UNIVERSIDADE ESTADUAL DA PARAÍBA – UEPB
CAMPUS VII – GOV. ANTÔNIO MARIZ
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA EM CIÊNCIAS EXATAS

JOSÉ BRUNO LEITE PARAGUAI

TEOREMA DE LAGRANGE

PATOS – PB
2010

JOSÉ BRUNO LEITE PARAGUAI

TEOREMA DE LAGRANGE

Trabalho acadêmico referente à conclusão do Curso de Licenciatura Plena em Ciências Exatas da Universidade Estadual da Paraíba (UEPB – Campus VII), campus de Patos.

Orientador: MSc. Vilmar Vaz da Silva

PATOS – PB
2010

P221t Paraguai, José Bruno Leite

Teorema de Lagrange Patos: UEPB, 2010.
54f.

Monografia (TRABALHO de Conclusão de Curso –
(TCC) – Universidade Estadual da Paraíba.
Orientador: prof.Msc. Vilmar Vaz da Silva

1. Álgebra 2. Teoria dos Números I. Titulo
II. Silva, Vilmar Vaz da

CDD 512.72

Universidade Estadual da Paraíba
Campus VII – Patos
Centro de Ciências Exatas e Sociais Aplicadas
Curso de Licenciatura em Ciências Exatas

ATA DE DEFESA DE TCC

Aos dezesseis dias do mês de dezembro do ano de 2016, às 9:30 horas, no laboratório de Informática, do Campus VII da Universidade Estadual da Paraíba, ocorreu a apresentação de Trabalho de Conclusão de Curso, requisito da disciplina TCC, do(a) aluno(a) José Bruno Leite Paraguai tendo como tema "Decomposição em soma de Quatro Quadr

Constituíram a Banca Examinadora os professores:

Professor(a) MS. Vilmar Vaz da Silva (Orientador(a)),

Professor(a) MS. José Wilker de Lima (Examinador(a)),

Professor(a) MS. Syana Monteiro de Alencar Ramos (Examinador(a)).

Após a apresentação e as observações dos membros da banca avaliadora, definiu-se que o trabalho foi aprovado, com nota 7,0 (sete).

Eu, Vilmar Vaz da Silva, Professor(a) – Orientador(a), lavrei a presente ata que segue assinada por mim e pelos demais membros da Banca Examinadora.

Vilmar Vaz da Silva
PROFESSOR(A) – NOME COMPLETO – ORIENTADOR(A)

PROFESSOR(A) – NOME COMPLETO – EXAMINADOR

Syana Monteiro de Alencar Ramos.
PROFESSOR(A) – NOME COMPLETO – EXAMINADOR

Dedico este trabalho a minha namorada e futura esposa Joseane Alves de Oliveira, pois além de ter me acolhido durante todo o curso, compartilhou comigo os momentos de tristezas e também de alegrias, nesta etapa em que, com a graça de Deus, está sendo vencida.

AGRADECIMENTOS

- A Deus, pela sua plenitude divina; pois sem ele, esse trabalho não tinha acontecido.
- Ao Professor MSc. Vilmar Vaz da Silva, pois com sabedoria e respeito auxiliou nos momentos mais difíceis. A sua participação foi de grande relevância para o meu trabalho.
- A Professora Syana Monteiro de Alencar que em muitos momentos me ajudou de forma atenciosa.
- Ao funcionário da biblioteca da UEPB Kleber, que por muitas vezes aconselhou-me a nunca desistir dos meus sonhos.
- Aos meus pais, José Maria Paraguai e Sônia Maria Paraguai, que acreditou na minha vitória.
- Ao Professor Francisco Sibério que pro muitas vezes dedicou sua paciência, para conversar comigo, para que eu melhorasse as dissertações matemáticas.
- Aos colegas do curso, em especial Robertano Segundo, Hugo Gautier, Mailson da Silva, que muitas vezes estudaram juntos, nos momentos de dificuldade do curso.
- A funcionária da coordenação Ana Lúcia, que por muitas vezes me ajudou nos momentos de apreensão do curso.
- Ao casal Alcides Neto e Kállyda Janne, pela paciência e compreensão na hora da elaboração desse trabalho.

“A ÁLGEBRA É GENEROSA: FREQUENTEMENTE ELA DÁ MAIS DO QUE SE LHE PEDIU”
(Jean Le Rand D’Alambert)

RESUMO

O principal objetivo deste trabalho é apresentar de forma clara e completa a demonstração do Teorema de Lagrange. Para isso organizou-se esse trabalho em 3 capítulos fundamentais. O primeiro contendo teoremas e resultados matemáticos, necessários para a compreensão da demonstração do teorema principal, o segundo apresentando a decomposição dos inteiros não negativos como soma de dois quadrados e o último explicitando o Teorema de Lagrange propriamente dito.

Palavras–chave: Números inteiros. Teorema de Lagrange. Decomposição em som de dois quadrados.

