Integer Numbers, Rational Points Groups on Conics.

Sumário

Lista de Figuras

Lista de símbolos

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{R}$	Conjunto dos números reais
(a, b)	Máximo Divisor Comum de a e b
$(a, b) = 1$	Números relativamente primos
$(G, *)$	Grupo G
$\#(G)$	Cardinalidade ou ordem de G
$a \equiv b(mod n)$	Congruência módulo n
$\overline{a}$	Classe de equivalência de a
$\mathbb{H} \trianglelefteq \mathbb{G}$	H subgrupo normal de G
$\mathbb{G}/\mathbb{H}$	Grupo quociente de H em G
$\mathbb{Z}/n\mathbb{Z}$	Conjunto das classes residuais módulo n
$< p >$	Conjunto gerado por p
$\lfloor \frac{a_i}{p} \rfloor$	Maior inteiro $\leq \frac{a_i}{p}$
$\cong$	Isomorfo
$(K, *, \diamond)$	Anel
M_n	Número de Mersenne
$\mathbb{F}_q$	Corpo com q elementos
$\mathbb{F}_q^*$	$F_q - \{0\}$
$(\frac{a}{p})$	Símbolo de Legendre
$[\frac{m}{n}]$	Símbolo de Jacobi
(a, b, c)	Terno Pitagórico
$sinx$	Sen x
$C(\mathbb{Q})$	Círculo unitário com coordenadas racionais
$C(\mathbb{Z}/n\mathbb{Z})$	Círculo unitário com coordenadas em
$\mathbb{Z}/n\mathbb{Z}$	
$C(\mathbb{F}_p)$	Círculo unitário com coordenadas no corpo $\mathbb{F}_p$
$(\mathbb{Z}/p\mathbb{Z})\sqrt{x}$	Corpo Quadrático
$\oplus$	Operação adição de pontos sobre cônicas
$\mathfrak{C}_{p,a}(\mathbb{F}_p)$	Cônica com coordenadas no corpo $\mathbb{F}_p$

Introdução

O presente trabalho pretende definir uma estrutura de grupo para o conjunto dos pontos sobre o círculo unitário de centro $(0, 0)$ e generalizar para anel comutativo R arbitrário com identidade através de uma função bijetora de R no círculo $C(R)$, além de utilizar essa estrutura para construir um algorítmo de fatoração para números inteiros da forma $n^2 + (q^2 - 1)$. Para tanto, é necessário construir o conjunto de pontos racionais sobre determinadas cônicas em anéis, cujos elementos são classes de restos no anel $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Na Aritmética, principalmente na Teoria dos Números, os conceitos, proposições e teoremas devem ter uma apresentação logica e organizada, de modo que após a demonstração da teoria faz-se necessária sua aplicação.

Com efeito, a construção do conjunto de pontos sobre cônicas utiliza a congruência quadrática para resolver equações, equivalentemente para encontrar pontos racionais sobre cônicas racionais.

Recentemente, o Último Teorema de Fermat, enunciado nos seguintes termos: "É impossível separar um cubo em dois cubos, ou uma biquadrada em duas biquadradas, ou em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes", foi provado pelo matemático inglês Andrew Wiles em 1995. A prova é baseada na teoria de curvas elípticas, isto é, curvas definidas por equaçõe cúbicas.

Uma grande parte dessa teoria está embasada nas deduções algébricas no conjunto de pontos racionais sobre curvas. Tal conjunto tem uma estrutura de grupo, que é particularmente satisfeita pelas cônicas.

Neste contexto, a análise das cônicas revela-se primordial para posterior conhecimento de resultados sobre a estrutura de grupo para pontos racionais em curvas elípticas.

Inicia-se o estudo, no capítulo inaugural, com uma breve síntese de algumas definições, proposições e teoremas, considerados pré-requisitos para entendimento dos capítulos seguintes.

No segundo capítulo é apresentada uma abordagem dos resíduos quadráticos módulo um número primo, bem como o Critério de Euler para averiguar se um determinado número a é

um resíduo quadrático. O símbolo de Legendre e o Lema de Gauss são apresentados dentro de um contexto teórico matemático que subsidiam a demonstração do Teorema da Lei da Reciprocidade Quadrática de forma diferenciada, objeto de estudo do capítulo três.

O quarto capítulo analisa os pontos sobre cônicas cujas coordenadas pertencem a um anel de classe de resíduos módulo número primo.

Por meio de uma parametrização da cônica, propõe-se definir uma lei de grupo para o conjunto de pontos que satisfazem a equação desta. Para tanto, é necessário construir o conjunto de pontos racionais sobre determinadas cônicas em anéis, cujos elementos são classes de restos no anel $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

A pesquisa baseou-se em publicações tais como livros, jornais e textos científicos, sendo possível delinear o desenvolvimento do trabalho bem como determinar uma solução para o objeto de estudo. Este trabalho pretende ser uma contribuição para ampliar o conhecimento sobre as leis da reciprocidade quadrática e suas aplicações, com informação histórica e demonstrações diferenciadas acerca do tema proposto.

Capítulo 1

Fundamentos Algébricos

A Teoria dos números teve sua origem nas antigas civilizações da humanidade, com o marco inicial na obra "Os Elementos ", de Euclides (aprox. 300 a.C). A evolução de uma noção intuitiva dos números naturais para um conceito mais elaborado foi lenta e teve a contribuição de muitos matemáticos por vários séculos.

Um algorítmo é um processo de cálculo definido com precisão. O Algorítmo de Euclides para o Máximo Divisor Comum, calcula corretamente o $m.d.c(a, b)$ para quaisquer dois inteiros positivos a e b. Ao supor a e b dois números primos extremamente grandes, não é difícil multiplicar esses números, mas se fosse representado um produto $n = ab$ e se procurasse fatorar n usando a divisão por tentativas, exigiria um período de tempo longo, mesmo no mais rápido dos computadores.

Há algorítmos mais sofisticados para fatoração, mais rápidos do que a divisão por tentativas. Ao considerar o tempo para multiplicar dois números primos extremamente grandes, o tempo necessário para fatorar esse produto aumenta enormemente, isso significa que fatorar números muito grandes é difícil.

A idéia é encontrar um processo de fatoração de números inteiros grandes que seja relativamente fácil de ser executado, mas que utilize conhecimentos de Teoria dos Números, que recentemente tornou-se central no mundo da criptografia e da segurança dos computadores.

A relação de congruência de números (módulo n) desempenha papel fundamental na Teoria dos Números indispensável ao propósito de estudar um método de fatoração de número inteiro através de pontos sobre o círculo unitário que satisfaçam uma equação de congruência

módulo n.

A abordagem de alguns teoremas, proposições e conceitos é necessária como pré-requisito ao desenvolvimento da pesquisa.

Definição 1.1 *O máximo divisor comum de dois inteiros a e b (a ou b diferente de zero) denotado por* (a, b)*, é o maior inteiro que divide a e b.*

Definição 1.2 *Seja G um conjunto não vazio onde está definida uma operação entre pares de G, denotada por,*

$* : G \times G \to G$

$(x, y) \longmapsto x * y$

Dizemos que o par $(G, *)$ *é um grupo se as seguintes propriedades são satisfeitas:*

1. $(a * b) * c = a * (b * c)$ *para todos a, b, c em G (associatividade da operação *).*

2. Existe um elemento e em G tal que $a * e = e * a = a$*, para todo a G (existência de elemento neutro em relação a operação *).*

3. Para cada a em G, existe b em G tal que $a * b = b * a = e$ *(existência de simétrico de cada elemento de G em relação a operação *).*

Definição 1.3 *Se um grupo* $(G, *)$ *satisfaz a propriedade,*

$a * b = b * a$*, para todos a e* $b \in G$*, G é denominado grupo comutativo ou abeliano.*

Definição 1.4 *A ordem ou cardinalidade de um grupo G é o número de elementos de G, e denotamos por* $\#(G)$*.*

Definição 1.5 *Seja G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se H for êle próprio um grupo com a mesma operação de G.*

Proposição 1.1 *Seja* $(G, *)$ *um grupo e H um subconjunto não vazio de G. H é um subgrupo de G se, e somente se,*

Para todos a, b, em $H \Rightarrow a * b' \in H$ *onde b' é o simétrico de b.*

Definição 1.6 *Sejam G um grupo e H um subgrupo de G. Dado* $a \in G$*, o conjunto* $a * H = \{ a * h : h \in H\}$*, é chamado classe lateral à esquerda de H em G determinada por a.*

De modo semelhante, a classe lateral à direita de H em G é o conjunto formado por todos os elementos $h * a$ *com* $h \in H$ *e* $a \in G$*.*

Definição 1.7 *O conjunto de todas as classes laterais à esquerda (à direita) de H em G forma uma partição de G, a qual denotamos por* $\frac{G}{H}$.

Definição 1.8 *Seja G um grupo e H um subgrupo de G. Se* $a * H = H * a$ *para todo* $a \in G$. *H é denominado subgrupo normal de G e denota-se* $H \trianglelefteq G$.

Teorema 1.1 *Sejam G um grupo e H um subgrupo normal de G. O conjunto* $\frac{G}{H}$ *é um grupo com a operação* $(a*H)(b*H) = (a*b)H$, *para todos a, b em G. Denominado grupo quociente de G em H.*

Definição 1.9 *Seja* $n \geq 1$ *um número inteiro. Dados* $a, b \in \mathbb{Z}$, *dizemos que a é côngruo b, módulo n, se, e somente se,* $n \mid (b - a)$.
Denota-se; $a \equiv b \ (mod\ n)$.

Proposição 1.2 *A relação R de congruência módulo n sobre* $\mathbb{Z}$:
$x\ R\ y \iff x \equiv y \ (mod\ n)$, *onde* $n \in \mathbb{Z}$ *e* $n > 1$, *determina em* $\mathbb{Z}$ *um conjunto das classes de equivalência módulo R denominado conjunto quociente*$\mathbb{Z}/R$, *indicado por* $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Definição 1.10 *Sejam os grupos* $(G, *)$ *e* $(H, \diamond)$, *a aplicação* $f : G \to H$ *é um homorfismo de G em H se, e somente se,*
Para todos $x, y \in G \Rightarrow f(x * y) = f(x) \diamond f(y)$.

Definição 1.11 *Um anel R é um conjunto R munido de uma operação binária denotada por* $*$ *e de uma operação binária denotada por* $\diamond$ *que satisfazem as seguintes condições:*
1. $(R, *)$ *é um grupo comutativo;*
2. $(x \diamond y) \diamond z = x \diamond (y \diamond z)$, *para todos x, y, z* $\in R$.
3. A operação $\diamond$ *é distributiva em relação à operação* $*$
$x \diamond (y * z) = x \diamond y \ * x \diamond z$
$(x * y) \diamond z = x \diamond z \ * y \diamond z$

Definição 1.12 *Sejam os anéis* $(G, *, \Delta)$ *e* $(H, \diamond, \bullet)$, *a aplicação* $f : G \to H$ *é um homomorfismo de G em H se, e somente se,*
(i) *Para todos x, y em* $G \Rightarrow f(x * y) = f(x) \diamond f(y)$
(ii) *Para todos x, y em* $G \Rightarrow f(x \Delta y) = f(x) \bullet f(y)$.

Definição 1.13 *Dado um homomorfismo de anéis $f : G \to H$, o núcleo de f é o subconjunto $Nuc(f) \subset G$ definido por:*
$Nuc(f) = \{x \in G \text{ tal que } f(x) = 0_H$.

Definição 1.14 *Sejam G e H dois anéis quaisquer. Uma aplicação $f : G \Rightarrow H$ é um isomorfismo de G em H se*
(i) f é bijetora
(ii) f é um homomorfismo de G em H.

Definição 1.15 *Uma função f é $\mathbb{Z}$- periódica se $f(x) = f(x + z)$, para x no domínio de f e para algum $z \in \mathbb{Z}$.*

Definição 1.16 *Seja G um grupo. G é um grupo cíclico se existir $a \in G$ tal que*
$G =< a >= \{a^n : n \in \mathbb{Z}\}$.

Definição 1.17 *A ordem de um elemento a de um grupo G é o menor número inteiro positivo k tal que $a^k = e$.*
Denota-se $\circ(a)$.

Exemplo 1.1 *Dado $n \in \mathbb{N}$, definimos no conjunto $\mathbb{Z}_n = \{\overline{a} : a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, onde $\overline{a} = \{m \in \mathbb{Z} : m \equiv a \ mod \ n\} = \{a + kn : k \in \mathbb{Z}\}$, uma operação binária:*
$\overline{a} \oplus \overline{b} = \overline{a+b}$.
$(\mathbb{Z}_n, \oplus)$ *é um grupo gerado por* $\overline{1}$.

Teorema 1.2 *Teorema de Lagrange.*
Sejam G um grupo finito e H um subgrupo de G. Então a ordem de H divide a ordem de G.

Definição 1.18 *Um anel R é um conjunto R munido de uma operação binária denotada por $*$ e de uma operação binária denotada por $\diamond$ que satisfazem as seguintes condições:*
1. $(R, *)$ é um grupo comutativo;
2. $(x \diamond y) \diamond z = x \diamond (y \diamond z)$, para todos x, y, z $\in R$.
3. A operação $\diamond$ é distributiva em relação à operação $*$
$x \diamond (y * z) = x \diamond y \ * \ x \diamond z$
$(x * y) \diamond z = x \diamond z \ * \ y \diamond z$

Definição 1.19 *Se no anel R existir o elemento 1 tal que* $x \diamond 1 = 1 \diamond x = x$, *para todo* $x \in R$, *1 é denominado elemento identidade de R.*

Definição 1.20 *Se* $x \diamond y = y \diamond x$, *para todos* $x, y \in R$. *R é um anel comutativo.*

Definição 1.21 *Se para todos* $x, y \in R$, *com* $x \diamond y = 0 \Rightarrow x = 0$ *ou* $y = 0$, *R é um anel sem divisores de zero.*

Definição 1.22 *Um corpo é um anel comutativo com elemento identidade tal que todo elemento não nulo tem um inverso.*

Definição 1.23 *Seja* $(\mathbb{K}, *, \diamond)$ *um corpo e seja P um subconjunto de* $\mathbb{K}$. *Diz-se que P é um subcorpo de* $\mathbb{K}$ *se, e somente se,* $(P, *, \diamond)$ *é um corpo.*

Definição 1.24 *Um corpo com um número finito de elementos é chamado corpo finito.*

Definição 1.25 *Seja p um número primo,* $< p >= \{n.p \text{ para } n \in \mathbb{Z}\} = p\mathbb{Z}$ *é o conjunto gerado por p.*

Definição 1.26 $\mathbb{Z}/ < p >= \{a + < p > \text{ tal que } a = 0, 1, 2, ..., p-1\}$.
$\mathbb{Z}/ < p >= \mathbb{Z}/p\mathbb{Z}$.

Definição 1.27 *P é um subcorpo primo do corpo* $\mathbb{K}$ *se P é um subcorpo de todos os subcorpos de* $\mathbb{K}$.

Definição 1.28 *A característica de um corpo* $\mathbb{K}$ *é um inteiro associado a* $\mathbb{K}$ *da seguinte maneira:*
i) se o corpo primo de $\mathbb{K}$ *é* $\mathbb{Z}/ < p >$ *a característica de* $\mathbb{K}$ *é p.*
ii) se o corpo primo de $\mathbb{K}$ *é* $\mathbb{Q}$ *a característica de* $\mathbb{K}$ *é zero.*

Observação: se a característica do corpo $\mathbb{K}$ é $p \neq 0$ então $p.x = 0$ para todo x $\in \mathbb{K}$.

Definição 1.29 *Seja* $\mathbb{K}$ *é um corpo de característica* $\neq 2$ *e* $x \in K$ *não um quadrado,*
$L = \{a + b\sqrt{x} \text{ tal que } a, b \in K\}$ *é um corpo com as operações adição e multiplicação definidas por:*

$(a + b\sqrt{x}) + (c + d\sqrt{x}) = (a + c) + (b + d)\sqrt{x}$
$(a + b\sqrt{x}).(c + d\sqrt{x}) = (ac + bdx) + (ad + bc)\sqrt{x}.$
Esse corpo é uma extensão algébrica de $\mathbb{K}$*, denominado corpo quadrático e denotado por* $L = \mathbb{K}(\sqrt{x})$.

Proposição 1.3 *Se m, n são inteiros com* $m.d.c(m, n) = 1$*, então os grupos* $\mathbb{Z}/mn\mathbb{Z}$ *e* $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$ *são isomorfos.*

Demonstração: Consideremos o subgrupo cíclico A de $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$ gerado por $(1, 1)$, onde
$A = \{(1, 1)^k,\ com\ k \in \mathbb{Z}\}$.
Para determinar a potência k de $(1, 1)$ em $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$ efetuamos a operação adição do elemento $(1, 1)$ k vezes.
Em $\mathbb{Z}/m\mathbb{Z}$ obteremos o elemento zero somente depois de adicionar o elemento 1 m vezes, e em $\mathbb{Z}/n\mathbb{Z}$ o elemento zero será obtido após adicionar o elemento 1 n vezes. Para obter o elemento zero simultâneamente em $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$ o número de vezes para adicionar o elemento 1 deve um múltiplo de nm. Como $m.d.c(m, n) = 1$, então o primeiro número tal que isso ocorre é mn. Assim $(1, 1)$ gera um subgrupo cíclico de ordem mn, que é a ordem do grupo $\mathbb{Z}/mn\mathbb{Z}$.
Logo, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$ ■

Dado n $\in \mathbb{N}$, o conjunto $\mathbb{Z}_n = \{\overline{0},\ \overline{1},\ ...,\ \overline{n-1}\}$, onde $\overline{a} = \{m \in \mathbb{Z} : m \equiv a\ mod\ n\} = \{a + kn : k \in \mathbb{Z}\}$.

Todo número m $\in \mathbb{Z}$ é congruente mod n a exatamente um dos números
$\{0,\ 1,\ 2,\ ...,\ n-1\}$,e estes últimos são incongruentes entre si mod n.
Para facilitar a escrita representaremos $\{\overline{0},\ \overline{1},\ ...,\ \overline{n-1}\}$ por $\{0,\ 1,\ 2,\ ...,\ n-1\}$.

Teorema 1.3 *O Pequeno Teorema de Fermat*

Seja p um número primo e a um inteiro tal que $p \nmid a$*. Então* $a^{p-1} \equiv 1\ mod\ p$.

Demonstração: Dados p e a com $p \nmid a$, consideremos os conjuntos
$\{1, 2, ..., p-1\}$ e $\{a, 2a, ..., (p-1)a\}$.
Tem-se: $a,\ 2a\ , ...,\ (p-1)a \not\equiv 0\ mod\ p$.

Se i, j $\in \{1,\ 2,\ ...,\ (p-1)\}$ e $ia \equiv ja\ mod\ p$, concluimos $i \equiv j mod\ p$, já que $m.d.c(a,p) = 1$. Então $i = j$, pois $0 \leq |i-j| <$ p. Isto significa que os números $a, 2a, ..., (p-1)a$ não são congruentes entre si mod p. Logo, os $a, 2a, ..., (p-1)a$ são congruentes, em alguma ordem, aos 1,2,...,p-1. Podendo concluir então que:
$(p-1)! = 1.2...(p-1) \equiv a.\ 2a\ ...\ (p-1)a \equiv\ mod\ p$, ou seja
$(p-1)! \equiv a^{p-1}(p-1)!\ mod\ p$.
Como $m.d.c(p,(p-1)!) = 1$, o fator $(p-1)!$ pode ser cancelado nesta congruência obtendo:
$a^{p-1} \equiv\ 1\ mod\ p$

■

Uma das utilidades do Teorema de Fermat é para mostrar que:

Propriedade 1.1 *Um número primo $q = 2n+1$ divide o número de Mersenne $M_n = 2^n - 1$ ou $M_n + 2 = 2^n + 1$*

Demonstração: O número q não divide M_n e $M_n + 2$, senão q dividiria $M_n + 2 - M_n = 2$, que não é verdadeiro.
Como q $\nmid a = 2$ e q é primo, pelo Teorema de Fermat $2^{q-1} \equiv 1\ mod\ q$, ou seja, $2^{2n} - 1 = 2^{q-1} - 1 \equiv 0\ mod\ q$. Logo $q|2^{2n} - 1 = (2^n - 1)(2^n + 1) = M_n(M_n + 2)$, concluindo que $q|M_n$ ou $q|M_n + 2$

■

Números de Mersenne com índice primo nem sempre são primos. O Teorema de Fermat pode ser aplicado para elaborar uma condição necessária para que um número de Mersenne com índice ímpar seja composto. Primeiramente será deduzido o seguinte resultado:

Proposição 1.4 *Seja q primo e a um inteiro não divisível por q. Seja k_0 o menor número natural tal que $a^{k_0} \equiv 1\ mod\ q$ e seja o número natural k com $a^k \equiv 1\ mod\ q$, então $k_0|k$. (k_0 é denominado ordem de a módulo q e denota-se $\circ_q(a)$)*

Demonstração: Existem r e s $\in \{0, 1, 2, ...\}$ com$k = sk_0 + r$ onde $0 \leq r < k_0$. Temos $1 \equiv a^k = a^{sk_0+r} = (a^{k_0})^s ar = 1^s a^r \equiv a^r\ mod\ q$. Como $a^r \equiv 1\ mod\ q$, e $0 \leq r < k_0$ e k_0 é o menor expoente natural com $a^{k_0} \equiv 1\ mod\ q$, concluimos $r = 0$. Assim $k_0|k$

■

Proposição 1.5 *Sejam p, q números primos ímpares.*
Se $q|M_p$ *então* $q = 2kp + 1$ *com* $k \in \mathbb{N}$.

Demonstração: $q|M_p = 2^p - 1$ significa $2^p \equiv 1 \ mod \ q$. Seja k_0 o menor expoente positivo com $2^{k_0} \equiv 1 \ mod \ q$, pelo resultado anterior $k_0|p$. De $2 \not\equiv 1 \ mod \ q$ concluimos $k_0 > 1$ e segue $k_0 = p$. Como $q \nmid 2$ temos por Fermat $2^{q-1} \equiv 1 \ mod \ q$, $p = k_0|q - 1$. Logo existe s $\in \mathbb{N}$ com $p.s = q - 1$ ou seja $q = p.s + 1$. Como p,q são ímpares, concluimos que $s = 2k$ é par. Assim $q = 2kp + 1$

■

Teorema 1.4 *Teorema de Wilson*

Para todo primo p vale $(p-1)! \equiv -1 \ mod \ p$

Em outras palavras: Sejam p $\in \mathbb{N}$, $p > 1$. A congruência $(p-1)! \equiv -1(mod p)$ é válido se, e somente se, p é primo.