ABSTRACT

The main objective of this paper is to present a clear and complete statement of the theorem of Lagrange. That was organized for this work in three key chapters. The first containing theorems and mathematical results needed to understand the statement of main theorem, the second presenting the decomposition of non-negative integers as sum of two squares and the latter explaining the Lagrange theorem itself.

Keywords: integer, Theorem of Lagrange Decomposition sound of two squares.

SUMÁRIO

INTRODUÇÃO

Através dos séculos, ilustres matemáticos como Pitágoras, Euclides, Gauss, Cauchy entre outros, descobriram fórmulas, resolveram problemas insolucionáveis pra suas épocas e demonstraram diversos e belíssimos teoremas, os quais perduram e se aplicam desde a antiguidade até a sociedade hodierna.

O presente trabalho é uma exposição sistemática de um desses tão importantes resultados o qual é conhecido como o famoso TEOREMA DE LAGRANGE que afirma ser possível escrever qualquer número inteiro não negativo como soma de quatro quadrados de inteiros. Este famoso resultado foi conjeturado pela primeira vez por Diofanto, um dos primeiros matemáticos gregos. Fermat, embora tenha tentado provar tal resultado, não obteve êxito, conseguindo apenas provar o teorema dos dois quadrados. Mais tarde, Euler aproveitando o resultado obtido por Fermat acrescentou resultados substânciais sobre o problema e, finalmente, em 1770, Lagrange deu a primeira demonstração completa do teorema, tendo como base o trabalho desenvolvido por Euler.

A exposição a seguir está organizada em três momentos. O capítulo inicial concentra todas as ferramentas matemáticas que serão utilizadas na demonstração dos resultados dos demais capítulos. O segundo momento consiste na representação de um inteiro como soma de dois quadrados. O terceiro e último capítulo explicita o mais importante resultado desse trabalho, o Teorema de Lagrange, o qual está enunciado e demonstrado de maneira clara e completa.

CAPITULO I

PRÉ-REQUISITOS

Este capítulo constitui-se de uma revisão de alguns algoritmos e resultados fundamentais que serão úteis para a compreensão o qual é o objeto central de estudo desse trabalho.

1 ALGORITMO DA DIVISÃO

TEOREMA 1.1. Dados dois inteiros a *e* $b, b > 0$, existe um único par de inteiros q e r tais que

$$a = bq + r, \text{como } 0 \leq r < b \ (r = 0 \Leftrightarrow b|a)$$

(q é fechado de quociente r de resto da divisão de a por b).

Demonstração. Pelo Teorema de Eudóxius, temos a garantia que se a, b são números inteiros, onde $b \neq 0$, então ou a é divisor de b ou se encontra entre dois múltiplos de b, ou seja,

$$qb \leq a < (q + 1)b$$

Segue deste teorema que

$$0 \leq a - qb < b$$

Dessa forma, se definirmos $r = a - qb$, fica garantida a existência de q e r. Observe que $a = qb + r$. Resta agora provar a unicidade de r e q.

Suponha que exista $r_1 \neq r$ e $q_1 \neq q$ que satisfaça $a = q_1 b + r_1$ com $0 \leq r_1 < b$. Como $a = qb + r$ e $a = q_1 b + r_1$, então

$$qb + r = q_1 b + r_1$$
$$qb - q_1 b = r_1 - r$$
$$(q - q_1)b = r_1 - r \implies b|(r_1 - r) \ (b \text{ divide } (r_1 - r))$$

Mas com $r_1 < b$ e $r < b$ segue que $|r_1 - r| < b$ e, portanto como $b|(r_1 - r)$, devemos ter $r_1 - r = 0$, o que implica $r = r_1$. Então

$$b(q - q_1) = 0, \text{ mas como } b \neq 0, \text{ então}$$
$$q - q_1 = q \implies q = q_1 \qquad \blacksquare$$

1.1 MDC E MMC

Definição 1.2. Sejam a e b dois números inteiros, b é dito um divisor de a ou a um múltiplo de b, se o resto da divisão euclidiana de a por b for zero, ou seja, se existir um inteiro q tal que $a = q \cdot b$. Diremos também que a é múltiplo de b.

Observação: Temos $1|a, b|0$ e $a|a, \forall\, a, b \in \mathbb{Z}$. Além disso, se $b|a$, então $|b| \leq |a|$.

Definição 1.3. O maior divisor comum entre a e b é um inteiro positivo d, denotado por $d = \text{mdc}\,(a, b)$ tal que

a) $d|a$ e $d|b$, ou seja, d é um divisor comum de a e b;

b) Se existe D tal que $D|a$ e $D|\, b$, então $D|d$, ou seja, se D for um outro divisor comum de a e b, então D também é divisor de d.

Além disso, diremos que a e b são primos entre si se $\text{mdc}\,(a, b) = 1$.

TEOREMA 1.4. O mdc de dois inteiros a e b sempre existe e é único.

Prova da Unicidade. Suponha que $(a, b) = d_1$ e $(a, b) = d_2$. Decorre imediatamente da definição que $d_1|\mathrm{d}_2$ e $d_2|d_1$, e, portanto $d_1 = d_2$.

Prova da Existência. Provemos inicialmente 2 lemas:

Lema 1.5. Dado um inteiro a, mdc $(a, 0)$ existe e vale a.

Vimos que $a|0$ e $a|a$, então a é um divisor comum de a e 0. Agora, qualquer outro divisor comum de a e de zero, divide arbitrariamente o número a. Portanto, a mdc, $(a, 0)$.

Lema 1.6. Seja r o resto da divisão euclidiana de a por b. Se mdc (b, r) existir, então existe também mdc (a, b) e os dois são iguais.

Prova. Observe

$$(b, r) = d \implies d|b \text{ e } d|r,$$

mas se $d|b \implies d|qb$, pois qb é múltiplo de b e como $d|qb$ e $d|r$, segue que

$$d|(qb + r) \implies d|a, \text{ pois } a = (qb + r).$$

Por outro lado, seja D um divisor comum de a e b, então,

$$D|qb \text{ e } D|r = qb - a.$$

Dessa forma, D é divisor comum de b e r e, portanto, $D|d$. Assim $d = \text{mdc}(a, b)$.

Conclusão da demonstração: Já demonstramos no Lema 1 o caso $b = 0$, portanto, podemos supor que $b \neq 0$ e fazer a divisão euclidiana de a por b:

$$a = q_1 b + r_2.$$

Observe que pelo Lema 1, se $r_2 = 0$, temos mdc $(b, r_2) = b$ e pelo Lema 2, mdc $(a, b) =$ mdc $(b, r_2) = b$.

Se $r_2 \neq 0$, fazemos uma segunda divisão euclidiana, agora com $r_1 = b$ dividido por r_2

$$r_1 = q_2 r_2 + r_3$$

Observe

Seja D um divisor comum de a e b, $D|a$, $D|b$ e $D|qb \implies D|qb - a \implies D|r$, pois $r = qb - a$ e como $D|b$ e $D|r \implies D|d, pois\ d$ é o maior mdc (b, r).

Continuamos assim por diante esta "descida", enquanto o resto for diferente de zero:

$k - ésimo$ passo fazemos a divisão euclidiana de $r_k - 1$ por r_k, o resto dela sendo denotado por r_{k+1}.

$$r_{k-1} = q_k r_k + r_{k+1}$$

Será que esse processo não tem fim? A resposta decorre do resto da divisão euclidiana, ele é sempre estritamente menor que o divisor. Assim na 1º divisão $r_2 < b$, no 2º $r_3 < r_2$. Na $k - ésima$ divisão, temos $r_{k+1} < r_k$. Temos então uma sequência de inteiros estritamente decrescente:

$$b = r_1 > r_2 > \cdots > r_k > r_{k+1} > \cdots$$

Portanto em um número finito de n passos, chegaremos a um resto r_{n+1} igual a zero.

Agora afirmamos que o mdc de a e b existe e vale r_n, já que $r_{n+1} = 0$, temos pelo Lema 1 que mdc $(r_n \cdot, r_{n+1}) = r_n$.

Por outro lado, a última divisão euclidiana que é

$$r_{n-1} = q_n r_n + r_{n+1,}$$

então, pelo Lema 2, mdc $(r_{n-1}, r_n) =$ mdc $(r_{n,} r_{n+1}) = r_n$.

Continuando assim por diante, chegaremos à conclusão que

$$\text{mdc}\,(a, b) = \text{mdc}\,(b, r_2) = \ldots = \text{mdc}(r_n, r_{n+1}) = r_n$$

Um raciocínio mais rigoroso usa a indução.

Usando a indução, vamos provar a seguinte afirmação

"Para todo $p, \leq p \leq n$, o mdc de r_{n-p} e r_{n-p+1} existe e vale r_n"

Prova. Já comprovamos que mdc $(r_n, r_{n+1}) = r_n$, então vale a afirmação para $p = 0$.

Além disso, da $(n - p)$-é*sima* divisão euclidiana

$$r_{n-(p+1)} = r_{n-p} \cdot q_{n-p} + r_{n-p+1}$$

e do lema 2, decorre que

$$\text{mdc}\,(r_{n-(p+1)}, r_{n-p}) = \text{mdc}\,(r_{n-p}, r_{n-p+1})$$

Portanto se a afirmação vale para n, isto é, mdc $(r_{n-p,} r_{n-p+1}) = r_n$ então vale para $p + 1$, ou seja, o mdc $(r_{n-(p+1),} r_{-(p+1)+1}) = r_n \cdot$

Uma vez que mostramos que a afirmação vale para todo p, fazendo $p = n$ deduzimos

$$\text{mdc}(r_0, r_1) = \text{mdc}\,(a, b) = r_n$$ ■

1.2 TEOREMA FUNDAMENTAL DA ARITMÉTICA

TEOREMA 1.7. Todo inteiro maior que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.

Demonstração.

Existência. Todo número inteiro n maior que 1 ou é primo ou não é primo.

Se n for primo nada há a demonstrar. Suponha que n não seja primo, ou seja, n é composto. Segue que se n é composto então n admite pelo menos um divisor (o qual é diferente de um (1) e de n).