Demonstração: Para $p = 2$; $(2-1)! \equiv 1 \equiv -1(mod \ 2)$, o resultado é válido.
Para $p > 2$. A congruência $ax \equiv 1 \ mod \ p$ tem uma única solução $x = b$ no conjunto $\{1, \ 2, \ ..., \ p-1\}$, com $b \neq 1$ e $b \neq p-1$, pois $a \not\equiv \pm 1 \ mod \ p$. Para $a \in \{2, \ 3, \ ..., \ p-2\}$ existe um único $b \in \{2, \ ..., \ p-2\}$ com $ab \equiv 1 \ mod \ p$ e $a \neq b$. O conjunto$\{2, \ ..., \ p-2\}$ pode ser reordenado como
$\{2, \ ..., \ p-2\} = \{a_1, \ b_1, \ ..., \ a_{\frac{p-3}{2}}, \ b_{\frac{p-3}{2}} \}$, onde
$a_1 b_1 \equiv a_2 b_2 \ ... \ \equiv a_{\frac{p-3}{2}} b_{\frac{p-3}{2}} \equiv 1 \ mod \ p$. Segue
$(p-1)! = 1 \ . \ 2 \ ...(p-1) = 1 \ . \ (a_1 b_1) \ ... \ (a_{\frac{p-3}{2}} b_{\frac{p-3}{2}})(p-1) \equiv 1.1....1(p-1) \equiv -1 \ mod \ p$

■

Teorema 1.5 *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*

$a_1 x \equiv c_1 \ (mod \ m_1)$
$a_2 x \equiv c_2 \ (mod \ m_2)$
$\vdots$
$a_r x \equiv c_r \ (mod \ m_r)$

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

Demonstração: Do fato de $(a_i, \ m_i) = 1$,e $1|c_i$ tem-se que $a_i x \equiv c_i \ (mod \ m_i)$ possui uma única solução denotada por b_i. Ao definir $y_i = \frac{m}{m_i}$ onde, $m = m_1 \ . m_2 \ ... \ m_r$, teremos $(y_i, \ m_i) = 1$, uma vez que $(m_i, \ m_j) = 1$ para $i \neq j$. Cada uma das congruências

$y_i x \equiv 1 \ (mod \ m_i)$ possui uma única solução denotada por $\overline{y}_i$. Logo, $y_i \overline{y}_i \equiv 1 \ (mod \ m_i)$, $i = 1, 2, ..., r$. O número dado por

$x = b_1 y_1 \overline{y}_1 + b_2 y_2 \overline{y}_2 + \ ... \ + \ b_r y_r \overline{y}_r$ é uma solução simultânea para o nosso sistema de congruências. De fato

$a_i x = a_i b_1 y_1 \overline{y}_1 + a_i b_2 y_2 \overline{y}_2 + \ ... \ + a_i b_r y_r \overline{y}_r \equiv a_i b_i \overline{y}_i \ (mod \ m_i) \equiv a_i b_i \equiv c_i \ (mod \ m_i)$, uma vez que y_j é divisível por m_i para $i \neq j$, $y_i \overline{y}_i \equiv 1 \ (mod \ m_i)$ e b_i é solução de $a_i x \equiv c_i \ (\ mod \ m_i)$

A solução é única, se supor que existe outra solução $\overline{x}$ que satisfaça o sistema, então $a_i \overline{x} \equiv c_i \equiv a_i x \ (mod \ m_i)$ e, sendo $(a_i, \ m_i) = 1$ obtemos $\overline{x} \equiv x \ (mod \ m_i)$. Logo $m_i | (\overline{x} - x)$, $i = 1, \ 2, \ ..., \ r$. Mas, como $(m_i, \ m_j) = 1$ para $i \neq j$ temos que

$m.m.c(m_1, \ m_2, \ ..., \ m_r) = m_1 . m_2 \ ... \ m_r$ então $\overline{x} \equiv x \ (mod \ m_1 . m_2 ... m_r)$ assim,

$m_1 . m_2 ... m_r | (\overline{x} - x)$, isto é $\overline{x} \equiv x \ (mod \ m)$, logo $x \in \overline{x}$ ■

Este capítulo constitui-se de uma introdução às idéias da álgebra abstrata especialmente dos sistemas algébricos chamados grupos e estendendo a outros sistemas como anéis, corpos, etc.

Alguns teoremas são citados, como O Pequeno Teorema de Fermat que pode ser usado como teste para verificar se o número é composto, isto é: Se existe a inteiro, $1 < a < n$ tal que $a^n \ \not\equiv a \ mod \ n$ então n é composto, pois podemos ter $a^n \ \equiv a \ mod \ n$ e n não ser primo, sendo denominado número de Carmichael.

O método de resolver um sistema com equações que envolvem equivalências modulares está na demonstração do Teorema do Resto Chinês.

O Teorema de Wilson fornece um critério para decidir sobre a primalidade de um número.

As definições, teoremas e proposições abordadas neste capítulo subsidiam a teoria dos resíduos quadráticos, as equações de congruência e o essencial Critério de Euler no estudo de verificação de resíduos quadráticos, que compõem o capítulo seguinte.

Capítulo 2

Resíduos Quadráticos

Carl Friederich Gauss (1777-1855) foi um dos maiores matemáticos de todos os tempos, nasceu em Brunswick, Alemanha,filho de uma modesta família, portador de uma genialidade surpreendente, ainda criança aprendeu a ler sozinho e possuia uma grande habilidade de realizar complicados cálculos mentais. Em 1798, Gauss produz uma das obras primas de toda a matemática, o livro Disquisitiones Arithmeticae, publicado em 1801. No livro, Gauss introduz a noção de congruência; desenvolve a teoria dos resíduos quadráticos, demonstra a Lei da Reciprocidade Quadrática; estuda as formas quadráticas binárias, deduzindo de forma geral o Teorema de Fermat, que assegura que todo número primo da forma $4n+1$ se escreve como soma de quadrados de dois números naturais; e, na última seção, deduz o teorema que diz que um polígono regular com um número primo n de lados, inscrito no círculo, é construtível com régua e compasso se, e somente se, n é um número primo de Fermat.
Gauss contribuiu de forma significativa à teoria das probabilidades, foi um dos criadores da geometria não-euclideana, da geometria diferencial, das funções de variável complexa, da topologia e da teoria algébrica dos números. Gauss descreveu a matemática como a rainha das ciências e a aritmética (isto é, teoria dos números) como a rainha da matemática, por isso, foi considerado, pelos seus contemporâneos e pelas gerações que se sucederam, um Príncipe da Matemática.

Definição 2.1 *Resíduos Quadráticos*

Seja um corpo $\mathbb{F}$. *Os elementos a de* $\mathbb{F}$ *com* $a = b^2$ *para algum* $b \in \mathbb{F}$ *são denominados quadrado em F. Quando o corpo* $\mathbb{F} = \mathbb{C}$, *temos que todo número complexo é um quadrado em* $\mathbb{C}$. *Dado o número complexo* $r + si = a$ *existe* $b \in \mathbb{C}$ *tal que* $a = b^2$ *para* $b = x + yi$, *onde* $r = x^2 - y^2$ *e* $s = 2xy$. *Para* $\mathbb{F} = \mathbb{R}$, *um número x é um quadrado se, e somente se* $x \geq 0$.

Conhecimento sobre quadrados é importante para resolver equações quadráticas. A equação $x^2 + ax + b = 0$ possui soluções reais se, e somente se o discriminante $a^2 - 4b$ é um quadrado, isto é $a^2 - 4b = x^2$ para algum x real. Para o corpo finito $\mathbb{Z}/p\mathbb{Z}$ com p ímpar também é possível determinar os quadrados. Por exemplo, para resolver a equação $x^2+2x-1 = 0$ em $\mathbb{Z}/p\mathbb{Z}$. As duas soluções em $\mathbb{R}$ obtidas são: $-1 \pm \sqrt{2}$ que serão soluções em $\mathbb{Z}/p\mathbb{Z}$ se 2 é um quadrado em $\mathbb{Q}(\sqrt{2})$ (relebrando: $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}$ com $a, b \in \mathbb{Q}\}$).
Se $p = 7$ temos $2 \equiv 3^2 \ mod\ 7$, assim a fórmula nos dá:
$-1 + \sqrt{2} \equiv (-1 + 3) \ mod\ 7 \equiv 2 \ mod\ 7$, e
$-1 - \sqrt{2} \equiv (-1 - 3) \ mod\ 7 \equiv -4 \ mod\ 7$.
De fato na equação dada, $2^2 + 2.2 - 1 \equiv (-4)^2 + 2.(-4) - 1 \equiv 0 \ mod\ 7$
A reciprocidade quadrática nos ajuda a verificar se certos elementos são quadrados ou não em $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
Os quadrados em $\mathbb{F}_p$ serão chamados de resíduos quadráticos módulo p e os não quadrados como resíduos não quadráticos modulo p. Cada resíduo quadrático em $\mathbb{F}_p$ representa os inteiros cuja classe de restos é um quadrado.
Como zero é sempre quadrado, consideremos $\mathbb{F}_p^* = \mathbb{Z}/p\mathbb{Z} - \{0\}$.
Em $\mathbb{F}_3^*$ temos $1 \equiv 1^2 \ mod\ 3$ mas $2 \not\equiv b^2 \ mod\ 3 \ com\ b \in \mathbb{F}_3^*$
Em $\mathbb{F}_5^*$ temos $1 \equiv 4^2 \ mod\ 5$; $4 \equiv 2^2 \ mod\ 5$; $-1 \equiv 2^2 \ mod\ 5$; mas $2 \not\equiv b^2 \ mod 5$ e $3 \not\equiv b^2 \ mod\ 5$.
Em $\mathbb{F}_{19}^*$:
$1 \equiv 18^2 \ mod\ 19$, $4 \equiv 17^2 \ mod\ 19$; $5 \equiv 9^2 \ mod\ 19$
$6 \equiv 5^2 \ mod\ 19$; $7 \equiv 8^2 \ mod\ 19$; $9 \equiv 3^2 \ mod\ 19$;
$11 \equiv 7^2 \ mod\ 19$; $16 \equiv 4^2 \ mod\ 19$; $17 \equiv 6^2 \ mod\ 19$;
$2 \not\equiv b^2 \ mod\ 19$; $3 \not\equiv b^2 \ mod\ 19$; $8 \not\equiv b^2 \ mod\ 19$;
$10 \not\equiv b^2 \ mod\ 19$; $12 \not\equiv b^2 \ mod\ 19$; $13 \not\equiv b^2 \ mod\ 19$;

$14 \not\equiv b^2 \ mod\ 19; \quad 15 \not\equiv b^2 \ mod\ 19; \quad 18 \not\equiv b^2 \ mod\ 19;$

$\{1^2, 2^2, 3^2, ..., 17^2, 18^2\} = \{1, 4, 9, 16, 6, 17, 11, 7, 5\}=$
$= \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$ são os resíduos quadráticos modulo 19, e $\{2, 3, 8, 12, 13, 14, 15, 18\}$ são os resíduos não quadráticos módulo 19.

primo	quadrado	não-quadrado
3	1	2
5	1, 4	2, 3
7	1,2,4	3,5,6
11	1,3,4,5,9	2,6,7,8,10
13	1,3,4,9,10,12	2,5,6,7,8,11
17	1,2,4,8,9,13,15,16	3,5,6,7,10,11,12,14
19	1,4,5,6,7,9,11,16,17	2,3,8,10,12,13,14,15,18

Em geral se $p > 2$ é primo, os resíduos quadráticos mod p do $\{1, 2, ..., p-1\}$ são os números representados por $\{1^2, 2^2, 3^2, ..., (\frac{p-1}{2})^2\}$.

$\{1^2, 2^2, ..., (p-1)^2\}=$

$=\{1^2, 2^2, .., (\frac{p-3}{2})^2, (\frac{p-1}{2})^2, (\frac{p+1}{2})^2, (\frac{p+3}{2})^2, ..., (p-2)^2, (p-1)^2\}=$

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

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

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

Este últimos $\frac{p-1}{2}$ números são incongruentes entre si, pois $x^2 \equiv b^2 \ mod\ p$ possui as duas soluções $x \equiv \pm b \ mod\ p$.
Assim, podemos afirmar que existem $\frac{p-1}{2}$ resíduos quadráticos modulo p e $\frac{p-1}{2}$ resíduos não quadráticos módulo p entre $\{1, 2, ..., p-1\}$. Não existe regularidade para descobrir quais são

resíduos quadráticos.

Quando o número -1 é um resíduo quadrático?

Para $p = 5$ 13 *e* 17, -1 é um resíduo quadrático, mas para $p = 3, 7$ *e* 11 não é um resíduo quadrático.
Sabemos que:
$5 \equiv 1 \ mod\ 4$
$13 \equiv 1 \ mod\ 4$
$17 \equiv 1 \ mod\ 4$
$3 \not\equiv 1 \ mod\ 4$
$7 \not\equiv 1 \ mod\ 4$
$11 \not\equiv 1 \ mod\ 4$.

Vamos caracterizar os primos p módulo para os quais -1 é um resíduo quadrático.

Proposição 2.1 *Seja $p > 2$ um primo. A congruência $-1 \equiv x^2 \ mod\ p$ admite uma solução se, e somente se, $p \equiv 1 \ mod\ 4$.*

Demonstração: Se $-1 \equiv x^2 \ mod\ p$, possui uma solução, então existe $b \in \mathbb{Z}$ tal que
$-1 \equiv b^2 \ mod\ p$
Pelo teorema de Fermat temos:
$1 \mod p \equiv b^{p-1} \equiv (b^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \ mod\ p$.
$1 \ mod\ p \equiv (-1)^{\frac{p-1}{2}} \ mod\ p \Rightarrow\ 1 = (-1)^{\frac{p-1}{2}},\ como\ 1 \not\equiv -1 \ mod\ p$
segue que $\frac{p-1}{2}$ é par, isto é: $\frac{p-1}{2} = 2k$.
$p - 1 = 4k \Rightarrow p \equiv 1 \ mod\ 4$.
Supondo $p \equiv 1 \ mod\ 4$. Pelo Teorema de Wilson temos:
$-1 \ mod\ p \equiv (p-1)! = 1.2...\frac{p-1}{2}.\frac{p-3}{2}...(p-2)(p-1) \equiv 1.2...\frac{p-1}{2}.(-\frac{p-1}{2})...(-2)(-1) \equiv (-1)^{\frac{p-1}{2}}[(\frac{p-1}{2})!]^2 \ mod\ p \equiv [(\frac{p-1}{2})!]^2 mod p$. Como $p \equiv 1 mod 4$, $\frac{p-1}{2}$ é par, tem-se:
$(-1)^{\frac{p-1}{2}} = 1$
$-1 \ mod\ p \equiv [(\frac{p-1}{2})!]^2 mod p$.
$-1 \equiv b^2 mod p$, para $b = (\frac{p-1}{2})!$ ■

A tabela abaixo fornece os números primos $p \leq 37$ tal que $p \equiv 1 \ mod \ 4$, e as duas soluções incongruentes da equação $-1 \equiv b^2 \ mod \ p$.

$p \equiv 1 mod 4$	Soluções b e $p-b$ da equação $-1 \equiv b^2 mod p$
5	2 , 3
13	5 , 8
17	4 , 13
29	12 , 17
37	6 , 31

Proposição 2.2 *Sempre* $a^{\frac{p-1}{2}} \equiv \pm 1 \ mod \ p$, *para* $p > 2$ *primo e* $p \nmid a$.

Demonstração: Pelo teorema de Fermat $1 \equiv a^{p-1} \ mod \ p \equiv (a^{\frac{p-1}{2}})^2 \ mod \ p$. Consequentemente

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

Assim, $p \mid (a^{\frac{p-1}{2}} + 1)$ ou $p \mid (a^{\frac{p-1}{2}} - 1)$. Como p é primo, conclui-se que:

$p \mid a^{\frac{p-1}{2}} + 1$ ou $p \mid a^{\frac{p-1}{2}} - 1$ obtendo: $a^{\frac{p-1}{2}} \equiv \pm 1 \ mod \ p$

■

Teorema 2.1 *Critério de Euler*

Se $a \in \mathbb{Z}$ *não é divisível por um primo ímpar p, então a é um resíduo quadrático (ou resíduo não quadrático) de acordo com* $a^{\frac{p-1}{2}} \equiv 1 \ mod \ p$ *(ou* $a^{\frac{p-1}{2}} \equiv -1 \ mod \ p$*).*

Demonstração: Seja a um resíduo quadrático modulo p, assim existe $b \in \mathbb{Z}$ tal que $a \equiv b^2 \ mod \ p$, pelo Teorema de Fermat

$a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \ mod \ p$. Supondo que a é um resíduo não quadrático modulo p.

Para todo $c \in \{1, 2, ..., p-1\}$ a congruência $cx \equiv a \ mod \ p$ possui possui apenas uma solução: $c' \in \{1, 2, ..., p-1\}$.

Como $c \neq c'$ (caso contrário $a \equiv cc' = c^2$), podemos escrever o conjunto:

$\{1, 2, ..., p-1\} = \{c_1, c_1', c_2, c_2', ..., c_{\frac{p-1}{2}}, c_{\frac{p-1}{2}}'\}$ tal que

$c_k.c_k' \equiv a \ mod \ p$. Para $1 \leq k \leq \frac{p-1}{2}$

Pelo Teorema de Wilson:

$-1 \equiv (p-1)! = (c_1.c_1').(c_2.c_2')...(c_{\frac{p-1}{2}}.c_{\frac{p-1}{2}}') \equiv a.a...a = a^{\frac{p-1}{2}} \ mod \ p$

■

Definição 2.2 *O Símbolo de Legendre*

Dado um primo p e um inteiro $a \in \mathbb{Z}$ não divisível por p. O símbolo de Legendre

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

O símbolo Legendre é uma "sim/não-função" para decidir se um número a é ou não é um resíduo quadrático módulo p.

Proposição 2.3 *Para todo primo $p > 2$, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.*

A proposição acima é uma tradução da proposição:

Proposição 2.4 *Para $p > 2$ primo. A congruência $-1 \equiv b^2 \ mod \ p$ posui uma solução se, e somente se $p \equiv 1 \ mod \ 4$, para o conceito do símbolo de Legendre.*
-1 é um resíduo quadrático mod p se, e somente se $p \equiv 1 \ mod \ 4$, isto é:
$\frac{p-1}{2}$ é par $\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1$.

O símbolo de Legendre possui algumas propriedades elementares que são:
(i) Se $a \equiv bmodp$, então $(\frac{a}{p}) = (\frac{b}{p})$

(ii) $(\frac{a^2}{p}) = 1$

(iii) $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} modp$

(iv) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

Demonstração:

(i) $$(\frac{a}{p}) = \begin{cases} 1, & \text{se} \quad a^{\frac{p-1}{2}} \equiv 1 modp \\ -1, & \text{se} \quad a^{\frac{p-1}{2}} \equiv -1 modp \end{cases}$$

Como $a \equiv b \ mod \ p$, tem-se $b^{\frac{p-1}{2}} \equiv 1 \ mod \ p \Rightarrow (\frac{b}{p}) = 1$ ou
$b^{\frac{p-1}{2}} \equiv -1 \ mod \ p \Rightarrow (\frac{b}{p}) = -1$
Assim $(\frac{a}{p}) = (\frac{b}{p})$.

(ii) $(\frac{a^2}{p}) = (\frac{a.a}{p}) = (\frac{a}{p})(\frac{a}{p}) = \begin{cases} 1.1=1 & \text{se a é um resíduo quadrático módulo p} \\ (-1)(-1)=1 & \text{se a é um resíduo não-quadrático módulo p} \end{cases}$

(iii) Pelo Critério de Euler, $a^{\frac{p-1}{2}} \equiv \pm 1 \ mod \ p \Rightarrow a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) mod \ p$.

(iv) $(\frac{a.b}{p}) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}.b^{\frac{p-1}{2}} \equiv (\frac{a}{p}).(\frac{b}{p}) mod p$
Ambos os lados dessa congruência são ± 1, e sabemos que $-1 \not\equiv 1 \ mod \ p$, podemos concluir que:
$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$
■

A propriedade (iv) pode ser traduzida como sendo: o produto de dois resíduos quadráticos ou de dois resíduos não quadráticos módulo p é um resíduo quadrático módulo p, e o produto de um resíduo quadrático por um resíduo não-quadrático é um resíduo não-quadrático.

Corolário 2.1 *O símbolo de Legendre induz um homomorfismo*
φ:$(\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ *definido por:* $\varphi(a) = \varphi(\frac{a}{p})$
Em outras palavras: $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$ *para todos* $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$

Lema 2.1 *Se* $p > 0$ *é um primo ímpar divisor de um inteiro da forma* $n^2 + 1$, *então* $p \equiv 1 \ mod \ 4$.

Demonstração: Por hipótese $p \mid n^2 + 1 \Rightarrow$ existe $q \in \mathbb{Z}$ tal que $n^2 + 1 = qp$
$n^2 = -1 + qp \Rightarrow n^2 \equiv -1 mod p \Rightarrow$ -1 é um resíduo quadrático módulo p, assim $p \equiv 1 \ mod \ 4$
■

Corolário 2.2 *Existem infinitos números primos da forma* $4n+1$ *com* $n \in \mathbb{N}$.

Demonstração: Supondo por contradição que existe somente um conjunto finito de números primos da forma $4n+1$, isto é:
$\{p_1 = 5, p_2 = 13, ..., p_r\}$ o conjunto de todos os primos congruentes a 1 módulo 4.
Para p primo e $p = 4n+1 \Rightarrow p \equiv 1 \ mod \ 4$
O número $N = 4p_1^2p_2^2...p_r^2 + 1 = (2p_1p_2...p_r)^2 + 1$ é da forma $4n+1$.
Seja q um número primo tal que $q \mid N$ então $(2p_1p_2...p_r)^2 + 1 \equiv 0 \ mod \ q$.
$(2p_1p_2...p_r)^2 \equiv -1 \ mod \ q$, para $b = 2p_1p_2...p_r$ a equação $b^2 \equiv -1 \ mod \ q$ possui solução, então pela proposição 2.4 $q \equiv 1 \ mod \ 4$.Assim $q \in \{p_1, p_2, ..., p_r\}$ e $q = 4k+1 \Rightarrow q \mid 1$, o que é absurdo.
Assim q primo $\notin \{p_1, p_2, ..., p_r\}$, logo $\{p_1, p_2, ..., p_r\}$ não está completo, não sendo finito
■

O Símbolo de Legendre para $a = 2$
Para $a = 2$ faremos um estudo em particular para determinar o símbolo de Legendre $(\frac{a}{p})$.

Para $p = 3$, $2^{\frac{3-1}{2}} = 2 \equiv -1 \ mod \ 3$, assim $(\frac{2}{3}) = -1$. Portanto 2 é um resíduo não quadrático módulo 3.
Não existe $b \in \mathbb{Z}$ tal que $2 \equiv b^2 \ mod \ 3$, assim em $\mathbb{Q}(\sqrt{2})$, 2 não é um resíduo quadrático.