Seja p_1 $(1 < p_1 < n)$ o menor dos divisores positivos de n.

Afirmação: p_1 é primo.

Isso é verdade, pois se p_1 não fosse primo, p_1 seria composto e neste caso, p_1 admitiria divisor d o qual seria menor que p_1 e, além disso, dividiria n, o que seria um absurdo, pela minimalidade de p_1.

Logo,

$$n = p_1 \cdot n_1$$

Se n_1 for primo acaba a demonstração. Caso contrário n_1 é composto, e neste caso, n, admite divisor $d < n_1$ onde$1 < d < n_1$. Seja p_2 o menor dos divisores de n_1.

Afirmação: p_2 é primo.

Isso é verdade, pois se não fosse $p_2$seria composto e admitiria divisor $d < p_2$ o qual dividiria também n_1, ferindo assim a minimalidade de p_2.

Então, temos que

$$n = p_1 \cdot p_2 \cdot n_2$$

Repetindo esse procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2 \cdot, \cdots, n_r$. Como todos eles são inteiros maiores que 1 este procedimento deve terminar. Ao final obteremos uma decomposição de n em fatores primos, assim:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

Como os primos na seqüência $p_1, p_2, \ldots p_k$, não são necessariamente distintos, n terá em geral a forma:

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$$

Unicidade. Para provarmos a unicidade usaremos indução sobre n (2ª forma de indução).

para $n = 2$ a afirmação é verdadeira, pois, é claro, que a fatoração de 2 é a trivial e é única.

Assumimos então que a unicidade se verifica para todos os inteiros maiores do que 1 e menores do que n. Devemos provar que ela é verdadeira para n.

Se n é primo, nada há para ser provado.

Vamos supor que n seja composto e que possua duas fatorações, isto é:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s \text{ e } n = q_1 \cdot q_2 \cdot \ldots \cdot q_r$$

Vamos provar que $s = r$ e que cada p_1 é igual a algum q_j.

Temos que $p_1$divide n, então $p_1 | q_1 \cdot q_2 \cdot \ldots \cdot q_r$.

Sabemos que se p é primo e $p|ab$ então $p|a$ ou $p|b$.

Por este fato, segue que $p_1|q_1$ ou $p_1|q_2 \cdot \ldots \cdot q_r$.

Repetindo esse raciocínio concluiremos que $p_1 | q_j$ para algum j. Sem perda de generalidade, podemos supor que $p_1 | q_1$ e como ambos são primos, então $p_1 = q_1$

Observe ainda que:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_r$$

$$\frac{n}{p_1} = p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_r$$

então, $1 < \frac{n}{p1} < n$.

Assim, pela hipótese de indução aplicada a $\frac{n}{p_1}$ temos que $p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_r$. E como já havíamos concluído que $p_1 = q_1$, então, as duas fatorações são idênticas a menos da ordem. ■

1.3 CONGRUÊNCIA

Definição 1.8. Se a e b são inteiros, dizemos que a é congruente a b módulo m ($m > 0$) se $m|(a - b)$. Denotamos isto por

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

Se $m \nmid (a - b)$dizemos que a é incongruente a b módulo m. E denotamos

$$a \not\equiv b (\text{mod } m).$$

Exemplo 1.9. Considere os inteiros 9 e 3. $9 \equiv 3$ (mod 2), pois 2 | (9 – 3), isto é, 2 | 6.

Exemplo 1.10. Considere os inteiros 9 e – 5. $9 \equiv 5$ (mod 7), pois $7 | (9 - (-5))$, isto é, $7 | 9 + 5 \Longrightarrow 7 | 14$.

Exemplo 1.11. Considere os inteiros 7 e 2. $7 \not\equiv 2$(mod 3), pois $3 \nmid (7 - 2)$.

Proposição 1.12 Se a e b são inteiros, temos que $a \equiv b$ (mod m) se, e somente se, existir um inteiro k tal que $a = b + km$.

Demonstração. $\Rightarrow|$ Se $a \equiv b \pmod{m}$ $m \mid (a - b) \implies (a - b) = km$, com $k \in \mathbb{Z}$, isto é, $a = km + b$.

$\Leftarrow|$ A recíproca é trivial, pois da existência de um k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, $m \mid a - b$, isto é, $a \equiv b \pmod{m}$

Em simples palavras estamos dizendo que se $a \equiv b \pmod{m}$ então isso quer dizer que b é o resto da divisão euclidiana de a por m.

O próximo Teorema é o de suma importância no estudo da congruência e para o entendimento das classes de Equivalência, as quais veremos mais adiante. ■

TEOREMA 1.13. Dois números inteiros são congruentes módulo p se e somente se eles têm o mesmo resto pela divisão euclidiana por p.

Prova. $\Rightarrow|$ Escreveremos as divisões euclidianas de a e b módulo p:

$$a = q_1 p + r_1 \quad b = q_2 p + r_2$$

Se $r_1 = r_2$, ao subtrairmos membro a membros as duas equações acima, teremos:

$$\begin{aligned} a - b &= q_1 p + r_1 - (q_2 + r_1) \\ &= q_1 p + r_1 - q_2 p - r_1 \\ &= (q_1 - q_2) p \end{aligned}$$

Isso implica que $p \mid (a - b) \implies a \equiv b \pmod{p}$.

$\Rightarrow|$ Reciprocamente se $a \equiv b \pmod{p} \implies p \mid (a - b) \implies$existe um inteiro x tal que $a - b = px$.

Por outro lado temos que $a - b = (q_1 - q_2)p + r_1 - r_2$ e logo deduzimos que $px = (q_1 - q_2)p + r_1 - r_2$.

E como $p \mid px$, $p \mid (q_1 - q_2)p \implies p \mid (r_1 - r_2)$ isso significa que $(r_1 - r_2)$ é um múltiplo de p.

Agora, usamos o fato que $0 \leq r_1 < p$ e $0 \leq r_2 < p$, que implica que $-p < r_1 - r_2 < p$.

E como $r_1 - r_2$ é múltiplo de p, então $r_1 - r_2$, pois o único múltiplo de p que é maior que $-p$ e menor que p é zero. Logo $r_1 = r_2$.

Esses outros teoremas que apresentaremos asseguram que a relação de congruência é compatível com a soma e com o produto. ■

TEOREMA 1.14. Se a, b, c, m são inteiros tais que $a \equiv b \pmod{m}$, então:

1. $a + c \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $a \cdot c \equiv b \cdot c \pmod{m}$

Demonstração.

1. Como $a \equiv b \pmod{m}$, temos $a - b = mk$ e, como $a - b = (a + c) - (b + c)$, segue que

$$a + c \equiv b + c \pmod{m}.$$

2. Como $\equiv b \pmod{m}$, temos $a - b = mk$. Mas $a - c \equiv (a - c) - (b - c)$, então

$$a - c \equiv b - c \pmod{m}.$$

3. Como $a \equiv b \pmod{m}$, então $a - b = mk$, então

$$c(a - b)cmk \Longrightarrow ca - cb = ckm \Longrightarrow ca - cb = k'm \Longrightarrow m|(ca - cb)$$

e, portanto,

$$ac \equiv bc \pmod{m}.$$ ■

TEOREMA 1.15. Se a, b, c, d e m são inteiros tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $a \cdot c \equiv b \cdot d \pmod{m}$

Demonstração.

1. De $a = b \pmod{m}$ e $c \equiv d \pmod{m}$, temos $a - b = k_1 m$ e $c - d = k_2 m$. Somando membro a membro obtemos

$$a - b + c - d = k_2 m \Longrightarrow (a + c) - (b + d) = (k_1 + k_2) m$$

$$\Longrightarrow (a + c) - (b + d) = k_2 \Longrightarrow m|(a + c) - (b + d) \Longrightarrow (a + c) \equiv (b + d) \pmod{m}$$

2. De $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, temos $a - b\ k_1\ m$ e $c - d = k_2\ m$. Se subtrairmos membro a membro obteremos

$(a-c)-(b-d) = k_1\, m\,(a-c)-(b-d) = (k_1-k_2)m \implies$

$\implies (a-c)-(b-d) = k_3\ m \implies m|(a-c)-(b-d) \implies (a-c) \equiv (b-d) \bmod m$

3. De $a = b(\text{mod } m)$ e $c \equiv$d (mod m), temos $a - b = k_1\, m$ e $c - d = k_2\, m$. Multiplicando ambos os lados de $a - b = k_1\, m$ por c e ambos os lados de $c - d = k_2\, m$ por d, obteremos:

- $ac - bc = k_1\, cm$ e
- $bc - bd = k_2 bm$

Somando membro a membro essas duas igualdades, teremos:

$$ac - bc + bc - db = ac - bd = (ck_1 + bk_2)m \implies m|(ac - bd) \implies ac \equiv bd(\text{mod } m)$$

■

1.4 RESÍDUOS QUADRÁTICOS

Definição 1.16. Se a congruência

$$x^2 \equiv (mod\ n)$$

tiver uma solução então n é dito resíduo quadrático módulo m; caso contrário é dito não-resíduo quadrático módulo m.

Exemplo: 0, 1, e todos os outros quadrados perfeitos são resíduos quadráticos módulo qualquer número.

Definição 1.17. (O símbolo de Legendre) Se $p > 2$ e $p \nmid$, então

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & \text{se } n \text{ for resíduo quadrático (mod } p) \\ -1, & \text{se } n \text{ for não-resíduo quadrático de (mod } p) \end{cases}.$$

Exemplo: $\left(\frac{m^2}{p}\right) = 1$ se $p > 2$ e $p \nmid$; em particular, $\frac{1}{p} = 1$ se $p > 2$.

TEOREMA 1.18. Seja $p > 2$. Se $n \equiv n'\ (mod\ p)$ e p ∤ n então

$$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right)$$

Prova: Por hipótese, certamente temos $p \nmid n'$. De $x^2 \equiv n(mod\ p)$ segue que $x^2 \equiv n' \pmod{p}$, e reciprocamente.