Para $p = 7$, $2^{\frac{7-1}{2}} = 2^3 \equiv 1 \ mod \ 7$, assim $(\frac{2}{7}) = 1$; isto é 2 é um resíduo quadrático módulo 7.

$2 \equiv 3^2 \ mod \ 7$. Em $\mathbb{Q}(\sqrt{2})$, $\sqrt{2} \equiv \pm 3 \ mod \ 7$.
Com procedimento análogo 2 é um resíduo quadrático módulo 17, 23 e 31 entre os primos de 3 a 31, e esses primos são da forma $p \equiv \pm 1 mod 8$.

Proposição 2.5 *O número primo 2 é um resíduo quadrático módulo um número primo p ímpar (um resíduo não quadrático módulo p) se* $p \equiv \pm 1 \ mod \ 8$ *(*$p \equiv \pm 3 \ mod \ 8$*).*

Em outras palavras $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Demonstração: Sendo p primo ímpar, necessariamente deverá ser congruente a 1, 3, 5 ou 7 módulo 8.

Se $p \equiv 1 \ mod \ 8 \Rightarrow p - 1 = 8k, \ k \in \mathbb{Z}$

$p + 1 = 8k + 2 = 2(4k + 1)$

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

$p \equiv 7 \ mod \ 8 \Rightarrow p - 7 = 8k, \ k \in \mathbb{Z}$.

$p - 1 = 8k + 6 = 2(4k + 3)$ e $p + 1 = 8k + 8 = 8(k + 1)$

$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{8(k+1)2(4k+3)}{8} = 2(2k + 1)(4k + 3)$ é par.

$7 \equiv -1 \ mod \ 8$, então $p \equiv -1 \ mod \ 8$.

Se $p \equiv \pm 1 \ mod \ 8$, tem-se $\frac{p^2-1}{8}$ é par.

Se $p \equiv 3 \ mod \ 8 \Rightarrow p - 3 = 8k, \ k \in \mathbb{Z}$

$p - 1 = 8k + 2$ e $p + 1 = 8k + 4$

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

$p \equiv 5 \ mod \ 8 \Rightarrow p - 5 = 8k, \ k \in \mathbb{Z}$

$p - 1 = 8k + 4, \quad p + 1 = 8k + 6$

$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = (2k + 1)(4k + 3)$ é ímpar

$5 \equiv -3 \ mod \ 8$ e $-3 \equiv 5 \ mod \ 8 \equiv p$

Se $p \equiv \pm 3 \ mod \ 8$, tem-se $\frac{p^2-1}{2}$ é ímpar

Consideremos: para i ímpar, $p - i \equiv i(-1)^i \ mod \ p$

para i par, $i \equiv i(-1)^i \ mod \ p$

Considerando as $\frac{p-1}{2}$ congruências :

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

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

$\vdots$

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

Caso $\frac{p-1}{2}$ seja par, a última congruência será $t \equiv \frac{p-1}{2} \ mod \ p \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \ mod \ p$.

Caso $\frac{p-1}{2}$ seja ímpar, a última congruência será $p - \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \ mod \ p$. Como p é ímpar $(p-1, p-3, ..., p-\frac{p-1}{2})$ são pares.

Na coluna da esquerda temos $p-1, 2, p-3, ..., \frac{p-1}{2}$ são todos pares, que são $(2, 4, 6, ..., p-1)$.

Multiplicando membro a membro nesta coluna, temos:

$2.4.6...(p-1) \equiv (-1)^{1+2+...+\frac{p-1}{2}}(\frac{p-1}{2})! mod p$

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

Como $mdc((\frac{p-1}{2})!, p) = 1$ podemos cancelar $(\frac{p-1}{2})!$ na expressão acima, obtendo $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} mod p$.

Lembrando que $(\frac{2}{p}) \equiv 2^{\frac{p-1}{2}} \ mod \ p$, obtem-se $(\frac{2}{p}) \equiv (-1)^{\frac{p^2-1}{8}} \ mod \ p$ que é 1 ou -1

Se $\frac{p^2-1}{8}$ é par $\Rightarrow (\frac{2}{p}) = 1$ para $p \equiv \pm 1 \ mod \ 8$

Se $\frac{p^2-1}{8}$ é impar $\Rightarrow (\frac{2}{p}) = -1$ para $p \equiv \pm 3 \ mod \ 8$

Logo 2 é um resíduo quadrático se $p \equiv \pm 1 \ mod \ 8$ ou um resíduo não quadrático se $p \equiv \pm 3 \ mod \ 8$

■

A ordem do grupo $(\mathbb{Z}/p\mathbb{Z})^*$ é $p-1$ e para $a \in (\mathbb{Z}/p\mathbb{Z})^*$, $a^{p-1} \equiv 1 mod p$, para p primo e $(a, p) = 1$, podemos substituir $p-1$ por $\varphi(p)$, onde φ é a função de Euler.

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

O Critério de Euler é uma generalização do Pequeno Teorema de Fermat quando assim enunciado:

Sejam n um inteiro positivo e a um inteiro relativamente primo com n. Então, $a^{\varphi(n)} \equiv 1 mod n$, onde $\varphi(n)$ é o número de inteiros positivos de 1 a n que são relativamente primos com n. E tal critério fornece condição de verificar se um número inteiro é um resíduo quadrático.

A função φ de Euler faz parte das funções chamadas "funções aritméticas".

Uma congruência do tipo $x^2 \equiv a \ mod \ m$, onde a e m são números naturais com $m > 1$, nem sempre tem solução. O Teorema chamado Lei da Reciprocidade Quadrática, juntamente com as propriedades do Símbolo de Legendre funciona como um algorítmo para determinar se um número é ou não é resíduo quadrático módulo um primo ímpar p. Tal teorema objeto de estudo do próximo capítulo, tem na sua formulação recursos no Símbolo de Legendre e Lema de Gauss.

Capítulo 3

Lema de Gauss e Reciprocidade Quadrática

Reciprocidade quadrática pertence à parte mais importante de toda introdução à teoria dos números. A versão preliminar foi descoberta em 1742 por Leonhard Euler (1707 - 1783) em sua primeira pesquisa sobre divisores primos de números da forma $a^n + b^n$ e a versão final de Euler foi publicada em 1785, dois anos após sua morte. Em 1788 Adrien-Marie Legendre (1752 - 1833) deu uma prova incompleta dessa lei. Carl Friedrich Gauss (1777 - 1855) redescobriu a lei da reciprocidade quadrática quando tinha 18 anos, e apresentou sua primeira demonstração um ano após, mas na décima semana seguinte encontrou uma demonstração simples usando a teoria das formas quadráticas binárias, tal lei foi publicada em "Gauss's Disquisitiones Arithmeticae", Gauss apresentou diferentes provas completas. Existem outras provas posteriores.

Definição 3.1 *O sistema reduzido módulo p, para o primo* $p = 2n + 1$*, é o conjunto* $A = \{a_1, a_2, ..., a_n\} = \{a_1, a_2, ..., a_{\frac{p-1}{2}}\}$*, com as seguintes propriedades:*
a) os a_j *são distintos módulo p, isto é: se* $a_i \equiv a_j \ mod \ p$*, então* $i = j$*;*
b) para todo inteiro ocorre exatamente um dos dois casos; ele é congruente a a_i *módulo p ou congruente a* $-a_i$ *módulo p, para algum* $1 \leq i \leq \frac{p-1}{2}$*.*
$A \cup -A$ *é o conjunto completo de classes de resíduos* $\neq \overline{0}$ *módulo primo p.*

Lema de Gauss

A principal demonstração por Gauss da lei da reciprocidade quadrática é através do Lema de Gauss.

3.1 Lema de Gauss

Seja $p = 2n + 1$ um número primo ímpar, seja um sistema reduzido $A = \{a_1, a_2, ..., a_n\}$, e a um número inteiro não divisível por p.

Consideremos o sistema:

$a_i.a \equiv (-1)^{s(i)} a_{t(i)} \ mod \ p$

para $a_i \in A$, onde $s(i) \in \{0, 1\}$ e $t(i) \in \{1, 2, ..., n\}$. Então

$a^n \equiv \prod_{i=1}^{n} (-1)^{s(i)} \ mod \ p$

Assim a é um resíduo quadrático ou resíduo não quadrático módulo p de acordo com o número de mudanças de sinais ser par ou ímpar.

Para a reciprocidade quadrática o Critério de Euler utiliza o fator $a^{\frac{p-1}{2}}$. Gauss relacionou o fator $\frac{p-1}{2}$ com um sistema reduzido módulo p e utilizou-o nas equações de congruência módulo p.

Para facilitar a compreensão da demonstração do Lema de Gauss, consideremos um exemplo em particular para o número primo $p = 13$, onde $p = 2.6 + 1$, obtemos $A = \{1, 2, 3, 4, 5, 6\}$, e seja $a = 2$.

Multipliquemos todos os elementos de A por 2 e obtemos:

$2.1 \equiv +2 \ mod \ 13$,

$2.2 \equiv +4 \ mod \ 13$,

$2.3 \equiv +3 \ mod \ 13$,

$2.4 \equiv -5 \ mod \ 13$,

$2.5 \equiv -3 \ mod \ 13$,

$2.6 \equiv -1 \ mod \ 13$.

Lembrando que 8,10,12 é respectivamente o simétrico de 5, 3 e 1 módulo 13.

Os três primeiros produtos estão em A, e os tres últimos estão em -A onde ocorreu três mudanças de sinais (quantidade impar), e 2 não é um resíduo quadrático módulo 13.
Multiplicando a congruência acima, obtemos
$2^6 6! \equiv (-1)^3 6!\ mod\ 13$,
sabendo que $m.d.c\ (6!, 13) = 1$, efetuamos o cancelamento tendo; $2^6 \equiv -1\ mod\ 13$
Pelo critério de Euler 2 é um resíduo não quadrático módulo 13.
Se tomarmos $a = 3$, temos o sistema de congruência:
$3.1 \equiv +3\ mod\ 13$,
$3.2 \equiv +6\ mod\ 13$,
$3.3 \equiv -4\ mod\ 13$,
$3.4 \equiv -1\ mod\ 13$,
$3.5 \equiv +2\ mod\ 13$,
$3.6 \equiv +5\ mod\ 13$.
Como o $m.d.c(6!, 13) = 1$, e no sistema ocorreu duas mudanças de sinais, multiplicando a congruência, e efetuando o cancelamento de 6! obtem-se a expressão $3^6 \equiv (-1)^2\ mod\ 13 \equiv 1\ mod\ 13$, assim 3 é um resíduo quadrático módulo 13.

Lema de Gauss

Demonstração: O índice $t(i) \in \{1, 2, ..., n\}$, então os elementos $a_{t(i)}$ são exatamente os elementos a_i de A em uma ordem diferente com $a_{t(i)} \neq a_{t(k)}$ para $i \neq k$
Os conjuntos $\{a_1, a_2, ..., a_n\}$ e $\{a_{t(1)}, a_{t(2)}, ..., a_{t(n)}\}$ são coincidentes, então o produto desses elementos é o mesmo para cada conjunto, isto é;
$\prod a_i = \prod a_{t(i)}$, temos por hipótese que $a_i a \equiv (-1)^{s(i)} a_{t(i)}\ mod\ p$, para $i = 1, 2, ..., n$.
Efetuando o produto das n-congruências acima e substituindo $\prod a_{t(i)}$ por $\prod a_i$, obtemos:
$\prod a_i a = a^n \prod a_i \equiv \prod (-1)^{s(i)} a_{t(i)}\ mod\ p \equiv \prod (-1)^{s(i)} \prod a_i\ mod\ p$.
Como o $m.d.c(\prod a_i, p) = 1$, podemos cancelar $\prod a_i$ na congruência, assim $a^n \equiv \prod (-1)^{s(i)}\ mod\ p$.
■

Uma segunda demonstração da Proposição 2.5 é aplicando o Lema de Gauss.

Proposição 3.1 *Para p primo ímpar,* $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Demonstração: É necessário saber o número de mudança de sinal nas congruências módulo p quando multiplicamos o sistema reduzido $\{1, 2, ..., \frac{p-1}{2}\}$ por $a = 2$.

Para o número primo ímpar p, consideremos dois casos:

1° Caso)

Para $p = 4k + 1$, k inteiro positivo $\Rightarrow \frac{p-1}{2} = 2k$, façamos

$\{1, 2, ..., \frac{p-1}{2}, ..., p-1\}$=$\{1, 2, ..., 2k\} \cup \{2k + 1, ..., 4k\}$.

Observando que,$p = 4k + 1 \equiv 0 \ mod \ p \Rightarrow 4k \equiv -1 \ mod \ p$ e $p = 4k + 1 = 2k + 2k + 1 \equiv 0 \ mod \ p$, logo $2k + 1 \equiv -2k \ mod \ p$, então para o sistema reduzido $\{1, 2, ..., 2k\}$, temos

$2.1 \equiv 2 \ mod \ p$

$2.2 \equiv 4 \ mod \ p$

$\vdots$

$2.k \equiv 2k \ mod \ p$

$2.(k + 1) = 2k + 2 = 2k + 1 + 1 \equiv -2k + 1 \ mod \ p$

$\vdots$

$2.2k = 4k \equiv -1 \ mod \ p$

Para as k primeiras congruências não ocorreu mudança de sinal, mas para as últimas k congruências ocorreram k mudanças de sinais. pela Lema de Gauss $(\frac{2}{p}) = (-1)^k$.

Precisamos mostrar que $k \equiv \frac{p^2-1}{8} \ mod \ 2$; isto é $k \in \mathbb{Z}/2\mathbb{Z}$, e consequentemente k é par se e somente se $\frac{p^2-1}{8}$ é par.

$p - 1 = 4k$ e $p + 1 = 4k + 2$.

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

$k \equiv \frac{P^2-1}{8} mod 2$. Se k é par $\Leftrightarrow \frac{p^2-1}{8}$ é par

Se k é ímpar $\Leftrightarrow \frac{p^2-1}{8}$ é ímpar.

2° Caso)

Para $p = 4k - 1$, k inteiro positivo $\Rightarrow \frac{p-1}{2} = 2k - 1$, teremos

$\{1, 2, ..., \frac{p-1}{2}\} \cup \{\frac{p+1}{2}, ..., p-1\} = \{1, 2, ..., 2k-1\} \cup \{2k, ..., 2(2k-1)\}$

$p = 4k - 1 = 2k + 2k - 1 \equiv 0 \ mod \ p \Rightarrow 2k \equiv (-2k + 1) \ mod \ p$.

Considerando o sistema reduzido $\{1, 2, ..., 2k - 1\}$, temos

$2.1 \equiv 2 \ mod \ p$

$2.2 \equiv 4 \ mod \ p$

$\vdots$

$2.(k-1) \equiv 2(k-1)\ mod\ p$

$2.k \equiv -2k+1\ mod\ p$

$\vdots$

$2.(2k-1) = 4k-1-1 \equiv -1\ mod\ p$

Não existe mudança de sinal nas $k-1$ primeiras equações de congruência, e existe k mudanças de sinal nas demais equações, novamente temos $(\frac{2}{p}) = (-1)^k$.

Sabemos que $p-1 = 4k-2$ e $p+1 = 4k$, temos $\frac{p^2-1}{8} = 2k^2 - k \Rightarrow k \equiv \frac{p^2-1}{8}\ mod\ 2$, concluindo que k é par $\Longleftrightarrow \frac{p^2-1}{8}$ é par. Assim $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

■

Caracterização dos números primos p para os quais o número 2 é um resíduo quadrático. Para p um número primo ímpar deve ocorrer que p é congruente a 1,3,5,ou 7.

Se $p \equiv 1\ mod\ 8 \Rightarrow p-1 = 8k$ e $p+1 = 8k+2$. Logo,

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

Se $p \equiv 7\ mod\ 8 \Rightarrow p-7 = 8k$, $p-1 = 8k+6$ e $p+1 = 8k+8$. Logo,

$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8k+6)(8K+8)}{8} = \frac{2(4k+3)8(k+1)}{8} = 2(4k+3)(k+1)$ é par.

Sabemos que $-1 \equiv 7 mod 8$. Assim se $p \equiv \pm 1 mod 8 \Rightarrow \frac{p^2-1}{8}$ é par.

Se $p \equiv 3 mod 8 \Rightarrow p-3 = 8k$, $p-1 = 8k+2$ e $p+1 = 8k+4$. Logo,

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

Se $p \equiv 5\ mod\ 8 \Rightarrow p-5 = 8k$, $p-1 = 8k+4$ e $p+1 = 8k+6$. Logo,

$\frac{p^2-1}{8} = \frac{4(2k+1)2(4k+3)}{8} = (2k+1)(4k+3)$ é ímpar.

Como $-3 \equiv 5\ mod\ 8$, temos que para $p \equiv \pm 3\ mod\ 8 \Rightarrow \frac{p^2-1}{8}$ é ímpar concluindo que:

Proposição 3.2 *Para p primo ímpar,*

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

Lei da Reciprocidade Quadrática

A lei da reciprocidade quadrática diz que para os números p e q primos ímpares, as congruências $x^2 \equiv p \ mod \ q$ e $x^2 \equiv q \ mod \ p$ são ambas solúveis ou ambas insolúveis, a menos que p e q sejam congruentes a 3 módulo 4, caso em que uma terá solução e a outra não, em outras palavras p é um quadrado módulo q se e somente se q é um quadrado módulo p, exceto no caso em que $p \equiv 3 \ mod \ 4$ e $q \equiv 3 \ mod \ 4$, quando p é um quadrado módulo q se e somente se q não é um quadrado módulo p.

3.2 Teorema da Lei da Reciprocidade Quadrática

Para primos ímpares p e q distintos, temos:
i) $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
ii) Leis suplementares:
$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ e $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

Uma das demonstrações que usa o Lema de Gauss é devido a Ferdinand Gottohold Eisenstein (1823 - 1853). Eisenstein usa uma variante do Lema de Gauss, a idéia é conhecer o número de mudança de sinais nas congruências $aa_i \equiv (-1)^{s(i)}a_{t(i)} \ mod \ m$ e utiliza a função seno para obter esse resultado, mas anteriormente vamos relembrar algumas propriedades da função seno e considerar um caso particular com a finalidade de ilustrar e facilitar o entendimento do que será feito na demonstração.
Usaremos a denotação sin para seno.
Dada a congruência $a \equiv b \ mod \ m \Rightarrow a = b + mr$ para algum r $\in \mathbb{Z}$, através da função $sin\frac{2\pi}{m}$ temos:
$sin\frac{2\pi}{m}a = sin2\pi\frac{a}{m} = sin2\pi(\frac{b}{m} + r) = sin2\pi\frac{b}{m}cos2\pi r + sin2\pi r cos2\pi\frac{b}{m} =$
$= sin2\pi\frac{b}{m}.1 + 0.cos2\pi\frac{b}{m} = sin2\pi\frac{b}{m}.$
A função seno é uma função $\mathbb{Z}$ - periódica, capaz de transformar congruência $a \equiv b \ mod \ m$ na equação $sin2\pi\frac{a}{m} = sin2\pi\frac{b}{m}$, e é uma função ímpar, isto é $sin2\pi(-x) = -sin2\pi x$.

No caso especial para a constante $a = 2$ e $m = 13$. Consideremos o sistema reduzido $\{1, 2, 3, 4, 5, 6\}$, e transformamos as congruências em equações como descritas acima, us-

ando o fato da função seno ser uma função ímpar e

$2.1 \equiv 2 \ mod\ 13,\ sin 2\pi\frac{2.1}{13} = sin 2\pi\frac{2}{13}$

$2.2 \equiv 4 \ mod\ 13,\ sin 2\pi\frac{2.2}{13} = sin 2\pi\frac{4}{13}$

$2.3 \equiv 6 \ mod\ 13,\ sin 2\pi\frac{2.3}{13} = sin 2\pi\frac{6}{13}$

$2.4 \equiv -5 \ mod\ 13,\ sin 2\pi\frac{2.4}{13} = -sin 2\pi\frac{5}{13}$

$2.5 \equiv -3 \ mod\ 13,\ sin 2\pi\frac{2.5}{13} = -sin 2\pi\frac{3}{13}$

$2.6 \equiv -1 \ mod\ 13,\ sin 2\pi\frac{2.6}{13} = -sin 2\pi\frac{1}{13}$

Efetuando a multiplicação entre os termos da igualdade nas congruências e a mesma operação nas equações, temos:
$2^6 6! \equiv (-1)^3 6! \ mod\ 13,$

$$\prod_{a=1}^{6} \sin 2\pi\frac{2a}{13} = (-1)^3 \prod_{a=1}^{6} \sin 2\pi\frac{a}{13}$$

$$(-1)^3 = \prod_{a=1}^{6} \frac{\sin 2\pi\frac{2a}{13}}{\sin 2\pi\frac{a}{13}}.$$

Se r é o número de mudanças de sinais nas congruências, podemos expressar $(-1)^r$ como um produto de valores da função seno.

Generalizando para p primo ímpar da forma $p = 2n + 1$.

Lema 3.1 *Seja $p = 2n + 1$ um número primo ímpar, $q \in \mathbb{Z}$, e a função $f : \mathbb{Q} \to \mathbb{C}$ com as seguintes propriedades*
i) $f(-z) = -f(z)$ para todo $z \in \mathbb{Q}$; (f é uma função ímpar)
ii) $f(r) = f(r + z)$ para algum $z \in \mathbb{Z}$; (f é uma função periódica)
iii) $f(\frac{a}{p}) \neq 0$ para todo inteiro a não divisível por p. Então

$(\frac{q}{p}) = \prod_{a\in A} \frac{f(\frac{q.a}{p})}{f(\frac{a}{p})}$, *onde* $A = \{1, 2, ..., \frac{p-1}{2}\} = \{1, 2, ..., n\}$.

Demonstração: Consideremos que $a_i.q \equiv (-1)^{s(i)} a_{t(i)}$ *mod* p, para a_i, $a_{t(i)} \in A$, $s(i) \in \{0, 1\}$.

Através de f transformamos a congruência na equação

$$f(a_i\frac{q}{p}) = f[(-1)^{s(i)}\frac{a_t(i)}{p}] = (-1)^{s(i)} f(\frac{a_t(i)}{p})$$

Como a_i e $a_{t(i)} \in A$ são incongruentes podemos efetuar o produto sobre todos os $a_i \in A$.

$\prod_{i=1}^{n} f(a_i\frac{q}{p}) = \prod_{i=1}^{n}(-1)^{s(i)} f(\frac{a_{t(i)}}{p}) = \prod_{i=1}^{n}(-1)^{s(i)} \prod_{i=1}^{n} f(\frac{a_t(i)}{p}) = (\frac{q}{p})\prod_{i=1}^{n} f(\frac{a_i}{p})$, obtendo

$$(\frac{q}{p}) = \frac{\prod_{i=1}^{n} f(a_i\frac{q}{p})}{\prod_{i=1}^{n} f(\frac{a_i}{p})}$$

■

Duas funções que satisfazem as propriedades da função f são:

1) $f(x) = (-1)^{\lfloor 2x \rfloor}$, onde $\lfloor 2x \rfloor$ é o maior inteiro menor do que ou igual a 2x, com x $\in \mathbb{Q}$.

2) $f(x) = \sin 2\pi x$.

Proposição 3.3 *Seja* $A = \{\alpha \in \mathbb{Z}$ *tal que* $1 \leq \alpha \leq \frac{p-1}{2}\}$, *um sistema reduzido módulo p, com p primo ímpar, então*

$(\frac{q}{p}) = \prod_{\alpha\in A} \frac{\sin(\frac{2\pi}{p}q\alpha)}{\sin(\frac{2\pi}{p}\alpha)}$, *onde consideramos* $f(x) = \sin 2\pi x$.

Na demonstração do Teorema da Reciprocidade Quadrática usaremos a expressão $\frac{\sin qz}{\sin z} = P(\sin z)$, onde P é um polinômio de variável $\sin z$ com coeficientes inteiros e coeficiente dominante $(-4)^{\frac{q-1}{2}}$. Essa prova é feita por indução.

Pela fórmula de Euler sabemos que:

$e^{it} = \cos t + i \sin t$, com $t \in \mathbb{R}$.

Para α e β reais, $e^{i(\alpha+\beta)} = e^{i\alpha+i\beta} = e^{i\alpha}e^{i\beta} = (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \cos\alpha.\cos\beta - \sin\alpha.\sin\beta + i(\cos\alpha.\sin\beta + \sin\alpha.\cos\beta)$.

$e^{i(\alpha+\beta)} = \cos(\alpha+\beta) + i\sin(\alpha+\beta)$.

Comparando as partes reais e imaginárias das duas expressões, temos
$\cos(\alpha+\beta) = \cos\alpha.\cos\beta - \sin\alpha.\sin\beta$
$\sin(\alpha+\beta) = \sin\alpha.\cos\beta + \sin\beta.\cos\alpha$

Determinemos fórmulas para $\sin qz$ e $\cos qz$, sabendo que:
$\sin 2z = 2\sin z\cos z$ e $\cos 2z = \cos^2 z - \sin^2 z = 1 - 2\sin^2 z$
$\sin 3z$=$\sin(z+2z)$=$\sin z\cos 2z + \sin 2z\cos z$=$\sin z(1-2\sin^2 z) + (2\sin z\cos z)\cos z$=$\sin z - 2\sin^3 z + 2\sin z\cos^2 z$=$\sin z - 2\sin^3 z + 2\sin z(1-\sin^2 z)$=$\sin z - 2\sin^3 z + 2\sin z - 2\sin^3 z$= $\sin z(3-4\sin^2 z)$

$\cos 3z$=$\cos(z+2z)$=$\cos z\cos 2z - \sin z\sin 2z$=$\cos z(1-2\sin^2 z) - \sin z(2\sin z\cos z)$=$\cos z - 2\cos z\sin^2 z - 2\sin^2 z\cos z$=$\cos z - 4\cos z\sin^2 z$=$\cos z(1-4\sin^2 z)$

Lema 3.2 *Para todo inteiro ímpar $q \geq 1$, existem polinômios P e $Q \in \mathbb{Z}[X]$ de grau $q-1$ e com coeficiente dominante $(-4)^{\frac{q-1}{2}}$ tal que*

$$\frac{\sin qz}{\sin z} = P(\sin z), \quad \frac{\cos qz}{\cos z} = Q(\cos z).$$

Demonstração: Para $q=1$, $\frac{\sin z}{\sin z} = 1 = (-4)^0.1(\sin z)^0$, e $\frac{\cos z}{\cos z} = 1$.
Para $q=3$, $\frac{\sin 3z}{\sin z} = \frac{\sin z(3-4\sin^2 z)}{\sin z} = -4\sin^2 z + 3$
$\frac{\cos 3z}{\cos z} = \frac{\cos z(1-4\sin^2 z)}{\cos z} = -4\sin^2 z + 1$

Por indução consideremos que para q inteiro ímpar, seja verdadeiro
$\frac{\sin qz}{\sin z} = P(\sin z) \Rightarrow \sin qz = \sin z\ P(\sin z)$ e $\frac{\cos qz}{\cos z} = Q(\sin z) \Rightarrow \cos qz = \cos z\ Q(\sin z)$,são polinômios de grau $q-1$ e coeficiente dominante $(-4)^{\frac{q-1}{2}}$, e provemos que é verdadeiro para o número ímpar $q+2$.

$\sin(q+2)z = \sin qz.\cos 2z + \sin 2z.\cos qz =$
$=\sin z.P(\sin z)(1-2\sin^2 z) + 2\cos z.\sin z.\cos z.Q(\sin z) =$
$=\sin z[P(\sin z)(1-2\sin^2 z) + 2\cos^2 z.Q(\sin z)] =$
$=\sin z[P(\sin z)(1-2\sin^2 z) + 2(1-\sin^2 z).Q(\sin z)].$

$\frac{\sin(q+2)z}{\sin z} = (1-2\sin^2 z)P(\sin z) + 2(1-\sin^2 z)Q(\sin z)$

Isso indica que $\frac{\sin(q+2)z}{\sin z}$ é um polinômio em $\sin z$ cujo grau é maior que o grau de P em duas unidades, onde grau P = grau Q, com coeficiente dominante
$(-4)^{\frac{q-1}{2}}(-2-2) = (-4)^{\frac{q-1}{2}}(-4) = (-4)^{\frac{q+1}{2}}$.

Com o mesmo procedimento podemos calcular

$\cos(q+2)z = \cos qz.\cos 2z - \sin qz.\sin 2z =$
$=\cos z.Q(\sin z)(1-2\sin^2 z) - \sin z.P(\sin z)2\sin z\cos z =$
$=\cos z[(1-2\sin^2 z)Q(\sin z) - 2\sin^2 z.P(\sin z)]$
Assim $\frac{\cos(q+2)z}{\cos z}$ é um polinômio em $\sin z$ dois graus superior ao grau de P e de Q, e possui coeficiente dominante $(-4)^{\frac{q+1}{2}}$

Ao considerarmos o polinômio $f(z) = \frac{\sin 2\pi qz}{\sin 2\pi z}$ que possui raízes quando $z = \pm\frac{\beta}{2q}$, onde β são todos os inteiros não divisíveis por q.
Se fizermos $\sin 2\pi z = X$, teremos $\frac{\sin 2\pi qz}{\sin 2\pi z} = P(\sin 2\pi z) = P(X)$ é um polinômio de grau $q-1$ em X e $P(X)$ possui raízes quando $X = \sin 2\pi(\pm\frac{\beta}{q})$, com β número inteiro não divisível por q.
Como a função seno é $\mathbb{Z}$ - periódica podemos restringir os valores de X distintos que são raízes de $P(X)$, isto é para valores $\pm\frac{\beta}{q}$ com $1 \leq \beta \leq \frac{q-1}{2}$ gera os diferentes zeros de $P(X)$.
O grau de $P(X) = q-1$, então não tem outras raízes, somente $q-1$ raízes sem repetição.
■

Proposição 3.4 *Sejam f e g polinômios mônicos(coeficiente dominante igual a 1) de grau n com coeficientes em um corpo F. Se f e g possuem em comum n raízes, então $f = g$.*

Demonstração: O polinômio $f-g$ é de grau $<$ n (os termos x^n se cancelam) as raízes comuns de f e g são também raízes de $f-g$, mas sobre corpos, os polinômios não-nulos podem ter uma quantidade maior de raízes que o grau do polinômio. Assim o polinômio $f-g$ pode não ter n raízes distintas, a menos que $f-g$ seja o polinômio nulo.
■

Demonstração: (Teorema da Reciprocidade Quadrática) $P(X) = P(\sin 2\pi z) = \frac{\sin 2\pi qz}{\sin 2\pi z}$ é um polinômio com coeficiente dominante $(-4)^{\frac{q-1}{2}}$ de grau $q-1$, e com raízes $\pm \sin 2\pi \frac{\beta}{q}$, onde $1 \leq \beta \leq \frac{q-1}{2}$

Para $f(X) = (-4)^{\frac{q-1}{2}} \prod_{\beta=1}^{\frac{q-1}{2}} (X^2 - \sin^2 2\pi \frac{\beta}{q})$ de grau $q-1$, cujas raízes são $\pm \sin 2\pi \frac{\beta}{q}$, onde $1 \leq \beta \leq \frac{q-1}{2}$.

Pela proposição anterior $P(X) = f(X)$. Colocando $X = \sin 2\pi z$, temos

$$\frac{\sin 2\pi qz}{\sin 2\pi z} = (-4)^{\frac{q-1}{2}} \prod_{\beta \in B} (\sin^2 2\pi z - \sin^2 2\pi \frac{\beta}{q}).$$

Para $z = \frac{\alpha}{p}$, temos

$$\frac{\sin 2\pi \frac{q\alpha}{p}}{\sin 2\pi \frac{\alpha}{p}} = (-4)^{\frac{q-1}{2}} \prod_{\beta \in B} (\sin^2 2\pi \frac{\alpha}{p} - \sin^2 2\pi \frac{\beta}{q}), \text{ com } \alpha \in A \text{ e } \beta \in B \text{ onde}$$

$A = \{1, ..., \frac{p-1}{2}\}$ e $B = \{1, ..., \frac{q-1}{2}\}$.

Pela proposição 3.3

$$(\frac{q}{p}) = \prod_{\alpha \in A} \frac{\sin(2\pi \frac{q\alpha}{p})}{\sin(2\pi \frac{\alpha}{p})} = \prod_{\alpha \in A} (-4)^{\frac{q-1}{2}} \prod_{\beta \in B} (\sin^2 2\pi \frac{\alpha}{p} - \sin^2 2\pi \frac{\beta}{q}) =$$

$$= (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{\alpha \in A} \prod_{\beta \in B} (\sin^2 2\pi \frac{\alpha}{p} - \sin^2 2\pi \frac{\beta}{q}) =$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} 4^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{\beta \in B} \prod_{\alpha \in A} (\sin^2 2\pi \frac{\beta}{q} - \sin^2 \pi \frac{\alpha}{p}) =$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{\beta \in B} 4^{\frac{p-1}{2}} \prod_{\alpha \in A} (\sin^2 2\pi \frac{\beta}{q} - \sin^2 2\pi \frac{\alpha}{p}) =$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{\beta \in B} \frac{\sin(2\frac{\pi}{q} p\beta)}{\sin(2\frac{\pi}{q}\beta)} =$$

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

■

3.3 Algumas aplicações da Lei da Reciprocidade Quadrática

1. Para primos $p > 3$, temos:

$$(\frac{3}{p}) = \begin{cases} (\frac{1}{3}) = 1 & \text{se } p \equiv 1 \ mod\ 12 \text{ ou } p \equiv 11 \ mod\ 12 \\ (\frac{2}{3}) = -1 & \text{se } p \equiv 5 \ mod\ 12 \text{ ou } p \equiv 7 \ mod\ 12 \end{cases}$$

Pela Lei da reciprocidade quadrática.

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

Pela definição do Símbolo de Legendre determinando os valores de:

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

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } \frac{p-1}{2} \text{ é par, isto é } p \equiv 1 \ mod\ 4 \\ -1 & \text{se } \frac{p-1}{2} \text{ é impar, isto é } p \equiv 3 \ mod\ 4 \end{cases}$$

Para $(\frac{p}{3}) = 1$ e $(-1)^{\frac{p-1}{2}} = 1$
e $(\frac{p}{3}) = -1$ e $(-1)^{\frac{p-1}{2}} = -1$
temos $(\frac{p}{3})(-1)^{\frac{p-1}{2}} = 1$ Temos os sistemas de congruências:

$$\begin{cases} p \equiv 1 \ mod\ 3 \\ p \equiv 1 \ mod\ 4 \end{cases}$$

$$\begin{cases} p \equiv 2 \ mod\ 3 \\ p \equiv 3 \ mod\ 4 \end{cases}$$

Pelo Teorema do Resto Chinês obtemos as soluções: $p \equiv 1\ mod\ 12$, e $p \equiv 11 \mod 12$ respectivamente.

Para $(\frac{p}{3}) = 1$ e $(-1)^{\frac{p-1}{2}} = -1$
e $(\frac{p}{3}) = -1$ e $(-1)^{\frac{p-1}{2}} = 1$
temos $(\frac{p}{3})(-1)^{\frac{p-1}{2}} = -1$, temos os sistemas de congruências:

$$\begin{cases} p \equiv 1\ mod\ 3 \\ p \equiv 3\ mod\ 4 \end{cases}$$

$$\begin{cases} p \equiv 2\ mod\ 3 \\ p \equiv 1\ mod\ 4 \end{cases}$$

com soluções $p \equiv 7\ mod\ 12$ e $p \equiv 5\ mod\ 12$, respectivamente.
Juntando as informações acima, concluimos:
$(\frac{3}{p}) = 1$ se $p \equiv 1\ mod\ 12$ ou $p \equiv 11\ mod\ 12$
$(\frac{3}{p}) = -1$ se $p \equiv 5\ mod\ 12$ ou $p \equiv 7\ mod\ 12$
■

2. O inteiro -3 é um resíduo quadrático módulo primo p $\neq 3$ se e somente se $p \equiv 1\ mod\ 3$.

Pela lei da reciprocidade quadrática temos
$(\frac{-3}{p}) = (\frac{-1.3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}(\frac{p}{3}) = (-1)^{p-1}(\frac{p}{3}) = (\frac{p}{3})$,
pois para p ímpar, p-1 é par. Assim
$(\frac{-3}{p}) = (\frac{p}{3}) = 1$ se $p \equiv 1\ mod\ 3$
■

3. Lei da Reciprocidade para Símbolos de Jacobi

Definição 3.2 *Para um inteiro positivo m relativamente primo com o inteiro positivo ímpar n com uma fatoração de primos $p_1, p_2, ..., p_r$, o Símbolo de Jacobi, denotado por $[\frac{m}{n}]$, é definido por:*
$[\frac{m}{n}] = (\frac{m}{p_1})(\frac{m}{p_2})...(\frac{m}{p_r})$

onde os símbolos à direita da igualdade são Símbolos de Legendre.

Sejam m e n inteiros ímpares positivos relativamente primos então

$(\frac{m}{n})(\frac{n}{m}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$
e as leis suplementares
$(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$; $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$

A prova consistirá em reduzir a lei da reciprocidade em Símbolos de Jacobi para a lei da reciprocidade para Símbolos de Legendre.
Considerando $n = p_1\ p_2\ ...\ p_r$ onde $(\frac{-1}{p_i}) = (-1)^{\frac{p_i-1}{2}}$, então
$(\frac{-1}{n}) = (\frac{-1}{p_1})...(\frac{-1}{p_r}) = (-1)^{\frac{p_1-1}{2}+...+\frac{p_r-1}{2}}$.
Usaremos a indução para mostrar que $\frac{n-1}{2} \equiv (\frac{p_1-1}{2} + ... + \frac{p_r-1}{2})\ mod\ 2$
Seja $n = p_1p_2$ com p_1 e p_2 ímpares , temos $p_1 - 1$ e $p_2 - 1$ são pares, temos $(p_1 - 1) + (p_2 - 1) \equiv 0\ mod\ 4$, sabendo que p_1p_2 é ímpar e $p_1p_2 - 1$ é par assim $p_1p_2 - 1 \equiv (p_1 - 1) + (p_2 - 1)\ mod\ 4$, dividindo por 2 obtemos
$\frac{p_1p_2-1}{2} \equiv (\frac{p_1-1}{2} + \frac{p_2-1}{2})\ mod\ 2$
Para $n = p_1p_2...p_r$ ímpar, com p_1, ... ,p_r ímpares e $p_1 - 1$, ...,$p_r - 1$ pares teremos $n - 1$ é par e $n - 1 \equiv 0\ mod\ 4$ e $((p_1 - 1) + (p_2 - 1) + ... + (p_r - 1)) \equiv 0\ mod\ 4$, obtendo
$n - 1 \equiv ((p_1 - 1) + (p_2 - 1) + ... + (p_r - 1))\ mod\ 4$, dividindo por 2, temos
$\frac{n-1}{2} \equiv ((\frac{p_1-1}{2}) + ... + (\frac{p_r-1}{2}))\ mod\ 2$
Assim $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$

Consideremos m,n ímpares escritos na forma fatorada,
$m = p_1\ p_2\ ...\ p_r,\ \ n = q_1\ q_2\ ...\ q_s$
$\frac{m-1}{2} \equiv (\frac{p_1-1}{2} + ... + \frac{p_r-1}{2})\ mod\ 2 = \sum_{i=1}^{r} \frac{p_i - 1}{2}\ mod\ 2$
$\frac{n-1}{2} \equiv (\frac{q_1-1}{2} + ... + \frac{q_s-1}{2})\ mod\ 2 = \sum_{j=1}^{s} \frac{q_j - 1}{2}\ mod\ 2$

$\frac{m-1}{2}\frac{n-1}{2} \equiv \sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2}\ mod\ 2$

$(\frac{m}{n}) = (\frac{p_1\ \dots\ p_r}{q_1\ \dots\ q_s}) = (\frac{p_1}{q_1})(\frac{p_2}{q_1})\ \dots\ (\frac{p_r}{q_1})\ \dots\ (\frac{p_1}{q_s})\ \dots\ (\frac{p_r}{q_s}) = \prod_{\substack{i=1\\j=1}}^{\substack{s\\r}}(\frac{p_i}{q_j})$

De forma análoga temos

$(\frac{n}{m}) = \prod_{\substack{j=1\\i=1}}^{\substack{r\\s}}(\frac{q_j}{p_i})$

$(\frac{m}{n})(\frac{n}{m}) = \prod_{i=1}^{r}\prod_{j=1}^{s}(\frac{p_i}{q_j})(\frac{q_j}{p_i}) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} =$

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

Novamente por indução mostraremos que:

$\frac{n^2-1}{8} \equiv \frac{p_1^2-1}{8} + \ \dots\ + \frac{p_r^2-1}{8}\ mod\ 2$

$p_1^2p_2^2 - 1 \equiv\ 0\ mod\ 16$ e $(p_1^2-1)+(p_2^2-1) \equiv 0\ mod\ 16$, assim

$p_1^2p_2^2 - 1 \equiv (p_1^2-1)+(p_2^2-1)\ mod\ 16$, dividindo por 8 obtemos

$\frac{p_1^2p_2^2-1}{8} \equiv (\frac{p_1^2-1}{8} + \frac{p_2^2-1}{8})\ mod\ 2$

Para $n\ =\ p_1\ p_2\ \dots\ p_r$, teremos

$\frac{n^2-1}{8} \equiv (\frac{p_1^2-1}{8} + \ \dots\ + \frac{p_r^2-1}{8})\ mod\ 2.$

$(\frac{2}{n}) = (\frac{2}{p_1})\ \dots\ (\frac{2}{p_r}) = (-1)^{\frac{p_1^2-1}{8}}\ \dots\ (-1)^{\frac{p_r^2-1}{8}} = (-1)^{\frac{p_1^2-1}{8}+\dots+\frac{p_r^2-1}{8}}\ mod\ 2 \equiv (-1)^{\frac{n^2-1}{8}}.$

■

O Símbolo de Legendre $(\frac{a}{p})$ fornece informação se a é um resíduo quadrático módulo p, isto é, se a congruência $x^2 \equiv a\ mod\ p$ tem solução, o que não ocorre com o Símbolo de Jacobi.

A asserção da Lei da Reciprocidade Quadrática de Euler/ Gauss diz que:

Para dois primos ímpares distintos p e q, ambos os símbolos de Legendre $(\frac{q}{p})$ e $(\frac{p}{q})$ estão definidos. A questão que surge é, o que acontece, se trocarmos neles os papéis de p e q ?, ou seja: O que tem a ver a questão se q é um resíduo quadrático módulo p com a questão se p é um resíduo quadrático módulo q ?.

Para um número ímpar m temos que $\frac{m-1}{2}$ é par se $m \equiv 1 mod 4$, enquanto ímpar se $m \equiv 3 mod 4$. Assim, o produto $\frac{p-1}{2}\frac{q-1}{2}$ é ímpar (par) se ambos p e q são $\equiv 3 mod 4$ (pelo menos

um de p ou q é $\equiv 1 mod 4$).

Logo a lei da reciprocidade quadrática diz que podemos simplesmente trocar p e q se pelo menos um de p ou q é $\equiv 1 mod 4$. Porém, se $p \equiv q \equiv 3 mod 4$, o símbolo invertido troca de sinal.

Os resíduos quadráticos, os Triplos Pitagóricos e a Lei da Reciprocidade Quadrática fornecem elementos para determinar as coordenadas dos pontos que satisfazem a equação de uma cônica.

No último capítulo é abordado a fatoração de um número inteiro utilizando pontos sobre o círculo unitário.

É possível conhecer a estrutura do grupo que contém os pontos que satisfazem a equação da cônica $y^2 - ax^2 \equiv 1 \ mod \ p$ ao determinar se a é um resíduo quadrático ou não. A versão original do Lema de Gauss é diferente da versão apresentada. Considere um número primo ímpar $p = 2m + 1$ e seja o sistema reduzido $A = \{\overline{1}, \overline{2}, ..., \overline{m}\}$. Para averiguar se a é um resíduo quadrático, multiplica-se todo elemento de A por a e faz-se o produto módulo p tal que o resto tenha valor mínimo absoluto, isto é um elemento em A dependendo do sinal. Em seguida seleciona os resíduos no conjunto $\{\overline{1}, \overline{2}, ..., \overline{p-1}\}$. Se existirem r resíduos negativos, na versão original do Lema de Gauss, esses resíduos estão no conjunto $\{\overline{m+1}, ..., \overline{2m}\}$. Em outras palavras:

Seja $p = 2m + 1$ um número primo ímpar, a um inteiro não divisível por p, e $A = \{\overline{1}, ..., \overline{m}\}$ um sistema reduzido módulo p.

Escrevemos $a \ . \ i = pq_i + r_i; \ \ 1 \leq r_i \leq p-1$ para $1 \leq i \leq m$, onde $q_i = \lfloor \frac{ai}{p} \rfloor$ é o maior inteiro $\leq \frac{ai}{p}$. Então $(\frac{a}{p}) = (-1)^r$, onde r é o número de resíduos r_i que são $> \frac{p}{2}$.

Capítulo 4

Pontos racionais sobre cônicas e fatoração de inteiros

As cônicas são estudadas desde a antiguidade, Apolônio de Perga (262 - 190 a.C) estudo-as em sua obra "As cônicas"' consistindo em oito livros. Séculos depois Nicolau Copérnico (1473 - 1543) como um astrônomo revolucionou a visão da Astronomia ao conseguir colocar a Terra movendo-se em torno do Sol. Posteriomente Isaac Newton (1642 - 1727) obteve que as possíveis trajetórias dos objetos em nosso sistema solar são exatamente as cônicas. Essas trajetórias podem ser descritas por equações da forma $ax^2 + by^2 = r^2$, com a e b > 0 descreve uma elípse, quando $a = b = 1$ temos o círculo de raio r, no caso em que $a > 0, b < 0$ obtem-se hipérboles. As equações como $y = ax^2 + bx + c$ descrevem parábolas para $a \neq 0$.