TEOREMA 1.19. Seja $p > 2$. em cada conjunto reduzido de resíduos mod p existem exatamente $\frac{p-1}{2}$ números n para os quais $\left(\frac{n}{p}\right) = 1$ e logo existem exatamente $\frac{p-1}{n}$ números n para os quais $\left(\frac{n}{p}\right) = -1$. O primeiro conjunto de $\frac{p-1}{2}$ números são representados pelas classes às quais pertencem $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$.

Em particular, portanto: dado $p > 2$ existe um n para o qual

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

Prova: A congruência

$$x^2 \equiv n \pmod{p},$$

se tiver alguma solução, tem pelo menos uma solução no intervalo $0 \leq x \leq p-1$: mas pelo teorema 72 ela tem no máximo duas soluções neste intervalo, e no caso p ∤ n o número 0 não é uma delas. Como

$$(p-x)^2 \equiv (-x)^2 \equiv x^2 \pmod{p},$$

existe, portanto exatamente uma solução no intervalo $1 \leq x \leq \frac{p-1}{2}$. Assim quaisquer dois entre os números

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

são incongruentes. O teorema foi assim provado. ■

TEOREMA 1.20. (O critério de Euler) Seja $p > 2$ e $p \nmid n$, então

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

Observação: O fato que

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

é para começar, uma consequência do teorema de Fermat; pois de

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

Segue que

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

Prova: O módulo n prova que será p o tempo todo.

1) Seja

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

Então existe um x tal que

$$x^2 \equiv n.$$

Assim, pelo Teorema de Fermat,

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

Seja

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

A congruência

$$x^{\frac{p-1}{2}} - 1 \equiv 0$$

tem no máximo $\frac{p-1}{2}$ soluções, e pelo teorema 1.19**,** ela tem no mínimo $\frac{p-1}{2}$ soluções, a saber, os resíduos quadráticos em qualquer conjunto reduzido de resíduos; assim não existem outras soluções. Logo, nosso número n, sendo um não-resíduo quadrático, satisfaz a congruência

$$n^{\frac{p-1}{2}} + 1 \equiv 0.$$ ■

TEOREMA 1.21. Seja $p > 2, p \nmid n$ e $p \nmid n'$, então

$$\left(\frac{nn'}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right).$$

Em palavras: a congruência $x^2 \equiv nn'$ é solúvel se e só se as congruências $x^2 \equiv n \; e \; x^2 \equiv n'$ são ambas solúveis ou ambas não solúveis. Expresso de outra maneira: se $n \; e \; n'$ são ambos resíduos quadráticos ou ambos não-resíduos quadráticos, então nn' é um resíduo quadrático; se um deles é um resíduo quadrático e o outro não-resíduo quadrático então o produto é não-resíduo quadrático. Tudo sob as hipóteses $p > 2, p \nmid n$ e $p \nmid n'$.

Prova: Pelo teorema 1.20, temos

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

uma vez que

$$\left(\frac{nn'}{p}\right) - \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right) = 0.$$

■

TEOREMA 1.22. Seja $p > 2, r \geq 2, p \nmid n_1, \ldots, p \nmid n_r$ então

$$\left(n_1 \ldots \frac{n_r}{p}\right) = \left(\frac{n_1}{p}\right) \ldots \left(\frac{n_r}{p}\right).$$

Prova: Teorema 1.21.

Se $p > 2 \; e \; p \; n$ então o símbolo $\left(\frac{n}{p}\right)$ se divide, pelo teorema 1.22, em símbolos mais simples de forma $\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right) e \; \left(\frac{q}{p}\right)$, onde q é um primo ímpar diferente de p. Os teoremas principais da teoria de resíduos quadráticos apresentados a seguir (teorema 1.23, 1.25 e 1.26) se referem a estas três situações. ■

TEOREMA 1.23. (Chamado o Primeiro Suplemento da Lei de Reciprocidade Quadrática)

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

ou, mais explicitamente,

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

Em palavras: cada divisor primo de $x^2 + 1$ é $\equiv 1 \pmod 4$, e cada $p \equiv 1 \pmod 4$ divide $x^2 + 1$ para números apropriados x.

Prova: Pelo Critério de Euler (teorema 1.20) temos

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p;$$

como $p > 2$, temos a igualdade. ■

TEOREMA 1.24. (chamado o Lema de Gauss) Seja $p > 2$ *e* $p \nmid n$. Considere os $\frac{p-1}{2}$ números

$$n, 2n, \ldots, \frac{p-1}{2}n$$

e determine seus resíduos mod p. Daí obtemos

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

números distintos, que são $> 0 > p$. Seja m o número destes resíduos que são $> \frac{p}{2}$ $\left(i.e., \geq \frac{p+1}{2}\right)$. ($m$ pode ainda ser = 0; por exemplo, se $n = 1$.)

Afirmamos que

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

Exemplo: $p = 7, n = 10$. Os números 10, 20 e 30 deixam resíduos 3,6 e 2, respectivamente. Neste caso $m = 1$, e logo $\left(\frac{3}{7}\right) = -1$ pelo teorema 1.24. E, de fato, a congruência $x^2 \equiv 3 \pmod 7$ é solúvel.

Prova: Fixe em p o módulo. $l = \frac{p-1}{2} - m$ é o número de resíduos que é $< \frac{p}{2}\left(i.e., \leq \frac{p-1}{2}\right)$. Se $l > 0$, denote estes números por $a_1, \ldots . a_{l;}$ sejam os resíduos $> \frac{p}{2}$ ocorrendo no teorema dados por $b_1, \ldots \cdot, b_m$ *se* $m > 0$. Se multiplicarmos todos os $\frac{p-1}{2}$ resíduos (ou seja, todos os a_s, b_t) obtemos a congruência

$$\prod_{s=1}^{l} a_s \prod_{t=1}^{m} b_t \equiv \prod_{h=1}^{\frac{p-1}{2}} hn \equiv \left(\frac{p-1}{2}\right)! \, n^{\frac{p-1}{2}}$$

Os "complementos" dos números b_t (quero dizer, os números $p - b_t$) pertencem ao intervalo de 1 a $\frac{p-1}{2}$. Quaisquer dois deles são distintos, já que isto vale para os números b_t. Além disso, cada a_s é distinto de $p - b_t$; pois

$$a_s = p - b_t$$

resultaria em

$$xn \equiv p - yn, \qquad 1 \leq x \leq \frac{p-1}{2}, \qquad 1 \leq y \leq \frac{p-1}{2},$$

$$xn \equiv -yn, \qquad x \equiv -y, \qquad x + y \equiv 0,$$

em contradição a

$$0 < x + y < p$$

Em consequência (já que existem $\frac{p-1}{2}$ números) os números a_s e os números $p - b_t$, juntos, são os números $1, \ldots, \frac{p-1}{2}$ em alguma ordem (o princípio da casa do pombo – ou dos escaninhos), de modo que

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv \prod_{s=1}^{l} a_s \prod_{t=1}^{m} (p - b_t) \\ &\equiv (-1)^m \prod_{s=1}^{l} a_s \prod_{t=1}^{m} b_t \\ &\equiv (-1)^m \left(\frac{p-1}{2}\right)! \, n^{\frac{p-1}{2}}\end{aligned}$$

$$1 \equiv (-1)^m n^{\frac{p-1}{2}},$$

e, consequentemente, pelo teorema 1.20,

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

$$\left(\frac{n}{p}\right) \equiv (-1)^m.$$

■

TEOREMA 1.25. (chamado o Segundo Suplemento da Lei de Reciprocidade Quadrática)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad para \quad p > 2;$$

Ou (observando que $\frac{(8a\pm 1)^2-1}{8} = 8a^2 \pm 2a$ *e* $\frac{(8a\pm 3)^2-1}{8} = 8a^2 \pm 6a + 1$ mais explicitamente:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{para } p \equiv \pm 1 \pmod 8, \\ -1, & \text{para } p \equiv \pm 3 \pmod 8. \end{cases}$$

Prova: Para $p > 2$ e $n = 2$ o teorema 1.24 fornece

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

pois os números

$$2, 2.2, \dots, \frac{p-1}{2} \cdot 2$$

já são eles próprios > 0 e $< p$, e logo são seus próprios resíduos; e

$$\frac{p}{2} < 2h < p$$

vale sempre

$$\frac{p}{4} < 2h < \frac{p}{2},$$

isto é, $\frac{p}{2} - \frac{p}{4}$ vezes; se $p = 8a + r$ onde $r = 1, 3, 5$ ou 7 então é $4a - 2a \equiv 0, 4a + 1 - 2a \equiv 1, 4a + 2 - 2a1 \equiv 1, 4a + 3 - 2a - 1 \equiv 0 \pmod 2$, respectivamente.

Uma prova mais elegante do teorema 85 é apresentada ao longo da prova do próximo teorema. ■

TEOREMA 1.26. (A Lei da Reciprocidade Quadrática, conjecturada primeiro Por Euler e provada primeiro por Gauss) Se $p > 2$ *e* $q > 2$ forem primos com $p \neq q$ então

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

Em palavras (uma vez que $\frac{p-1}{2}\frac{q-1}{2}$ é ímpar para$p \equiv q \equiv 3 \pmod 4$ e par caso contrário), as congruências

$$x^2 \equiv p \pmod q, \qquad x^2 \equiv q \pmod p,$$

são ambas solúveis ou ambas insolúveis a não ser que $p \equiv q \equiv 3 \pmod 4$; se $p \equiv q \equiv 3 \pmod 4$ então uma é solúvel e a outra insolúvel.

Prova: Por enquanto admitimos $q = 2$; mas seja q ainda um primo $\pm p$. Se $1 \leq k \leq \frac{p-1}{2}$ então

$$kq = q_k p + r_k, \qquad 1 \leq r_k \leq p-1$$

Onde os números r_k são os números a_s e b_t na prova do teorema 1.24 (com $n = q$).