O estudo das cônicas será feito sobre os anéis cujos elementos são classes de resíduos ou classes de restos no anel $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Se tomarmos como exemplo $\mathbb{Z}/5\mathbb{Z}$, o círculo unitário sobre $\mathbb{Z}/5\mathbb{Z}$ é o conjunto dos pontos (x, y) com x *e* $y \in \mathbb{Z}/5\mathbb{Z}$ tal que $x^2 + y^2 \equiv 1 \ mod\ 5$, isto é: teremos o conjunto $\{(0,1),(1,0),(-1,0),(0,-1)\}$.Ao desenharmos esse círculo, o resultado não é o círculo que conhecemos na geometria euclidiana, porisso necessitamos de sermos exatos quando usamos a intuição geométrica para estudar objetos como esses.

4.1 Ternos Pitagóricos

Definição 4.1 *Um Terno Pitagórico consiste de três números inteiros não nulos (a,b,c) com* $a^2 + b^2 = c^2$

Definição 4.2 *O Terno Pitagórico é chamado primitivo se o* $mdc(a, b, c) = 1$ *(isto é: a,b,c, são primos entre si).*

Dividindo a equação $a^2 + b^2 = c^2$ por $d^2 = [mdc(a, b, c)]^2$ e colocando $\frac{a}{d} = x$ e $\frac{b}{d} = y$, temos um Terno Pitagórico primitivo $(x, y, 1)$ que corresponde aos pontos com valores racionais que pertencem ao círculo unitário $x^2 + y^2 = 1$, que são os elementos do conjunto

$C(\mathbb{Q}) = \{(x, y)\ com\ x\ e\ y \in \mathbb{Q}$ tal que $x^2 + y^2 = 1\}$.

Existem vários métodos para determinar todos os pontos racionais sobre o círculo unitário. Leopold Kronecker (1823-1891) forneceu dois métodos para deduzir as fórmulas dos Ternos Pitagóricos.

Uma delas é baseada na parametrização do círculo C por funções trigonométricas,onde $x = cos\ \alpha$ e $y = sin\ \alpha$ é uma parametrização do círculo $C(\mathbb{R}) = \{(x, y)\ com\ x,\ y \in \mathbb{R}$ tal que $x^2 + y^2 = 1\}$, através de funções trigonométricas.

As identidades trigonométricas $cos^2\alpha + sin^2\alpha = 1$ e $cos^2\alpha - sin^2\alpha = cos2\alpha$, nos fornecem os valores de x e y através de um parâmetro m.

$$x = cos\alpha = cos2\tfrac{\alpha}{2} = \frac{cos^2\frac{\alpha}{2} - sin^2\frac{\alpha}{2}}{cos^2\frac{\alpha}{2} + sin^2\frac{\alpha}{2}} = \frac{1 - tg^2\frac{\alpha}{2}}{1 + tg^2\frac{\alpha}{2}} = \frac{1 - m^2}{1 + m^2}$$

$$y = sin\alpha = sin2\tfrac{\alpha}{2} = \frac{2sin\frac{\alpha}{2}cos\frac{\alpha}{2}}{cos^2\frac{\alpha}{2} + sin^2\frac{\alpha}{2}} = \frac{2\frac{sin\frac{\alpha}{2}}{cos\frac{\alpha}{2}}}{1 + \frac{sin^2\frac{\alpha}{2}}{cos^2\frac{\alpha}{2}}} = \frac{2tg\frac{\alpha}{2}}{1 + tg^2\frac{\alpha}{2}} = \frac{2m}{1 + m^2}.$$

onde $m = tg\frac{\alpha}{2}$.

Ao escolher um valor racional para m, obtemos um ponto racional sobre o círculo C.

Inversamente, se x e y são números racionais e $y \neq 0$, temos $m = tg\frac{\alpha}{2} = \sqrt{\frac{1-x}{1+x}}$, consequentemente: $m^2 = \frac{1-x}{1+x}$ logo $1 + m^2 = \frac{2}{1+x}$, sabendo que $x = \frac{1-m^2}{1+m^2}$ e $y = \frac{2m}{1+m^2}$.

Assim, $1 + m^2 = \frac{2m}{y}$ e $1 + m^2 = \frac{2}{1+x}$, igualando as duas expressões obtemos: $m = \frac{y}{1+x}$ que também é um número racional.

Essa parametrização fornece todos os pontos racionais $(x, y) \neq (-1, 0)$ sobre o círculo

unitário C.

Uma das melhores deduções conhecidas para as fórmulas dos Ternos Pitagóricos é a parametrização dos pontos racionais sobre o círculo unitário C através da técnica de deslizamento de retas. Consideremos um ponto P sobre o círculo unitário C, seja $P = (-1, 0)$ e tracemos as retas l passando por P com uma declividade racional m, a equação $y = m(x + 1)$ define a reta l que intercepta o círculo C em um segundo ponto $P_m = (\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2})$.

Inversamente, um ponto racional Q sobre o círculo unitário C com $Q \neq (-1, 0)$ define uma reta PQ com declividade racional. Assim, a função $\varphi : m \longmapsto P_m$ é uma bijeção entre o conjunto $\mathbb{Q}$ dos números racionais e o conjunto dos pontos racionais sobre o círculo unitário C diferentes de $(-1, 0)$.

$\varphi : \mathbb{Q} \to C(\mathbb{Q}) - \{P\}$.

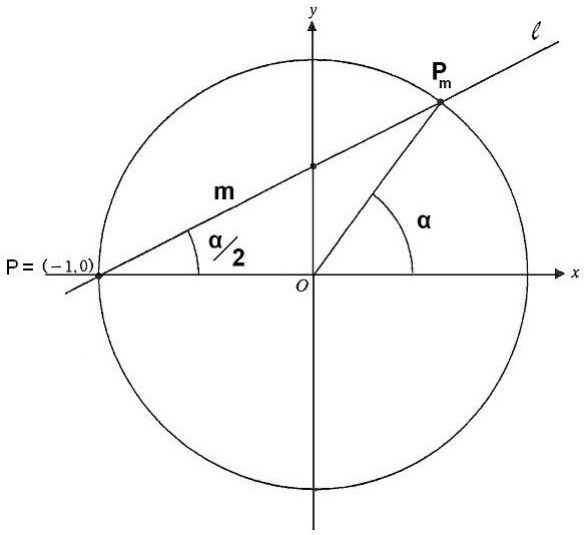

Figura 4.1: Círculo unitário e reta com declividade m

Exemplo 4.1 *O ponto* $(\frac{a}{c}, \frac{b}{c}) = (\frac{4}{5}, \frac{3}{5}) \in C(Q)$. *Para determinar os números inteiros x e y tais que* $(x, y) \in C(\mathbb{Z}/7\mathbb{Z})$ *satisfazendo a equação* $x^2 + y^2 \equiv 1 \ mod\ 7$, *primeiramente resolvemos a equação* $5w \equiv 1 \ mod\ 7$ *cuja solução é* $w = 3$, *pois* $15 \equiv 1 \ mod\ 7$.

Em seguida consideramos: $(\frac{a}{c}, \frac{b}{c}) = (\frac{4.3}{5.3}, \frac{3.3}{5.3}) = (12, 9) = (5, 2)$, *sabendo que:*

$12 \equiv 5 \ mod\ 7$ *e* $9 \equiv 2 \ mod\ 7$. *Assim o ponto* $(5, 2) \in C(\mathbb{Z}/7\mathbb{Z})$.

4.2 O círculo unitário sobre anéis arbitrários

A definição de $C(\mathbb{Q})$ pode ser generalizada para anéis arbitrários R que são comutativos e possuem elemento unidade 1.

Consideremos $C(R) = \{(x, y) \text{ com } x,\ y \in anel\ R \text{ tal que } x^2 + y^2 = 1\}$

Se R é um anel finito, então C(R) também é finito, logo podemos determinar sua cardinalidade.

Seja o anel $R = \mathbb{Z}/n\mathbb{Z}$.

Para o círculo $C(\mathbb{Z}/n\mathbb{Z}) = \{(x, y) \text{ com } x, y \in \mathbb{Z}/n\mathbb{Z} \text{ tal que } x^2 + y^2 = 1\}$, utilizamos o método de encontrar todos os pontos sobre $C(\mathbb{Q})$ adaptando-o ao círculo unitário $C(\mathbb{Z}/n\mathbb{Z})$.

A reta que inicia no ponto $P = (-1, 0)$ com declividade $m \in \mathbb{Z}/n\mathbb{Z}$ intercepta o círculo $C(\mathbb{Z}/n\mathbb{Z})$ no segundo ponto $P_m = (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})$ onde $m.d.c(1 + m^2, n) = 1$, pois se $m.d.c(1 + m^2, n) \neq 1$ podemos ter $m^2 + 1 \equiv 0\ mod\ n$ e conseguentemente não será possível determinar P_m.

Reciprocamente, se $Q = (x, y)$ é um ponto diferente de $(-1, 0)$ sobre o círculo unitário $C(\mathbb{Z}/n\mathbb{Z})$, então $Q = P_m$ para algum $m = \frac{y}{x+1} \in \mathbb{Z}/n\mathbb{Z}$, desde que $m.d.c(1 + x, n) = 1$.

Para $n = 2$, $C(\mathbb{Z}/2\mathbb{Z}) = \{(1, 0), (0, 1)\}$

Seja p primo ímpar, existem duas possibilidades para p em termos de congruência modulo 4, $p \equiv 1\ mod\ 4$ ou $p \equiv 3\ mod\ 4$.

Se $p \equiv 3\ mod\ 4$, então $m.d.c(m^2 + 1, p) = 1$ para todo m, assim para cada $m \in \mathbb{Z}/p\mathbb{Z}$ obtemos um ponto sobre $C(\mathbb{Z}/p\mathbb{Z})$.

Para m, n $\in \mathbb{Z}/p\mathbb{Z}$ com $m \neq n$ temos $P_m \neq P_n$.

Supondo que $P_m = P_n$, isto é;

$$(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}) = (\frac{1-n^2}{1+n^2}, \frac{2n}{1+n^2})$$

Igualando as coordenadas x: $\frac{1-m^2}{1+m^2} = \frac{1-n^2}{1+n^2}$

multiplicando ambos os lados da igualdade por $(1 + m^2)(1 + n^2)$ e simplificando os denominadores,obtemos,

$(1 + n^2)(1 - m^2) = (1 + m^2)(1 - n^2)$, obtendo

$m^2 = n^2$, assim, $m^2 \equiv n^2 \ mod \ p$, isto é; $m \equiv \pm n \ mod \ p$, substituindo na coordenada y segue,

$$\frac{2m}{1+m^2} \equiv \frac{2n}{1+n^2} \ mod \ p$$

Como $m^2 \equiv n^2 \ mod \ p$, podemos ter que $1 + m^2 \equiv (1 + n^2) \ mod \ p$, consequentemente $m \equiv n \ mod \ p$, concluindo que para $m \neq n$ teremos $P_m \neq P_n$.

Os pontos de$C(\mathbb{Z}/p\mathbb{Z})$ que não são obtidos, são aqueles que $mdc(x + 1, p) \neq 1$, isto é:

$x \equiv -1 \ mod \ p$.

$(x + 1 \equiv 0 \ mod \ p)$; $(x, y) = (-1, 0)$.

Assim podemos ter uma função bijetora entre $\mathbb{Z}/p\mathbb{Z}$ e $C(\mathbb{Z}/p\mathbb{Z}) - \{(-1, 0)\}$.

É possível determinar a cardinalidade de $C(\mathbb{Z}/p\mathbb{Z})$ através da cardinalidade de $\mathbb{Z}/p\mathbb{Z}$.

Proposição 4.1 *Para p primo ímpar, existem* $p - (\frac{-1}{p})$ *pontos sobre* $C(\mathbb{Z}/p\mathbb{Z})$.

Demonstração: $p = \#(\mathbb{Z}/p\mathbb{Z}) = \#\{C(\mathbb{Z}/p\mathbb{Z}) - \{(-1, 0)\}$, logo a $\#C(\mathbb{Z}/p\mathbb{Z}) = p + 1$

Se $p \equiv 1 \ mod \ 4$, temos que -1 é um resíduo quadrático módulo p, isto é:

$m^2 \equiv -1 \ mod \ p \Rightarrow m^2 + 1 \equiv 0 \ mod \ p$, possui duas soluções (a saber m e $-m$).

Assim a cardinalidade de $\mathbb{Z}/p\mathbb{Z}$ é igual a cardinalidade de $\{C(\mathbb{Z}/p\mathbb{Z}) + \{(-1, 0)\}\}$, logo $\#(C(\mathbb{Z})) = p - 1$ ■

4.3 O grupo sobre o círculo

História dos Grupos sobre Cônicas.

O conceito de grupos abstratos desenvolveu-se lentamente, os axiomas desses grupos tornaram-se conhecidos após o ano de 1890. Os de grupos abstratos foram descobertas primeiramente para o conjunto dos números complexos. Quando Gauss identificou o conjunto dos pontos sobre o círculo de centro $(0, 0)$ e raio 1 com o conjunto $\mathbb{C}$ dos números complexos com valor absoluto igual a 1, definiu implicitamente uma lei de grupo sobre o círculo com a operação multiplicação em $\mathbb{C}$.

A estrutura de grupos algébricos sobre o círculo unitário foi definida primeiramente sobre anéis finitos $R = \mathbb{Z}/n\mathbb{Z}$ e não sobre $\mathbb{Q}$. Schönemann (1839) mostrou que o conjunto

$C(\mathbb{Z}/n\mathbb{Z}) = \{(x, y)\ com\ x,\ y \in \mathbb{Z}/n\mathbb{Z}\ tal\ que\ x^2 + y^2 \equiv 1\ mod\ n\}$ é fechado com relação à operação adição:
$(x, y) \oplus (x', y') = (xx' - yy',\ xy' + x'y)$. A definição de Schönemann foi algébrica, mas Juel (1896) definiu geometricamente a lei de grupo sobre cônicas.

O círculo unitário $C(\mathbb{R})$ no plano euclideano é descrito como o conjunto dos pontos $(x, y) \in \mathbb{R} \times \mathbb{R}$ satisfazendo a equação $x^2 + y^2 = 1$, o qual pode ser parametrizado pelas funções trigonométricas.

Seja a função $\varphi : \mathbb{R} \to C(\mathbb{R})$ definida por: $\varphi(\alpha) = (cos2\pi\alpha, sin2\pi\alpha)$
sobre o círculo unitário associando a todo arco de comprimento $\alpha \in \mathbb{R}$ o ponto $\varphi(\alpha)$ sobre $C(\mathbb{R})$.
Se $\varphi(\alpha + n) = \varphi(\alpha)$ para algum n $\in \mathbb{Z}$, a função φ cobre o círculo infinitas vezes.
Seja $\mathbb{R}/\mathbb{Z} = \{\alpha + \mathbb{Z}, \alpha \in \mathbb{R}\}$, o conjunto quociente de $\mathbb{Z}$ em $\mathbb{R}$.
A função φ induz a uma função bijetora $\mu : \mathbb{R}/\mathbb{Z} \to C(\mathbb{R})$.
Para $x + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$, $\mu(x + \mathbb{Z}) = P \in C(\mathbb{R})$.
O elemento neutro $(1, 0) \in C(\mathbb{R})$, então existe $x + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ tal que
$\mu(x + \mathbb{Z}) = (1, 0) = \varphi(x) = (\cos 2\pi x, \sin 2\pi x)$.
$\cos 2\pi x = 1$ e $\sin 2\pi x = 0$, temos $x = 0$
$\mu(0 + \mathbb{Z}) = (1, 0)$, assim o núcleo de $\mu = \{0 + \mathbb{Z}\}$, o que mostra que μ é injetora.
Para qualquer ponto P $\in C(\mathbb{R})$, existe $\alpha \in \mathbb{R}$ tal que $\varphi(\alpha) = P$, mas $\varphi(\alpha) = \varphi(\alpha + n)$ para todo $n \in \mathbb{Z}$, logo $\alpha + n$ pertence à classe lateral $\alpha + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ tal que $P = \mu(\alpha + \mathbb{Z})$, provando que μ é sobrejetora.

O conjunto $\mathbb{R}/\mathbb{Z}$ é um grupo aditivo abeliano ao definirmos a operação adição entre seus elementos como sendo:
Para todos $\alpha_1 + \mathbb{Z}$, $\alpha_2 + \mathbb{Z}$ em $\mathbb{R}/\mathbb{Z}$
$\alpha_1 + \mathbb{Z} + \alpha_2 + \mathbb{Z} = (\alpha_1 + \alpha_2) + \mathbb{Z}$
Usando a função φ, podemos tornar o círculo unitário $C(\mathbb{R})$ em um grupo abeliano. Para somar dois pontos P_1 e P_2 sobre o círculo, determinamos as imagens inversas $\alpha_1 = \mu^-1(P_1)$ e $\alpha_2 = \mu^-1(P_2)$ e colocando $P_1 \oplus P_2 = \mu(\alpha_1 + \alpha_2)$
Para cada ponto P sobre o círculo unitário define um ângulo $\sphericalangle NOP$, onde $O = (0, 0)$ e

$N = (1, 0)$ e somando pontos sobre o círculo estamos somando seus ângulos correspondentes.

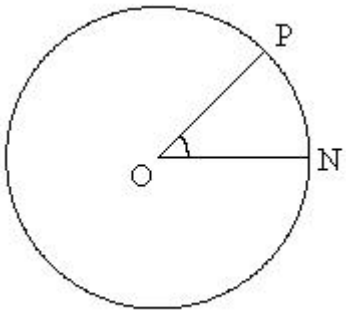

Figura 4.2: Círculo unitário com ângulo determinado por dois pontos

Para deduzir a lei que define a operação entre os pontos $P_j = (x_j, y_j)$ com $j = 1, 2$; e determinar $\alpha_j \in \mathbb{R}$ (definido módulo $\mathbb{Z}$) com $x_j = \cos 2\pi\alpha_j$ e $y_j = \sin 2\pi\alpha_j$, tomamos os pontos:

$P_1 = (x_1, y_1) = (\cos 2\pi\alpha_1, \sin 2\pi\alpha_1)$.

$P_2 = (x_2, y_2) = (\cos 2\pi\alpha_2, \sin 2\pi\alpha_2)$.

As fórmulas de adição de arcos para as funções seno e cosseno nos fornecem,

$\cos 2\pi(\alpha_1 + \alpha_2) = \cos 2\pi\alpha_1 . \cos 2\pi\alpha_2 - \sin 2\pi\alpha_1 . \sin 2\pi\alpha_2 = x_1.x_2 - y_1.y_2$.

$\sin 2\pi(\alpha_1 + \alpha_2) = \cos 2\pi\alpha_1 . \sin 2\pi\alpha_2 + \cos 2\pi\alpha_2 . \sin 2\pi\alpha_1 = x_1.y_2 + x_2.y_1$.

Se $P_1 \oplus P_2 = \mu(\alpha_1 + \alpha_2) = (\cos 2\pi(\alpha_1 + \alpha_2), \sin 2\pi(\alpha_1 + \alpha_2))$, temos;

$P_1 \oplus P_2 = (x_1, y_1) + (x_2, y_2) = (x_1.x_2 - y_1.y_2, x_1.y_2 + x_2.y_1)$.

Ao considerar um anel comutativo R com elemento unidade, podemos definir $C(R) = \{(x, y) com\ x,\ y \in R\ tal\ que\ x^2 + y^2 = 1\}$ como o conjunto de pontos sobre o círculo com coordenadas no anel R e fazer de $C(R)$ um grupo com a operação adição acima.

Em $C(R)$ o elemento neutro é $(1, 0) = \mu(0 + \mathbb{Z})$.

Suponhamos que o elemento neutro seja $(e_1, e_2) \in C(R)$ tal que:

$(x, y) \oplus (e_1, e_2) = (x, y)$, para $(x, y) \in C(R)$.

$(xe_1 - ye_2, xe_2 + ye_1) = (x, y)$

Ao resolver o sistema linear,

$xe_1 - ye_2 = x$

$ye_1 + xe_2 = y$

temos o resultado: $e_1 = 1$ e $e_2 = 0$.

O elemento simétrico de (x, y) em $C(R)$ é $(x, -y)$.
$\mu(\alpha + \mathbb{Z}) = (x, y)$ onde $x^2 + y^2 = 1$.
Supondo que o inverso de (x, y) em $C(R)$ seja (a, b) tal que:
$(x, y) \oplus (a, b) = (1, 0)$
$(xa - yb, xb + ya) = (1, 0)$
Resolvendo o sistema linear com variáveis a e b, obtemos $a = x$ e $b = -y$, assim
$-(x, y) = (x, -y)$.
Provando a propriedade associativa
$[(x_1, y_1) \oplus (x_2, y_2)] \oplus (x_3, y_3) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) + (x_3, y_3) =$
$= (x_1x_2x_3 - y_1y_2y_3 - x_1y_2y_3 - x_2y_2y_3 - x_2y_1y_3, x_1x_2y_3 + x_1x_2y_3 + x_2x_3y_1 - y_1y_2y_3) =$
$= [x_1(x_2x_3 - y_2y_3) - y_1(y_2x_3 + x_2x_3), x_1(x_2y_2 + x_3y_2) + y_1(x_2x_3 - y_2y_3)] =$
$= (x_1, y_1) + [(x_2x_3 - y_2y_3, x_2y_3 + x_3y_2)] = (x_1y_1) \oplus [(x_2, y_2) \oplus (x_3, y_3)]$.
As demonstrações das demais propriedades são imediatas.

Proposição 4.2 *Sejam o círculo C definido pela equação $x^2 + y^2 = 1$, o ponto $N = (1, 0)$ sobre o círculo C e o anel comutativo R com elemento unidade. Então a operação adição para pontos no conjunto $C(R) = \{(x, y)\ com\ x,\ y\ em\ R\ tal\ que\ x^2 + y^2 = 1\}$ com elemento neutro N tal que $C(R)$ é grupo dada por:*
$(r, s) \oplus (t, u) = (rt - su, ru + st)$.

Demonstração: Para adicionar os pontos $P = (r, s)$ e $Q(t, u)$ pertencentes ao círculo, traçamos por N uma reta paralela ao segmento PQ que ao interceptar o círculo determina o ponto M, obtendo o segmento de reta NM paralelo ao segmento PQ cuja declividade é $m = \dfrac{s - u}{r - t}$. Assim a reta NM possui a mesma declividade e tem equação $y = m(x - 1)$.
Para determinar o ponto M, fazemos a intersecção dessa reta com o círculo substituindo $x = \frac{y}{m} + 1$ na equação $x^2 + y^2 = 1$, obtendo:
$\dfrac{y}{m^2} + \dfrac{2}{m} + y^2 = 0$. Como $y \neq 0$ pois para $x = 1$ temos o ponto N, assim $\dfrac{y}{m^2} + \dfrac{2}{m} + y = 0$ resultando que $y = \dfrac{-2m}{1 + m^2}$ e $x = \dfrac{y}{m} + 1$, temos $M = (x, y)$ em função de m
Para definir a operação adição entre os pontos P e Q , precisamos determinar x e y em função das coordenadas r, s, t, u lembrando que $r^2 + s^2 = 1$ e $t^2 + u^2 = 1$

$$y = \frac{-2m}{1+m^2} = \frac{-2(\frac{s-u}{r-t})}{1+(\frac{s-u}{r-t})^2} = \frac{-2(s-u)(r-t)}{(r-t)^2(s-u)^2} =$$

$$= \frac{-2(s-u)(r-t)}{(r^2+u^2)+(s^2+t^2)-2(rt+su)} = \frac{-2(s-u)(r-t)}{2-2(rt+su)} =$$

$$= \frac{(s-u)(r-t)(ru+st)}{[-1+(rt+su)](ru+st)} = \frac{(sr-st-ur+ut)(ru+st)}{-(ru+st)+su(ru+st)+rt(ru+st)} =$$

$$= \frac{[(sr+ut)-(ru+st)](ru+st)}{-(ru+st)+ut(r^2+s^2)+sr(t^2+u^2)} =$$

$$= \frac{[(sr+ut)-(ru+st)](ru+st)}{[(sr+ut)-(ru+st)]} = ru+st.$$

$$x = \frac{y}{m}+1 = \frac{(ru+st)+\frac{s-u}{r-t}}{\frac{s-u}{r-t}} = \frac{(ru+st)(r-t)+(s-u)}{s-u} =$$

$$= \frac{r^2u-rut+str-st^2+s-u}{s-u} = \frac{tr(s-u)+s(-t^2+1)-u(1-r^2)}{s-r} =$$

$$= \frac{tr(s-u)+su^2-us^2}{s-u} = \frac{rt(s-u)-su(s-u)}{s-u} = \frac{(rt-su)(s-u)}{s-u} = rt-su.$$

Assim $(r,s) \oplus (t,u) = (rt-su, ru+st)$

■

4.4 Fatorando Inteiros com o Círculo Unitário

Dado um número inteiro S, queremos fatorar tal número como um produto de números primos utilizando pontos sobre o círculo unitário $C(\mathbb{Z}/S\mathbb{Z})$.

Lembremos que se a, m são números inteiros positivos com $m > 1$ e $mdc(a,m) = 1$, a ordem de a com respeito a m é o menor inteiro positivo i tal que $a^i \equiv 1 \ mod \ m$.

O ponto $P = (x,y)$ possui ordem k se $k.P = (1,0)$. Um ponto P é dito ser não trivial quando sua ordem não é tão pequena, em particular os pontos $P = (\pm 1, 0) e (0, \pm 1)$ são considerados

triviais, pois: $1(1,0) = (1,0)$.
$2(-1,0) = (-1,0) \oplus (-1,0) = ((-1)(-1) - 0, (-1)0 + 0(-1)) = (1,0)$. $2(-1,0) = (1,0)$;
$4(0,\pm 1) = (1,0)$.
$2(0,-1) = (0,-1) \oplus (0,-1) = (0-1, 0+0) = (-1,0)$.
$4(0,-1) = 2(0,-1) \oplus 2(0,-1) = (-1,0) \oplus (-1,0) = (1-0, 0+0) = (1,0)$.

Para $S = n^2 + 3$, temos o ponto $P = (\overline{n}, \overline{2}) \in C(\mathbb{Z}/S\mathbb{Z})$ pois $n^2 + 2^2 = n^2 + 3 + 1 = S + 1 \equiv 1 \ mod \ S$.
Para $S = n^2 + 8$, temos o ponto $P = (\overline{n}, \overline{3}) \in C(\mathbb{Z}/S\mathbb{Z})$ pois $n^2 + 3^2 = n^2 + 8 + 1 = S + 1 \equiv 1 \ mod \ S$.
Para $S = n^2 + 15$, temos o ponto $P = (\overline{n}, \overline{4}) \in C(\mathbb{Z}/S\mathbb{Z})$ pois $n^2 + 4^2 = n^2 + 15 + 1 = S + 1 \equiv 1 \ mod \ S$. Assim,

Para $S = n^2 + (q^2 - 1) \in \mathbb{Z}$.
$n^2 + q^2 = n^2 + (q^2 - 1) + 1 = S + 1 \equiv 1 mod S$.
$n^2 + q^2 \equiv 1 mod S$, assim o ponto $P = (\overline{n}, \overline{q}) \in C(\mathbb{Z}/S\mathbb{Z})$. Supomos que temos um fator primo p que divide S. Vamos verificar o que ocorre quando calculamos $kP = (x, y) = (1, 0)$ para $k = p - (\frac{-1}{p})$.
$\{kP\}$ é o conjunto dos multiplod de P e um subgrupo de $C(\mathbb{Z}/p\mathbb{Z})$.
Como a ordem do grupo $\{kP\}$ é um múltiplo da ordem de P sobre o círculo unitário $C(\mathbb{Z}/p\mathbb{Z})$ percebemos que $x \equiv 1 \ mod \ p$ e $y \equiv 0 \ mod \ p$.
Assim, para y não divisível por S podemos recorrer a um fator não trivial de S proveniente das coordenadas de kP calculando o $mdc(y, S)$ ou $mdc(x - 1, S)$. Ao substituir k por alguns múltiplos podemos obter um algoritmo de fatoração.
Se $k = p - (\frac{-1}{p})$ é composto de pequenos fatores primos, então é possível escrever um M como multiplo de k sem conhecer p. Considere um valor B como potência de 10 (digamos $B = 10, 10^2, 10^3, ...$) e formamos o produto $M = \prod p^a(p)$ onde $p^a(p)$ é a maior potência de um p primo menor do que B.
Descreveremos o algorítmo para fatorar inteiros $S = n^2 + (q^2 - 1)$.
1°) Escolha um B , coloque $m = 0$, $p_m = 1$, $P_m = (n, q)$.
2°) Seja p_{m+1} o menor $primo > p_m$, se $p_{m+1} > B$ então $S = 1.S$ (S é primo). Se $p_{m+1} < B$ escolha o maior número natural b tal que $p_{m+1}^b < B$;

3°) Determine o ponto $P_{m+1} = (x, y) = p_{m+1}^b.P_m$; se $mdc(y, S) = 1$, substitua $m + 1$ por $m + 2$ e faça o 2° passo; se
$mdc(y, S) = S$, repita o algoritmo com um menor B determinado (ou refaz o cálculo de $p_m^b P_m$ verificando se $mdc(y, S) = 1$ depois de cada passo); caso contrário coloque $mdc(y, S)$ como um fator de S.
O cálculo de $p^n P$ é feito adicionando convenientemente p^n vezes o ponto P

Exemplo 4.2 *Seja* $S = (56)^2 + (2^2 - 1) = (56)^2 + 3 = 3139$, $P_0 = (56, 2)$ *e* $B = 10$.
O primeiro primo é $p = 2$ *e* $2^3 = 8 < B$.
Calcular $P_1 = 2^3.P_0 = 8(56, 2)$.
Para facilitar o cálculo, fazemos:
$2P_0 = 2(56, 2) = (56, 2) \oplus (56, 2) = (3136 - 4, 112 + 112) = (3132, 224) = (-7, 224)$.
Sabendo que: $3132 \equiv -7$ *mod* S.
$4P_0 = (-7, 224) \oplus (-7, 224) = (-3042, -3136) = (97, 3)$, *já que* $97 \equiv -3042$ *mod* S *e* $3 \equiv -3136$ *mod* S.
$8P_0 = (97, 3) \oplus (97, 3) = (9400, 582) = (-17, 582)$, *onde* $9400 \equiv -17 mod\ S$.
Assim $P_1 = (-17, 582)$ *e* $mdc(582, S) = 1$. *Como* $mdc(y, S) = 1$ *continuamos com o primo* $p = 3$ *e* $3^2 = 9 < B$.
Para determinar $P_2 = 3^2 P_1 = 9P_1 = 8P_1 \oplus P_1$.
$2P_1 = (577, -954)$, $4P_1 = (389, 873)$, $8P_1 = (1297, 1170)$.
$9P_1 = (1520, 438)$ *e* $mdc(438, S) = 73$, *73 é um fator primo de S, assim* $S = 73.43$

Quando consideramos a lei de composição de grupo sobre o círculo unitário, determinar um ponto racional não trivial sobre ele pode não ser tão simples e imediato, então podemos substituir o círculo unitário pela cônica $y^2 + ax^2 = 1$ escolhendo aleatoriamente x e y inteiros e colocando $a \equiv \frac{1-y^2}{x^2}$ *mod* N, mas para isso precisamos da lei de composição de grupo sobre cônica.
Para $N = n^2 + (q^2 - 1)$ o ponto $(n, q) \in C(\mathbb{Z}/N\mathbb{Z})$. O coeficiente angular da reta que passa pelos pontos (n, q) e $(-1, 0)$ é $t = \dfrac{q}{1 + n}$.
Dada a função $\Phi : Q \to C(Q) \ - \{(-1, 0)\}$ sobre o círculo unitário definida por:
$\Phi(t) = (\dfrac{1 - t^2}{1 + t^2}, \dfrac{2t}{1 + t^2})$, tem-se:

$\Phi(t) = \Phi(\frac{q}{1+n}) = (n, q) \in C(Q) - \{(-1, 0)\}$.

4.5 A estrutura de $C(\mathbb{Z}/n\mathbb{Z})$

Para anéis comutativos R com unidade, qual seria o procedimento para determinar o grupo $C(R)$?

Ao tomarmos o anel $R = \mathbb{Z}/n\mathbb{Z}$ podemos determinar $C(\mathbb{Z}/n\mathbb{Z})$, faremos isso para $n = 2$ e inteiros ímpares $n \leq 15$.

Para $n = 2$. O ponto $P = (0, 1)$ em $C(\mathbb{Z}/2\mathbb{Z})$ gera o sub-grupo {(0,1),(1,0)}.

$2.(0, 1) = (0, 1) \oplus (0, 1) = (-1, 0) = (1, 0)$ em $\mathbb{Z}/2\mathbb{Z}$.

$C(\mathbb{Z}/2\mathbb{Z}) = \{(0, 1), (1, 0)\}$ e a estrutura de círculo é $\mathbb{Z}/2\mathbb{Z}$.

Para $n = 3$. $C(\mathbb{Z}/3\mathbb{Z}) = \{(0, 1), (0, -1), (1, 0), (-1, 0)\}$.

O ponto $(0, 1)$ em $(\mathbb{Z}/3\mathbb{Z})$ gera o sub-grupo $\{(0, \pm 1), (\pm 1, 0)\}$.

Logo a estrutura de $C(\mathbb{Z}/3\mathbb{Z})$ é $\mathbb{Z}/4\mathbb{Z}$.

Para $n = 5$

$C(\mathbb{Z}/5\mathbb{Z}) = \{(0, \pm 1), (\pm 1, 0)\}$, cuja estrutura é $\mathbb{Z}/4\mathbb{Z}$.

Para $n = 7$

O ponto $P = (2, 2)$ satisfaz a equação: $(\pm 2)^2 + (\pm 2)^2 \equiv 1 \ mod \ 7$.

$C(\mathbb{Z}/7\mathbb{Z}) = \{(0, \pm 1), (\pm 1, 0), (\pm 2, \pm 2)\}$ com estrutura do grupo $\mathbb{Z}/8\mathbb{Z}$.

Para $n = 9$

Os pontos $(\pm 1, \pm 3) e (\pm 3, \pm 1)$ satisfazem a equação: $(\pm 1)^2 + (\pm 3)^2 \equiv 1 \ mod \ 9$.

$C(\mathbb{Z}/9\mathbb{Z}) = \{(0, \pm 1), (\pm 1, 0), (\pm 1, \pm 3), (\pm 3, \pm 1)\}$, com estrutura do grupo $\mathbb{Z}/12\mathbb{Z}$.

Para $n = 11$

Os pontos $(\pm 3, \pm 5) e (\pm 5, \pm 3)$ satisfazem a equação: $(\pm 3)^2 + (\pm 5)^2 \equiv 1 mod 11$.

$C(\mathbb{Z}/11\mathbb{Z}) = \{(0, \pm 1), (\pm 1, 0), (\pm 3, \pm 5), (\pm 5, \pm 3)\}$ com a estrutura do grupo $\mathbb{Z}/12\mathbb{Z}$.

Para $n = 13$

Os pontos $(\pm 2, \pm 6) e (\pm 6, \pm 2)$ satisfazem equação: $(\pm 2)^2 + (\pm 6)^2 \equiv 1 \ mod \ 13$.

$C(\mathbb{Z}/13\mathbb{Z}) = \{(0, \pm 1), (\pm 1, 0), (\pm 2, \pm 6), (\pm 6, \pm 2)\}$ cuja estrutura de grupo é de $\mathbb{Z}/12\mathbb{Z}$

E para $n = 15$, os pontos $(0, \pm 4), (\pm 4, 0), (\pm 5, \pm 6), (\pm 6, \pm 5)$ além dos triviais satisfazem a equação:

$x^2 + y^2 \equiv 1 \ mod \ 15$

$C(\mathbb{Z}/15\mathbb{Z}) = \{(0, \pm 1), (\pm 1, 0), (0, \pm 4), (\pm 4, 0), (\pm 5, \pm 6), (\pm 6, \pm 5)\}$ cuja estrutura de grupo é de $\mathbb{Z}/4\mathbb{Z} \otimes \mathbb{Z}/4\mathbb{Z}$.
Observemos que $C(\mathbb{Z}/9\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$, segue que $\#\ (C(\mathbb{Z}/9\mathbb{Z})) = 12$.

Para primos $p = 3, 7, 11$ $p \equiv\ 3\ mod\ 4$ e $\#(C(\mathbb{Z}/p\mathbb{Z})) = p + 1$.
Para primo $p = 5, 13$, $p \equiv\ 1\ mod\ 4$ e $\#(C(\mathbb{Z}/p\mathbb{Z})) = p - 1$.
Para $p = 15 = 3.5$, notamos que $\#(C(\mathbb{Z}/15\mathbb{Z})) = 16$.

Proposição 4.3 *Sejam R e S anéis com unidade, e seja $\Phi : R \to S$ um homomorfismo entre anéis. Então Φ induz um homomorfismo Φ_C entre os grupos C(R) e C(S) definido por:* $\Phi_C(x, y) = (\Phi(x), \Phi(y))$.

Demonstração: Sejam x, y, x', y' $\in$ R, (x, y) e $(x', y') \in\ C(R)$, temos que:
$\Phi_C(x, y) = (\Phi(x), \Phi(y))$ e $\Phi_C(x', y') = (\Phi(x'), \Phi(y'))$.
$\Phi_C[(x, y) + (x', y')] = \Phi_C(x + x', y + y') = (\Phi(x + x', y + y')) = (\Phi(x) + \Phi(x'), \Phi(y) + \Phi(y'))$
$= (\Phi(x), \Phi(y)) + (\Phi(x'), \Phi(y')) = \Phi_C(x, y) + \Phi_C(x', y')$

■

Proposição 4.4 *Se Φ é um isomorfismo do anel R no anel S então Φ_C também é um isomorfismo de C(R) em C(S).*

Demonstração: Por hipótese Φ é um homomorfismo de R em S, pela proposição anterior Φ_C é um homomorfismo. Ao provar que Φ_C é bijetor, temos que Φ_C é um isomorfismo.
Supondo que $\Phi_C(x, y) = \Phi_C(x', y')$.
$(\Phi(x), \Phi(y)) = \Phi_C(x, y) = \Phi_C(x', y') = \Phi(x'), \Phi(y')$. Φ é um isomorfismo, obtendo que:
$\Phi(x) = \Phi(x')$ e $\Phi(y) = \Phi(y')$, concluindo que: $(x, y) = (x', y')$, logo Φ é injetor.
Seja $(u, v) \in C(S)$ tal que $(u, v) = \Phi_C(x, y)$ para algum $(x, y) \in C(R)$.
$(u, v) = \Phi_C(x, y) = (\Phi(x), \Phi(y))$, obtendo que: $u = \Phi(x)$ e $v = \Phi(y)$. Φ é um isomorfismo, logo para todo $(u, v) \in\ C(S)$, existe (x, y) *in* $C(R)$ tal que $\Phi_C(x, y) = (u, v)$. Assim Φ_C é sobrejetor

■

Proposição 4.5 *Seja o homormorfismo Φ entre os anéis R e S cujo núcleo de Φ é dado por Nuc $(\Phi) = \{x \in R$ tal que $\Phi(x) = 0\}$. O homomorfismo é injetor se, e somente se Nuc $(\Phi) = \{0\}$.*

Demonstração: Por hipótese Φ é um homomorfismo injetor e $\Phi(0) = 0$ seja a $\in$ R tal que $\Phi(a) = 0_S$, então $a = 0_R$. Assim o núcleo de $\Phi = \{0_R\}$
Se o núcleo de $\Phi = \{0_R\}$ *e* $\Phi(a) = \Phi(b)$, então $0_S = \Phi(a) - \Phi(b) = \Phi(a - b)$ e
$a - b = 0_R$ ou $a = b$. Logo Φ é injetor.

■

Proposição 4.6 *Se $\Phi : R \to S$ é um homomorfismo injetor entre anéis, então $\Phi_C : C(R) \to C(S)$ também é um homomorfismo injetor.*

Demonstração: Seja $P = (x, y) \in C(R)$ e suponhamos que $\Phi_C(x, y) = (1, 0)$ assim $(1, 0) = (\Phi(x), \Phi(y))$.
Φ é um homomorfismo injetor, assim, $x = 1$ *e* $y = 0$
$\Phi_C(1, 0) = (1, 0) \Rightarrow \Phi_C^{-1}(1, 0) = \{(1, 0)\} \Rightarrow \Phi_C$ é um homomorfismo injetor. ■

Se $\Phi : R \to S$ for um homomorfismo sobrejetor entre R e S, o homomorfismo $\Phi_C : C(R) \to C(S)$ não precisa ser sobrejetor.
Por exemplo $\Phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ é um homomorfismo sobrejetor, mas $\Phi_C : C(\mathbb{Z}) \to C(\mathbb{Z}/n\mathbb{Z})$ geralmente não é um homomorfismo sobrejetor, pois $C(\mathbb{Z}) = \{(\pm 1, 0), (0, \pm 1)\}$.
Temos que $\mathbb{Z}/m.n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$, para m,n inteiros com $m.d.c(m, n) = 1$.

Das proposições 4.3, 4.4 e 4.5, segue que:

Corolário 4.1 *Se m e n são inteiros com $m.d.c(m, n) = 1$, então $C(\mathbb{Z}/m.n\mathbb{Z}) \cong C(\mathbb{Z}/m\mathbb{Z}) \otimes C(\mathbb{Z}/n\mathbb{Z})$.*

Isso reduz o problema ao determinar a estrutura de $C(\mathbb{Z}/m\mathbb{Z})$ quando m é uma potência de um número primo, $(m = p^n)$.

4.6 Construção de Corpos

Proposição 4.7 *Se $\mathbb{K}$ é um corpo de característica $\neq 2$ e se $x \in \mathbb{K}$ não é um quadrado, então*

$L = \{a + b\sqrt{x}$ tal que $a, b \in \mathbb{K}\}$ é um corpo com as operações adição e multiplicação definida por:

$(a + b\sqrt{x}) + (c + d\sqrt{x}) = (a + c) + (b + d)\sqrt{x}$

$(a + b\sqrt{x}).(c + d\sqrt{x}) = (ac + bdx) + (ad + bc)\sqrt{x}.$

Esse corpo é denotado por $L = \mathbb{K}(\sqrt{x})$.

Demonstração: (L,+) é um grupo comutativo com elemento neutro $0 = 0 + 0\sqrt{x}$, e o elemento simétrico de $a + b\sqrt{x}$ é $-a - b\sqrt{x}$.

$(L^* = L - \{0\}, .)$ é um grupo comutativo com elemento unidade $1 = 1 + 0\sqrt{x}$.

Para $a + b\sqrt{x} \neq 0$ seu inverso $(a + b\sqrt{x})^{-1} = \frac{a}{a^2 - b^2x} - \frac{b}{a^2 - b^2x}\sqrt{x}$

com $a^2 - b^2x \neq 0$.

Esse resultado é obtido quando admitimos que existe $c + d\sqrt{x} \in L - \{0\}$ tal que:

$(a + b\sqrt{x}).(c + d\sqrt{x}) = 1 + 0\sqrt{x}$.

Para provar que $a^2 - b^2x \neq 0$, usamos a contradição, supondo que $a^2 - b^2x = 0$, se $b = 0$ $\Rightarrow a^2 = 0 \Rightarrow a = 0$, temos $a + b\sqrt{x} = 0 + 0\sqrt{x}$ o que contradiz a hipótese, se $b \neq 0$ então $x = (\frac{a}{b})^2 \Rightarrow x$ é um quadrado; absurdo, pois por hípótese x não é um quadrado.

Provando a propriedade associativa para a operação multiplicação.

Dados $a + b\sqrt{x}, c + d\sqrt{x}, e + f\sqrt{x} \in L - \{0\}$

$[(a + b\sqrt{x})(c + d\sqrt{x})](e + f\sqrt{x}) = [ac + bdx + (ad + bc)\sqrt{x}]$.

$.(e + f\sqrt{x}) = ace + bdex + adfx + bcfx + (acf + bdfx + ade + bce)\sqrt{x}$

Por outro lado $(a + b\sqrt{x})[(c + d\sqrt{x}).(e + f\sqrt{x})=$

$= (a + b\sqrt{x})[ce + dfx + (cf + de)\sqrt{x}]=$

$ace + adfx + bcfx + bdex + (acf + ade + bce + bdfx)\sqrt{x}$

Para a propriedade distributiva é válido:

$[(a + b\sqrt{x}) + (c + d\sqrt{x}].(e + f\sqrt{x}) = [a + c + (b + d)\sqrt{x}].(e + f\sqrt{x}) =$

$= ae + ce + bfx + dfx + (af + cf + be + de)\sqrt{x} =$

$[ae + bfx + (af + be)\sqrt{x}] + [ce + dfx + (cf + de)\sqrt{x}] =$

$= (a + b\sqrt{x})(e + f\sqrt{x}) + (c + d\sqrt{x})(e + f\sqrt{x}).$

As demais propriedades de corpo são de verificação imediata. ■

Considerando $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, se $x \in \mathbb{K}$ é um resíduo não-quadrático modulo p, então $L = \mathbb{K}(\sqrt{x})$ é um corpo.

$L = \mathbb{K}(\sqrt{x}) = \{a + b\sqrt{x}$ com $a, b, x \in \mathbb{Z}/p\mathbb{Z}\}$
Para cada $a \in \mathbb{Z}/p\mathbb{Z}$ temos p possibilidades em $\mathbb{Z}/p\mathbb{Z}$, logo temos $p.p = p^2$ possibilidades de formamos o elemento $a + b\sqrt{x}$ em $(\mathbb{Z}/p\mathbb{Z})(\sqrt{x})$.
Assim $(\mathbb{Z}/p\mathbb{Z})(\sqrt{x})$ é um corpo finito com p^2 elementos.
Um corpo finito com n elementos é denotado $\mathbb{F}_n$
Uma questão interessante é saber quantos corpos finitos com p^2 elementos existem.
Temos $\frac{p-1}{2}$ resíduos não quadráticos modulo p, e para $x \in corpo\ \mathbb{K}$ e sendo um resíduo não quadrático, então construímos $\frac{p-1}{2}$ corpos.
Se x e y são resíduos não quadráticos, então existe $z \in \mathbb{Z}/p\mathbb{Z}$ com $y = xz^2$, obtendo $\sqrt{y} = z\sqrt{x}$ o elemento $a + b\sqrt{y} \in (\mathbb{Z}/p\mathbb{Z})(\sqrt{y})$ é $a + bz\sqrt{x} \in (\mathbb{Z}/p\mathbb{Z})(\sqrt{x})$ concluimos que esses corpos são isomorfos.
Para toda potência p^n de um número primo p existe um corpo finito com p^n elementos.

4.7 A cardinalidade de $C(\mathbb{F}_q)$

Na seção 4.5 vimos que para p primo ímpar $\#(C(\mathbb{Z}/p\mathbb{Z}))$ é $p+1$ quando $p \equiv 3\ mod\ 4$ ou $p-1$ quando $q \equiv 1\ mod\ 4$, o que sugere $C(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/(p \pm 1)\mathbb{Z})$.
Ao determinar a estrutura do corpo $\mathbb{F}_q$ com $q = p^n$, obtem-se $C(\mathbb{F}_q) \cong (\mathbb{Z}/(q \pm 1)\mathbb{Z})$ para primos $p \equiv \pm 1 mod 4$, onde a característica de $\mathbb{F}_q \neq 2$.
Podemos determinar a cardinalidade de $C(\mathbb{F}_q)$ da seguinte forma:

Proposição 4.8 *Se $\mathbb{K} = \mathbb{F}_q$ é um corpo de característica $\neq 2$, então*

$$\#(C(\mathbb{K})) = \#(C(\mathbb{F}_q)) = \begin{cases} q-1 & se\ q \equiv 1\ mod\ 4 \\ q+1 & se\ q \equiv 3\ mod\ 4 \end{cases}$$

Demonstração: Seja a equação $y^2 - ax^2 = 1$, p um número primo ímpar, $\mathbb{F}_q$ um corpo finito. Para $a = -1 \in \mathbb{F}_q$,temos o círculo $C(\mathbb{F}_q)$. Consideremos as duas possibilidades: $q \equiv 1\ mod\ 4$ e $q \equiv 3\ mod\ 4$.
Para $q \equiv 1\ mod\ 4$, sabemos que:

$a = -1$ é um resíduo quadrático módulo q, temos $(\frac{-1}{q}) = 1$.
Se $y = 0$, então $x^2 \equiv 1 \ mod \ q \Leftrightarrow x \equiv \pm 1 \ mod \ q$, e $(\frac{1}{q}) = 1 \Rightarrow 1 \ \in \mathbb{F}_q$. Assim existem dois pontos $(\pm 1, 0)$ sobre o círculo $C(\mathbb{F})_q)$.
Se $x = 0$, então $y^2 \equiv 1 \ mod \ q \Leftrightarrow y \equiv \pm 1 \ mod \ q$, portanto existem dois pontos $(0, \pm 1)$ sobre o círculo $C(\mathbb{F}_q)$, assim temos quatro pontos sobre $C(\mathbb{F}_q)$ cujas coordenadas pertencem a $\mathbb{F}_q$.
Seja o conjunto $L_q = \{2, 3, ..., q-2\} \subset \mathbb{F}_q$, considerando as restantes classes de resíduos módulo q, então existem $\frac{q-5}{2}$ elementos y em L_q tais que $1 - y^2$ é um quadrado. Seja $t^2 = 1 - y^2$ para algum t $\in \mathbb{F}_q^*$.
Então $x^2 \equiv t^2 \ mod \ q \Leftrightarrow x \equiv \pm t \ mod \ q$.
Se (t, y) é solução de $y^2 - (-1)x^2 = 1$ então $(-t, y)$ também é solução, logo (t, y) e $(-t, y)$ $\in C(\mathbb{F}_q)$.
Para cada y $\in L_q$ tal que $1 - y^2$ é um quadrado, temos dois pontos $(\pm t, y)$ sobre $C(F_q)$,assim existem $2.(\frac{q-5}{2}) = q - 5$ pontos sobre $C(\mathbb{F}_q)$ com $y \in L_q$.
Sabemos que existem quatro pontos $(\pm 1, 0)$ e $(0, \pm 1)$ sobre $C(\mathbb{F}_q)$, assim existe um total de $q - 5 + 4 = q - 1$ pontos sobre $C(\mathbb{F}_q)$.

Para $q \equiv 3 \ mod \ 4$, sabemos que:
$a = -1$ não é um resíduo quadrático. Se $y = 0$, então
$x^2 \equiv 1 \ mod \ q \Leftrightarrow x \equiv \pm 1 \ mod \ q$ portanto $(-1, 0)$ e $(1, 0) \in C(\mathbb{F}_q)$.

Se $x = 0$, então $y^2 \equiv 1 \ mod \ q \Leftrightarrow y \equiv \pm 1 \ mod \ q$
Assim existem dois pontos $(0, \pm 1) \in C(\mathbb{F}_q)$.
Como anteriormente, existem $\frac{q-3}{2}$ elementos y em L_q tais que $1 - y^2$ é um quadrado. Seja $t^2 = 1 - y^2$ para algum t $\in L_q$. Então
$x^2 \equiv t^2 \ mod \ q \Leftrightarrow x \equiv \pm t \ mod \ q$.
Se $(t, y) \in C(\mathbb{F}_q)$ então $(-t, y) \in C(\mathbb{F}_q)$.
Para cada y $\in L_q$ com $1 - y^2$ temos dois pontos sobre $C(\mathbb{F}_q)$, assim existem $2.(\frac{q-3}{2}) = q - 3$ pontos sobre $C(\mathbb{F}_q)$.
Conhecemos quatro pontos $(\pm 1, 0)$ e $(0, \pm 1)$ em $C(\mathbb{F}_q)$,totalizando $q - 3 + 4 = q + 1$ pontos racionais sobre $C(\mathbb{F}_q)$ demonstrando a proposição.

■

4.8 O Grupo sobre Cônicas

Para definir o grupo sobre a cônica$\mathfrak{C}$ diferente do círculo dada pela equação $y^2 - ax^2 = 1$, escolhemos uma operação $\oplus$ sobre quaisquer dois pontos P e Q pertencentes a essa cônica, conforme a proposição seguinte:

Proposição 4.9 *Seja a cônica* $\mathfrak{C}(R)$ *sobre um anel R, a um elemento não nulo de R e o ponto* $N = (0,1)$ *sobre a cônica* $\mathfrak{C}$. *Então a lei de grupo sobre o conjunto* $\mathfrak{C}(R) = \{(x,y)\ com\ x,\ y\ em\ R\ tal\ que\ y^2 - ax^2 = 1\}$ *com elemento neutro N e operação adição para pontos de* $\mathfrak{C}(R)$ *é dada por:*
$(r,s) \oplus (t,u) = (ru + st, rt + asu)$ *e o inverso de* $(r,s) = (-r,s)$.

Demonstração: Para adicionar os pontos $P = (r,s)$ e $Q = (t,u)$ pertencente à cônica, traçamos por N uma reta paralela ao segmento PQ que ao interceptar a cônica determina o ponto M , obtendo o segmento de reta NM paralelo ao segmento PQ cuja declividade é $m = \frac{s-u}{r-t}$. Assim a reta NM possui a mesma declividade e tem equação $y = mx + 1$.
Para determinar o ponto M, fazemos a intersecção dessa reta com a cônica substituindo $mx + 1$ na equação $y^2 - ax^2 = 1$, obtendo $m^2x^2 + 2mx - ax^2 = 0$. Como $x \neq 0$ pois para $x = 0$ temos o ponto N, assim $m^2x + 2m - ax = 0$ resultando que $x = \frac{2m}{a-m^2}$ e $y = mx + 1$ $= \frac{a+m^2}{a-m^2}$, temos $M = (x,y)$
Para definir a operação adição entre os pontos P e Q , precisamos determinar x e y em função das coordenadas r, s, t, u, a, lembrando que $s^2 - ar^2 = 1$ e $u^2 - at^2 = 1$
Como $m = \dfrac{s-u}{r-t}$ temos,

$$x = \frac{2m}{a-m^2} = \frac{2(s-u)(r-t)}{a(r-t)^2 - (s-u)^2} = \frac{2(s-u)(r-t)}{(ar^2 - s^2) + (at^2 - u^2) - 2art + 2st + 2su} =$$

$$= \frac{2(s-u)(r-t)}{-1-1-2art+2su} = = -\frac{(s-u)(r-t)}{1+art-su} = = -\frac{(s-u)(r-t)(ru+st)}{(1+art-su)(ru+st)} =$$

$$= -\frac{[(rs+ut)-(ru+st)](ru+st)}{(ru+st)+rs(at^2-u^2)+tu(ar-s^2)} = = -\frac{[(rs+ut)-(ru+st)](ru+st)}{(ru+st)-(rs+tu)} = ru+st$$

Assim $x = ru + st$

Para obter y usamos m e x acima.

$y = mx + 1 = \frac{s-u}{r-t}(ru + st) + 1 = \frac{sru + s^2t - ru^2 - ust + r - t}{r-t} =$

$= \frac{su(r-t) + t(s^2-1) - r(u^2-1)}{r-t} = = \frac{su(r-t) + tar^2 - rat^2}{r-t} =$

$= \frac{su(r-t) + atr(r-t)}{r-t} = = su + atr.$

Assim $y = su + atr$.

Concluindo que a operação adição de dois pontos sobre a cônica fica definida por:

$P \oplus Q = (r, s) \oplus (t, u) = (ru + st, su + art)$

Seja $(r, s) \in \mathfrak{C}(R)$ e (x, y) o simétrico de (r, s), tal que $(r, s) \oplus (x, y) = (0, 1)$, assim $(ry + sx, sy + arx) = (0, 1)$. resolvendo o sistema obtemos, $(x, y) = (-r, s)$.

■

Vamos considerar R = $\mathbb{F}_p$ e o conjunto de pontos sobre a cônica dado por:

$\mathfrak{C}_{p,a}(\mathbb{F}_p) = \{(x, y),\ com\ x,\ y,\ a \in \mathbb{F}_p\ tal\ que\ y^2 - ax^2 = 1\}$

Teorema 4.1 *Sejam $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, e p um primo ímpar que não divide a, então:*

$$\#(\mathfrak{C}_{p,a}(\mathbb{F}_p) = p - (\frac{a}{p}) = \begin{cases} p-1 & se\ (\frac{a}{p}) = 1 \\ p+1 & se\ (\frac{a}{p}) = -1 \end{cases}$$

Demonstração: Seja $\mathbb{F}_p$ um corpo finito e a $\in \mathbb{F}_p^*$. Consideremos as duas possibilidades: $p \equiv 1\ mod\ 4$ e $p \equiv 3\ mod\ 4$.

Para $p \equiv 1\ mod\ 4$, temos dois casos:

i) a é um resíduo quadrático módulo p, temos $(\frac{a}{p}) = 1$. Se $y = 0$, então
$ax^2 \equiv -1 \ mod \ p \Leftrightarrow x^2 \equiv -\frac{1}{a} \ mod \ p \Leftrightarrow x \equiv \pm\sqrt{-\frac{1}{a}} \ mod \ p$, então $(-\frac{1}{a}) = 1$ devido a $(\frac{a}{p}) = 1$, portanto $\sqrt{-\frac{1}{a}} \in \mathbb{F}_p$
Assim existem dois pontos $(\pm\sqrt{-\frac{1}{a}}, 0)$ sobre a cônica $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Se $x = 0$, então $y^2 \equiv 1 \ mod \ p \Leftrightarrow y \equiv \pm 1 \ mod \ p$, portanto existem dois pontos $(0, \pm 1)$ sobre a cônica $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, assim temos quatro pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ cujas coordenadas pertencem a $\mathbb{F}_p$.
Seja o conjunto $L_p = \{2, 3, ..., p-2\} \subset \mathbb{F}_p$, considerando as restantes classes de resíduos módulo p, então existem $\frac{p-5}{2}$ elementos y em L_p tais que $\frac{y^2-1}{a}$ é um quadrado. Seja $t^2 = \frac{y^2-1}{a}$ para algum t $\in \mathbb{F}_p^*$.
Então $x^2 \equiv t^2 \ mod \ p \Leftrightarrow x \equiv \pm t \ mod \ p$.
Se (t, y) é solução de $y^2 - ax^2 = 1$ então $(-t, y)$ também é solução, logo (t, y) e $(-t, y)$ $\in \mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Para cada y $\in L_p$ tal que $\frac{y^2-1}{a}$ é um quadrado, temos dois pontos $(\pm t, y)$ sobre
$\mathfrak{C}_{p,a}(\mathbb{F}_p)$,assim existem $2.(\frac{p-5}{2}) = p - 5$ pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Sabemos que existem quatro pontos $(\pm\sqrt{\frac{1}{a}}, 0)$ e $(0, \pm 1)$ sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, assim existe um total de $p - 5 + 4 = p - 1$ pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.

ii) a não é um resíduo quadrático módulo p, temos $(\frac{a}{p}) = -1$. Se $y = 0$, então $ax^2 \equiv -1 mod p \Leftrightarrow x^2 \equiv -\frac{1}{a} \ mod \ p \Leftrightarrow x \equiv \pm\sqrt{\frac{-1}{a}} \ mod \ p$, obtemos que $(\frac{-1}{a}) = -1$, devido a $(\frac{a}{p}) = -1$, portanto $\sqrt{\frac{-1}{a}} \notin \mathbb{F}_p$, logo não existe pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.

Se $x = 0$, então $y^2 \equiv 1 \ mod \ p \Leftrightarrow y \equiv \pm 1 \ mod \ p$, obtemos dois pontos $(0, \pm 1)$ $\in \mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Existem $\frac{p-1}{2}$ elementos y em L_p tais que $\frac{y^2-1}{a}$ é um quadrado. Seja $t^2 = \frac{y^2-1}{a}$ para algum $t \in \mathbb{F}_p^*$.
Então $x^2 \equiv t^2 \ mod \ p \Leftrightarrow x \equiv \pm t \ mod \ p$.
Temos (t, y) e $(-t, y) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$, mas quando $\frac{y^2-1}{a}$ é um quadrado para y $\in L_p$ temos dois pontos $(\pm t, y)$ sobre a cônica $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, assim existem $2.(\frac{p-1}{2}) = p - 1$ pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Já sabemos que $(0, \pm 1) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$, logo teremos um total de pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ igual a

$p-1+2=p+1$.

Para $p \equiv 3 \ mod \ 4$, consideremos os dois casos:

i) Seja $(\frac{a}{p}) = 1$. Se $y = 0$, então
$ax^2 \equiv -1 \ mod \ p \Leftrightarrow x^2 \equiv \frac{-1}{a} \ mod \ p \Leftrightarrow x \equiv \sqrt{\frac{-1}{a}} \ mod \ p$, $(\frac{-1}{p}) = -1$, quando $p \equiv 3 \ mod \ 4$, isto é -1 não é um resíduo quadrático módulo p, assim $(\frac{-1}{a}) = -1$, portanto $\sqrt{\frac{-1}{a}} \notin \mathbb{F}_p$. Logo não existem pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.

Se $x = 0$, então $y^2 \equiv 1 \ mod \ p \Leftrightarrow y \equiv \pm 1 \ mod \ p$.
Assim existem dois pontos $(0, \pm 1)$ sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Existem $\frac{p-3}{2}$ elementos y em L_p tais que $\frac{y^2-1}{a}$ é um quadrado. Seja $\frac{y^2-1}{a} = t^2$ para algum t $\in \mathbb{F}_p$.
Então $x^2 \equiv t^2 \ mod \ p \Leftrightarrow x \equiv \pm t \ mod \ p$.
Temos os pontos (t, y) e $(-t, y) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$, mas quando $\frac{y^2-1}{a}$ é um quadrado para y $\in L_p$ temos dois pontos $(\pm t, y)$ sobre a cônica $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, assim existem $2.(\frac{p-3}{2}) = p-3$ pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, mas $(0, \pm 1) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$, então teremos um total de $p-3+2 = p-1$ pontos racionais sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.

ii) Seja $(\frac{a}{p}) = -1$. Se $y = 0$, então
$ax^2 \equiv -1 \ mod \ p \Leftrightarrow x^2 \equiv \frac{-1}{a} \ mod \ p \Leftrightarrow x \equiv \pm\sqrt{\frac{-1}{a}} \ mod \ p$
Como $(\frac{a}{p}) = -1 \Rightarrow (\frac{-1}{a}) = 1$, portanto $(\sqrt{\frac{-1}{a}}, 0) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$.

Se $x = 0$, então $y^2 \equiv 1 \ mod \ p \Leftrightarrow y \equiv \pm 1 \ mod \ p$
Assim existem dois pontos $(0, \pm 1) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Como anteriormente, existem $\frac{p-3}{2}$ elementos y em L_p tais que $\frac{y^2-1}{2}$ é um quadrado. Seja $t^2 = \frac{y^2-1}{a}$ para algum t $\in L_p$. Então
$x^2 \equiv t^2 \ mod \ p \Leftrightarrow x \equiv \pm t \ mod \ p$.
Se $(t, y) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$ então $(-t, y) \in \mathfrak{C}_{p,a}(\mathbb{F}_p)$.
Para cada y $\in L_p$ com $\frac{y^2-1}{a}$ temos dois pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, assim exitem $2.(\frac{p-3}{2}) = p-3$ pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$.

Conhecemos quatro pontos $(\pm\sqrt{\frac{1}{a}}, 0)$ e $(0, , \pm 1)$ sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$,totalizando $p-3+4 = p+1$ pontos racionais sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ demonstrando o teorema.

■

Exemplo 4.3 *Seja $p = 7$, os elementos do conjunto $\{1, 2, 4\}$ são os resíduos quadráticos módulo 7, pois:*
$1 \equiv 1^2 \ mod\ 7$,
$2 \equiv 3^2 \ mod\ 7$,
$4 \equiv 5^2 \ mod\ 7$.
Vamos determinar os pontos racionais sobre as cônicas $y^2 - ax^2 = 1$ sobre $\mathbb{Z}/7\mathbb{Z}$, com x,y, $a \in \mathbb{Z}/7\mathbb{Z}$

Para $a = 1$, $(\frac{1}{7}) = 1 \Rightarrow \#(\mathfrak{C}_{7,1}(\mathbb{Z}/7\mathbb{Z})) = 6$
O ponto $(1, 3)$ satisfaz a equação $3^2 - 1^2 \equiv 1 \ mod\ 7$
$\mathfrak{C}_{7,1}(\mathbb{Z}/7\mathbb{Z})$ = {(0,1),(0,6),(1,3),(1,4),(6,3),(6,4)}

Para $a = 2$, $(\frac{2}{7}) = 1 \Rightarrow \#(\mathfrak{C}_{7,2}(\mathbb{Z}/7\mathbb{Z})) = 6$
$\mathfrak{C}(\mathbb{Z}/7\mathbb{Z}) = \{(0, 1), (0, 6), (2, 3), (2, 4), (5, 3), (5, 4)\}$
da mesma forma o ponto $(5, 3) \in \mathfrak{C}_{7,2}(\mathbb{Z}/7\mathbb{Z})$ pois satisfaz a equação $3^2 - 2.5^2 = -41 \equiv 1 \ mod\ 7$

Para $a = 3$, não é um residuo quadrático módulo 7, $(\frac{3}{7}) = -1 \Rightarrow \#(\mathfrak{C}_{7,3}(\mathbb{Z}/7\mathbb{Z})) = 8$
$\mathfrak{C}_{7,3}(\mathbb{Z}/7\mathbb{Z}) = \{(0, 1), (0, 6), (1, 2), (1, 5), (3, 0), (4, 0), (6, 2), (6, 5)\}$.

Para $a = 4$, é um resíduo quadrático módulo 7, $\#(\mathfrak{C}_{7,4}(\mathbb{Z}/7\mathbb{Z})) = 6$
$\mathfrak{C}_{7,4}(\mathbb{Z}/7\mathbb{Z}) = \{(0, 1), (0, 6), (3, 3), (3, 4), (4, 3), (4, 4)\}$

Para $a = 5$, não é um resíduo quadrático módulo 7, $\#(\mathfrak{C}_{7,5}(\mathbb{Z}/7\mathbb{Z})) = 8$
$\mathfrak{C}_{7,5}(\mathbb{Z}/7\mathbb{Z}) = \{(0, 1), (0, 6), (2, 0), (3, 2), (3, 5), (4, 2), (4, 5), (5, 0)\}$

Para $a = 6$, não é um resíduo quadrático módulo 7, $\#(\mathfrak{C}_{7,6}(\mathbb{Z}/7\mathbb{Z})) = 8$
$\mathfrak{C}_{7,6}(\mathbb{Z}/7\mathbb{Z}) = \{(0, 1), (0, 6), (1, 0), (2, 2), (2, 5), (5, 2), (5, 5), (6, 0)\}$

Teorema 4.2 *Sejam $\mathbb{F}_p$ um corpo finito com p primo, o grupo $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ e $\sum \mathfrak{C}^x_{p,a}(\mathbb{F}_p)$ a soma das primeiras coordenadas x de todos pontos racionais (x, y) em $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, então*

$$\sum \mathfrak{C}^x_{p,a}(\mathbb{F}_p) = \begin{cases} \frac{p^2-3p}{2} & se\ (\frac{a}{p}) = 1 \\ \frac{p^2-p}{2} & se\ (\frac{a}{p}) = -1 \end{cases}$$

Demonstração: Seja $p \equiv 1\ mod\ 4$ e a um resíduo quadrático módulo p. Então existem $\frac{p-5}{2}$ pontos com y $\in L_p = \{2, 3, ..., p-2\} \subset \mathbb{F}_p$, tais que $\frac{y^2-1}{a}$ é um quadrado. Seja $t^2 = \frac{y^2-1}{a}$ para algum t $\in \mathbb{F}_p^*$.
Então $x^2 \equiv t^2\ mod\ p \Leftrightarrow x \equiv \pm t\ mod\ p$.
Quando $\frac{y^2-1}{a}$ é um quadrado, temos dois pontos (t, y) e $(p-t, y)$, portanto o total da soma das coordenadas x desses pontos é p.
Existem $\frac{p-5}{2}$ pontos em L_p tais que $\frac{y^2-1}{a}$ é um quadrado, assim a soma dos pontos (x, y) sobre a cônica é:
$p(\frac{p-5}{2}) = \frac{p^2-5p}{2}$.
Quando $y = 0$, temos dois pontos $(\pm\sqrt{\frac{-1}{a}}, 0)$ sobre a cônica $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ e a soma das coordenadas x desses pontos é p. Assim a soma total das coordenadas x de todos os pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ é
$\frac{p^2-5p}{2} + p = \frac{p^2-3p}{2}$

Seja $p \equiv 1\ mod\ 4$ e a um resíduo não quadrático módulo p.Então existem $\frac{p-1}{2}$ y $\in L_p$ tais que $\frac{y^2-1}{a}$ é um quadrado. Seja $t^2 = \frac{y^2-1}{a}$ para algum t $\in \mathbb{F}_p^*$. Então $x^2 \equiv t^2\ mod\ p \leftrightarrow x \equiv \pm t\ mod\ p$. Quando $\frac{y^2-1}{a}$ é um quadrado temos dois pontos (t, y) e $(p-t, y)$ com t$\in \mathbb{F}_p^*$, portanto o total da soma das coordenadas x desses pontos é p.
Existem $\frac{p-1}{2}$ pontos em L_p tais que $\frac{y^2-1}{a}$ é um quadrado.
Assim a soma total das coordenadas x desses pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ é
$p(\frac{p-1}{2}) = \frac{p^2-p}{2}$
Quando $y = 0$ não temos pontos sobre a cônica pois a não é resíduo quadrático, logo a soma total das coordenadas x de todos os pontos sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ é $\frac{p^2-p}{2}$.

Seja $p \equiv 3\ mod\ 4$ e a um resíduo quadrático. Então existem $\frac{p-3}{2}$ y em L_p tais que $\frac{y^2-1}{a}$ é um quadrado. Seja $t^2 = \frac{y^2-1}{a}$ para algum t $\in \mathbb{F}_p^*$. Então $x^2 \equiv t^2\ mod\ p \leftrightarrow x \equiv \pm t\ mod\ p$.

Quando $\frac{y^2-1}{a}$ é um quadrado temos dois pontos (t, y) e $(p-t, y)$ com t$\in \mathbb{F}_p$, portanto o total da soma das coordenadas x desses pontos é p.
Existem $\frac{p-3}{2}$ pontos em L_p tais que $\frac{y^2-1}{a}$ é um quadrado, assim a soma das coordenadas x desses pontos é: $\frac{p^2-3p}{2}$.
Quando $y = 0$ não temos pontos sobre a cônica, pois -1 não é resíduo quadrático módulo p para $p \equiv 3\ mod\ 4$, consequentemente $\sqrt{\frac{-1}{a}} \notin \mathbb{F}_p$ logo a soma total das coordenadas x de todos os sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ é $\frac{p^2-3}{2}$

Seja $p \equiv 3\ mod\ 4$ e a um resíduo não quadrático. Então existem $\frac{p-3}{2}$ y em L_p tais que $\frac{y^2-1}{a}$ é um quadrado. Seja $t^2 = \frac{y^2-1}{a}$ para algum t $\in \mathbb{F}_p^*$. Então $x^2 \equiv t^2\ mod\ p \leftrightarrow x \equiv \pm t\ mod\ p$.
Quando $\frac{y^2-1}{a}$ é um quadrado temos dois pontos (t, y) e $(p-t, y)$ com t $\in L_p$, portanto a soma das coordenadas x desses pontos é p.
Existem $\frac{p-3}{2}$ pontos em L_p tais que $\frac{y^2-1}{a}$ é um quadrado, logo a soma total das coordenadas x de todos os pontos (x, y) sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ é $p(\frac{p-3}{2}) = \frac{p^2-3p}{2}$

Quando $y = 0$, temos dois pontos $(\pm\sqrt{\frac{-1}{a}}, 0)$ sobre a cônica $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ pois $(\frac{-1}{a})$ é um resíduo quadrático, e a soma das coordenadas x desses dois pontos é p.
Assim a soma de todas as coordenadas x da cônica $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ é $\frac{p^2-3p}{2} + p = \frac{p^2-p}{2}$
■

Teorema 4.3 *Sejam $\mathbb{F}_p$ um corpo finito com p primo, o grupo $\mathfrak{C}_{p,a}(\mathbb{F}_p)$ e $\sum \mathfrak{C}^y_{p,a}(\mathbb{F}_p)$ a soma das segundas coordenadas de todos os pontos racionais (x, y) sobre $\mathfrak{C}_{p,a}(\mathbb{F}_p)$, então*

$$\sum \mathfrak{C}^y_{p,a}(\mathbb{F}_p) = \begin{cases} \frac{p^2-3p}{2} & se\ p \equiv 1(mod 4)\ e\ (\frac{a}{p}) = 1 \\ \frac{p^2+p}{2} & se\ p \equiv 1(mod 4)\ e\ (\frac{a}{p}) = -1 \\ \frac{p^2-p}{2} & se\ p \equiv 3(mod 4) \end{cases}$$

Demonstração: Seja $p \equiv 1\ mod\ 4$ e a um resíduo quadrático módulo p. Então existem $\frac{p-5}{2}$ pontos com y $\in L_p = \{2, 3, ..., p-2\} \subset \mathbb{F}_p$, tais que $\frac{y^2-1}{a}$ é um quadrado.
Se y é um resíduo tal que $\frac{y^2-1}{a}$ é um quadrado, então $-y=p-y$ é um resíduo tal que $\frac{y^2-1}{a}$ também é um quadrado. Então a soma das coordenadas y desses pontos é p. Como são $\frac{p-5}{2}$ pontos em L_p tais que $\frac{y^2-1}{2}$ é um quadrado, então a soma das coordenadas y desses pontos

é:
$p(\frac{p-5}{2}) = \frac{p^2-5p}{2}$.
Quando $y = 0$ temos dois pontos $(1, 0)$ e $(-1, 0)$ cuja soma das coordenadas y é p.
Existem $\frac{p^2-5p}{2}$ pontos em L_p tais que $\frac{y^2-1}{a}$ é um quadrado, assim a soma das coordenadas y dos pontos (x, y) sobre a cônica é:
$p + (\frac{p^2-5p}{2}) = \frac{p^2-3p}{2}$.

Seja $p \equiv 1 \ mod\ 4$ e a um resíduo não quadrático módulo p. Então existem $\frac{p-1}{2}$ y $\in L_p$ tais que $\frac{y^2-1}{a}$ é um quadrado. Se y é um resíduo tal que $\frac{y^2-1}{a}$ é um quadrado, então $-y{=}p-y$ é um resíduo tal que $\frac{y^2-1}{a}$ também é um quadrado. Então a soma das coordenadas y desses pontos é p. Como são $\frac{p-1}{2}$ pontos em L_p tais que $\frac{y^2-1}{2}$ é um quadrado, então a soma das coordenadas y desses pontos é:
$p(\frac{p-1}{2}) = \frac{p^2-p}{2}$.
Quando $y = 0$ temos dois pontos $(1, 0)$ e $(-1, 0)$ cuja soma das coordenadas y é p.
Existem $\frac{p^2-p}{2}$ pontos em L_p tal que $\frac{y^2-1}{a}$ é um quadrado, assim a soma das coordenadas y dos pontos (x, y) sobre a cônica é:
$p + (\frac{p^2-p}{2}) = \frac{p^2+p}{2}$.

Seja $p \equiv 3 \ mod\ 4$ e a um resíduo quadrático módulo p. Então existem $\frac{p-3}{2}$ y $\in L_p$ tais que $\frac{y^2-1}{a}$ é um quadrado. Se y é um resíduo tal que $\frac{y^2-1}{a}$ é um quadrado, então $-y{=}p-y$ é um resíduo tal que $\frac{y^2-1}{a}$ também é um quadrado. Então a soma das coordenadas y desses pontos é p. Como são $\frac{p-3}{2}$ pontos em L_p tais que $\frac{y^2-1}{2}$ é um quadrado, então a soma das coordenadas y desses pontos é:
$p(\frac{p-3}{2}) = \frac{p^2-3p}{2}$.
Quando $y = 0$ temos dois pontos $(1, 0)$ e $(-1, 0)$ cuja soma das coordenadas y é p.
Existem $\frac{p^2-3p}{2}$ pontos em L_p tal que $\frac{y^2-1}{a}$ é um quadrado, assim a soma das coordenadas y dos pontos (x, y) sobre a cônica é:
$p + (\frac{p^2-3p}{2}) = \frac{p^2-p}{2}$.

Seja $p \equiv 1 \ mod\ 4$ e a um resíduo não quadrático módulo p. Então existem $\frac{p-3}{2}$ y $\in L_p$ tais que $\frac{y^2-1}{a}$ é um quadrado. Se y é um resíduo tal que $\frac{y^2-1}{a}$ é um quadrado, então $-y=p-y$ é um resíduo tal que $\frac{y^2-1}{a}$ também é um quadrado. Então a soma das coordenadas y desses pontos é p. Como temos $\frac{p-3}{2}$ pontos em L_p tal que $\frac{y^2-1}{2}$ é um quadrado, então a soma das coordenadas y desses pontos é:
$p(\frac{p-3}{2}) = \frac{p^2-3p}{2}$.
Quando $y = 0$ temos dois pontos $(1, 0)$ e $(-1, 0)$ cuja soma das coordenadas y é p.
Existem $\frac{p^2-p}{2}$ pontos em L_p tais que $\frac{y^2-1}{a}$ é um quadrado, assim a soma dos pontos (x, y) sobre a cônica é:
$p + (\frac{p^2-3p}{2}) = \frac{p^2-p}{2}$

■

Exemplo 4.4 *Considerando o exemplo 4.3 temos que:* $\sum \mathfrak{C}^x_{p,a}(\mathbb{F}_p) = 14$ *e* $\sum \mathfrak{C}^y_{p,a}(\mathbb{F}_p) = 21$

Observação 4.1 *De modo análogo são válidos os seguintes resultados para o grupo* $\mathfrak{C}_{p,a}(\mathbb{F}_p) = \{ (x, y)\ com\ x,\ y\ em\ \mathbb{F}_p\ tal\ que\ x^2 - ay^2 = 1\}$

$$\sum \mathfrak{C}^x_{p,a}(\mathbb{F}_p) = \begin{cases} \frac{p^2-3p}{2} & se\ p \equiv 1(mod4)\ e\ (\frac{a}{p}) = 1 \\ \frac{p^2+p}{2} & se\ p \equiv 1(mod4)\ e\ (\frac{a}{p}) = -1 \\ \frac{p^2-p}{2} & se\ p \equiv 3(mod4) \end{cases}$$

$$\sum \mathfrak{C}^y_{p,a}(\mathbb{F}_p) = \begin{cases} \frac{p^2-3p}{2} & se\ (\frac{a}{p}) = 1 \\ \frac{p^2-p}{2} & se\ (\frac{a}{p}) = -1 \end{cases}$$

4.9 Interpretação Geométrica

Seja o corpo K, tomemos um ponto arbitrário N como elemento neutro, a lei de composição para adicionar dois pontos P e Q, sobre a cônica C, devemos traçar uma paralela ao segmento PQ iniciando em N. Essa reta intercepta a cônica C em um segundo ponto R, coloque $P \oplus Q = R$. Se C é o círculo unitário, a adição coincide com a lei da adição já definida e $N = (1, 0)$.

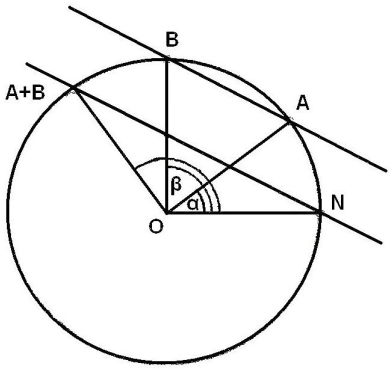

Figura 4.3: Adição de pontos A e B sobre o círculo

Para subcorpos K de $\mathbb{R}$, é possível provar geometricamente que a definição acima define uma lei de grupo sobre o círculo unitário que coincide com o método visto anteriormente. Sejam $N = (1, 0)$ e os pontos A e B sobre o círculo unitário, determinando $C = A \oplus B$ através da interseção entre a paralela ao segmento AB iniciando em N com o círculo. A intersecção das retas BA e ON obtém-se o ponto Q.

Sejam os ângulos:

$\alpha = \sphericalangle NOA$

$\beta = \sphericalangle NOB$

$\gamma = \sphericalangle ONC$

$\sphericalangle ONC = \sphericalangle OQB$

No $\triangle OQB$

$\pi = \sphericalangle OQB + \beta + \sphericalangle OBA$

$\sphericalangle OQB = \pi - \beta - \sphericalangle OBA$

No $\triangle OBA$ (isósceles)

$\sphericalangle OAB = \widehat{A} \equiv \widehat{B} = \sphericalangle OBA$

$\pi = (\beta - \alpha) + 2\sphericalangle OBA$

$\pi = \sphericalangle OAB + \sphericalangle OBA$

$\sphericalangle ONC = \sphericalangle OQB = \pi - \beta - \sphericalangle OBA$

$2\sphericalangle ONC = 2\pi - 2\beta - 2\sphericalangle OBA$

$\pi = \beta - \alpha + 2\sphericalangle OBA$

obtemos: $2\sphericalangle ONC = \pi - \beta - \alpha$

No $\triangle CON$ (isósceles)
$\sphericalangle ONC = \sphericalangle OCN$
$\sphericalangle CON = \pi - 2\sphericalangle ONC = \pi - \pi + \beta + \alpha = \alpha + \beta$

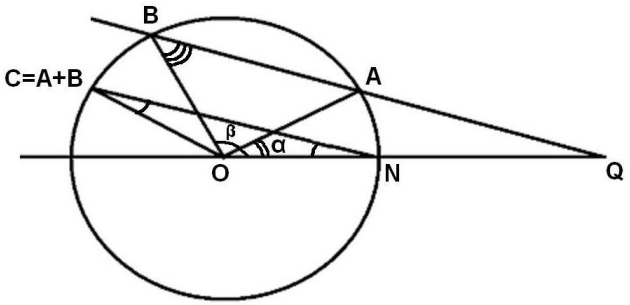

Figura 4.4: Adição dos pontos A e B sobre o círculo unitário, visão detalhada.

A adição dos pontos A e B é a adição dos ângulos correspondentes.
Se o corpo K não é um subcorpo de $\mathbb{R}$, a definição de lei de grupo sobre cônica tem que ser provada computacionalmente ou usar alguma geometria algébrica.
Se K for apenas um anel, pode parecer que a definição da lei de grupo não faça sentido pois a intersecção de uma reta passando pelo ponto P $\in K \times K$ com a cônica definida sobre K,leva a uma equação quadrática e em anéis a equação quadrática pode ter mais de duas raízes. (Por exemplo em $\mathbb{Z}/8\mathbb{Z}$ a equação $x^2 - 1$ possui 1,3,5,7, 9 como raízes). A equação quadrática possui uma solução em K que corresponde a um ponto P da cônica, a outra raiz da equação possui multiplicidade, assim a operação adição de pontos sobre cônicas também é válida para anéis.
Relebrando que para adicionarmos os pontos A e B sobre uma cônica, escolhemos um ponto N sobre ela e traçamos por N segmento de reta paralela ao segmento AB, a intersecção desse segmento com a cônica é um ponto $P = A \oplus B$
A propriedade associativa para a lei de grupo com a operação adição é válida quando $(A \oplus B) \oplus C = A \oplus (B \oplus C)$ para os pontos A, B, C sobre a cônica.
Usando o método acima, colocamos $P = A \oplus B$ e $Q = B \oplus C$, a propriedade associativa é equivalente à seguinte afirmação geométrica: se A, B, C, P, Q e N são pontos sobre a cônica tais que $AB \parallel NP$ e $BC \parallel QN$, então $AQ \parallel CP$.

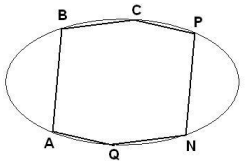

Figura 4.5: Representação geométrica da propriedade associativa

Através da parametrização do círculo por funções trigonométricas é possível determinar os pontos sobre êle, e é possível definir uma estrutura de grupo para o conjunto de pontos que satisfazem a equação do círculo. Essa estrutura de grupo pode ser estendida ao anel $\mathbb{Z}/n\mathbb{Z}$, e utilizando pontos sobre o círculo unitário $C(\mathbb{Z}/n\mathbb{Z})$ é possível fatorar um número inteiro.

A estrutura do grupo $C(\mathbb{Z}/m\mathbb{Z})$ é determinada quando fatoramos m.

Ao considerarmos o corpo $K = F_q$ com $q = p^n$, p primo, é possível determinar a estrutura de $C(F_q)$ através da estrutura do grupo $\mathbb{Z}/(q \pm 1)\mathbb{Z}$.

A lei de grupo sobre cônica com a operação adição de pontos sobre a mesma também é determinada através do coeficiente angular da reta que passa por dois pontos e o elemento neutro $N = (0, 1)$da cônica.

O ponto resultante da adição de dois pontos dados fica determinado através da parametrização da cônica dada por $P_m = (\frac{2m}{a - m^2}, \frac{a + m^2}{a - m^2})$.

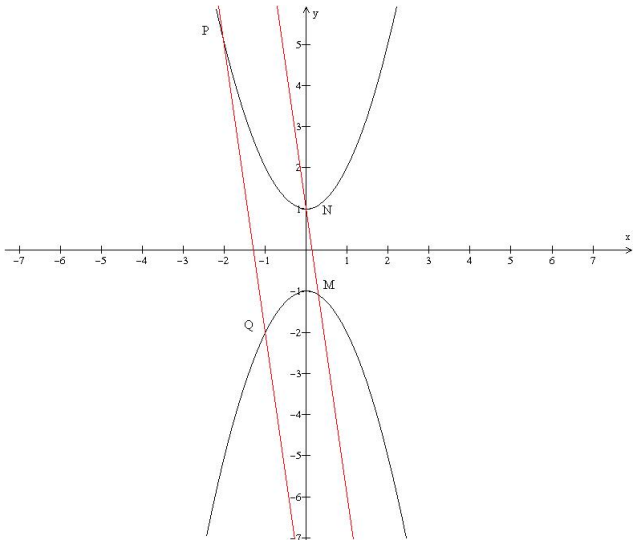

Figura 4.6: Adição de pontos P e Q sobre a hipérbole $y^2 - x^2 = 1$

Considerações Finais

Na passagem de um para outro dos capítulos que integram esse trabalho foram ponderados os principais temas abordados e foi indicado qual seria o objetivo dos passos seguintes.

A leitura deste trabalho não exige pré-requisito específico uma vez que no capítulo 1 os assuntos tratados contemplam as informações necessárias para tornar este trabalho acessível a todos.

A teoria de grupo cíclico forneceu subsídios para determinar pontos sobre o círculo unitário ao ser parametrizado pelas funções trigonométricas.

O Critério de Euler e o Símbolo de Legendre mereceram destaque pelo fato de serem essenciais na averiguação de um número ser resíduo quadrático módulo um número primo p.

A Lei da Reciprocidade Quadrática contribuiu para identificar se um dado número a é um resíduo quadrático módulo um número primo p, como também é a principal ferramenta utilizada para o estudo da estrutura de grupo identificando os pontos que satisfazem a equação da cônica.

A lei de grupo foi de suma importância na construção do conjunto de pontos que satisfazem a equação de uma cônica.

Através do círculo unitário, por ser um caso especial de uma cônica, e a lei de grupo sobre o conjunto de seus pontos que satisfazem a equação $x^2 + y^2 \equiv 1 \ mod \ p$ foi possível determinar a lei de grupo sobre a cônica geral $\mathfrak{C}(\mathbb{K}$, e o método mais simples para determinar a lei de grupo sobre essa cônica geral é tomar um ponto P sobre ela sendo $\mathbb{K}$ um corpo e usar a parametrização de $\mathfrak{C}(\mathbb{K})$, que é uma bijeção entre $\mathbb{K}$ e $\mathfrak{C}(\mathbb{K}) - \{P\}$ para tornar $\mathfrak{C}(\mathbb{K}) - \{P\}$ um grupo.

Conhecendo os pontos do círculo que satisfazem a equação $x^2 + y^2 \equiv 1 \ mod \ p$, foi possível fatorar um número inteiro da forma $n^2 + (q^2 - 1)$.

Para as cônicas com equação $y^2 - ax^2 \equiv 1 \ mod \ p$ com p primo, o conjunto de pontos que satisfazem a equação possui uma estrutura de grupo que fica definida ao determinar se a é um resíduo quadrático módulo p ou não é um resíduo quadrático.

Os assuntos aqui abordados podem dar início a alguma pesquisa dos grupos sobre curvas elípticas.

Referências Bibliográficas

[1] APOSTOL,Tom.M. *Introduction to Analytic Number Theory*. Springer-Verlag New York, New York: 1976.

[2] FILHO,BARBARESCO. Valdir. *Pontos Racionais Sobre Círculo unitário*. Dissertação de Especialização em Matemática, Instituto de Ciências Exatas e Naturais, Campus de Rondonópolis, Universidade Federal de Mato Grosso, Mato Grosso: 2001.

[3] BOYER, Carl B. *História da Matemática*. 7. ed., Edgard Blücher Ltda, São Paulo: 1987.

[4] HOWARD, Eves. *Introdução à história da matemática*. 2. ed., Editora Unicamp, Campinas: 2005.

[5] HEFEZ, Abramo. *Curso de Álgebra*. 1. ed., IMPA, Rio de Janeiro: 1993.

[6] HEFEZ, Abramo. *Elementos de Aritmética*. 2. ed., Coleção Textos Universitários, Sociedade Brasileira de Matemática, Rio de Janeiro: 2006.

[7] LEMMERMEYER, F. *Introduction to Number Theory*. Manucristo do curso de Introdução à teoria dos números realizado em CSU, San Marcos, Estados Unidos da América, 2000.

[8] MAIER, Rudolf. R. *Teoria dos Números*. Texto de aula, Universidade de Brasília, Distrito Federal: 2005.

[9] SHOKRANIAN, Salahoddin. SOARES, Marcus. GODINHO, Hemar. *Teoria dos Números*. 2. ed., Editora UnB, Brasília: 1999.

[10] SANTOS, José Plinio de Oliveira. *Introdução à Teoria dos Números*. 1. ed., IMPA, Rio de Janeiro: 2006.

[11] TAN, Lin. *The Group of Rational Points on the Unit Circle*. Mathematics Magazine, 69 (1996), June 1996.

[12] TECKAN, Ahmet. *The Number of Rational Points on Conics*. International Journal of Mathematics Sciences volume 1 number 2 2007 ISSN 1306-9292.