Nesta fórmula

$$q_k = \left(\frac{kq}{p}\right)$$

já sabemos que os números a_s e $p - b_t$, exceto pela ordem, são 1, 2, ..., $\frac{p-1}{2}$. Se, por brevidade, colocarmos

$$\sum_{s=1}^{l} a_s = a, \qquad \sum_{t=1}^{m} b_t = b,$$

então

$$\sum_{k=1}^{\frac{p-1}{2}} r_k = a + b,$$

$$\frac{p^2-1}{8} = \frac{\frac{p-1}{2}\frac{p+1}{2}}{2} = \sum_{k=1}^{\frac{p-1}{2}} k = a + mp - b.$$

Somando as equações resulta em

$$\frac{p^2-2}{8} q = p\sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} r_k = p\sum_{k=1}^{\frac{p-1}{2}} q_k + a + b,$$

daí

$$\frac{p^2-1}{8}(q-1) = p\sum_{k=1}^{\frac{p-1}{2}} q_k - mp + 2b,$$

$$\frac{p^2-1}{8}(q-1) \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + m \pmod 2.$$

1) (Prova alternativa do teorema 1.25.) Seja $q = 2$. Então todo $q_k = 0$, de forma que, por

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

e logo, pelo teorema 1.24,

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

2) Seja $q > 2$. Assim, temos,

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k(\text{mod } 2),$$

de modo que, pelo teorema 1.24,

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

Por simetria temos

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

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{k_p}{p}\right)+\sum_{l=1}^{\frac{q-1}{2}}\left(\frac{l_p}{q}\right)}.$$

Com isso é suficiente mostrar que

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{k_q}{p} + \sum_{l=1}^{\frac{q-1}{2}} \frac{l_p}{q} = \frac{p-1}{2}\frac{q-1}{2}(\text{mod } 2).$$

De fato acontece mesmo que

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{k_q}{p} + \sum_{l=1}^{\frac{q-1}{2}} \frac{l_p}{q} = \frac{p-1}{2}\frac{q-1}{2},$$

e não faremos uso do fato que p *e* q são primos ímpares distintos, apenas do fato que são números ímpares >1 relativamente primos entre si.

De fato, consideremos os $\frac{p-1}{2}\frac{q-1}{2}$ números

$$lp - kq, \quad \text{onde} \quad k = 1, \ldots, \frac{p-1}{2};\ l = 1, \ldots, \frac{q-1}{2}.$$

(Não nos interessa saber se são distintos: é um exercício para o leitor).

Nenhum destes números é 0; pois senão teríamos

$$lp = kp, \quad q|lp, \quad q|l.$$

A quantidade de números positivos entre estes $\frac{p-1}{2}\frac{q-1}{2}$ números é claramente

$$\sum_{l=1}^{\frac{q-1}{2}} \frac{lp}{q}$$

porque seja

$$k < \frac{lp}{q}, \qquad 1 \leq k \leq \frac{p-1}{2}$$

para todo $l = 1, \ldots, \frac{q-1}{2}$; como $\frac{lp}{q}$ não é um inteiro segue que $1 \leq k \leq \frac{lp}{q}$ tem exatamente $\left(\frac{lp}{q}\right)$; soluções, e, além disso, $k < \frac{\frac{q}{2}p}{q} = \frac{p}{2}, k \leq \frac{p-1}{2}$ é automaticamente verdade.

A quantidade de números negativos entre estes é

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{kq}{p},$$

por simetria. Assim esta provado.

Exemplo de aplicação a Lei de Reciprocidade: Com esta lei podemos rapidamente dizer quais primos tem o número 3 como resíduo quadrático.

De fato, segue a Lei de Reciprocidade para $p > 3$ que

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

Pelos teoremas 1.18 e 1.23 temos, nesta fórmula.

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

além disso,

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

assim

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

mas geralmente vemos que par um primo impar fixo q o símbolo $\left(\frac{q}{p}\right)$ tem o mesmo valor para todos p (desde que existam) pertencendo à mesma classe residual reduzida mod $4q$. De fato, $\left(\frac{p}{q}\right)$ tem, pelo teorema 1.18, o mesmo valor para todos os p ímpares pertencendo á mesma classe residual reduzida mod $q(-1)^{\frac{p-1}{2}}$ tem o mesmo valor para todos os p pertencendo à mesma classe residual reduzida mod 4. ■

TEOREMA 1.27. Seja $l > 0$ e $p \nmid n$. Então o número de soluções é

$$x^2 \equiv n \equiv (\ mod\ p^l)$$

tem o seguinte valor:

$$1\ para\ p = 2, l = 1,$$
$$0\ para\ p = 2, l = 2, n \equiv 3\ (mod\ 4)$$
$$2\ para\ p = 2, l = 2, n \equiv 1 (mod\ 4)$$
$$0\ para\ p = 2, l > 2, n \not\equiv 3\ (\ mod\ 8)$$
$$4\ para\ p = 2, l > 2\ n \equiv 1 (\ mod\ 8)$$
$$1 + \left(\frac{n}{p}\right) para\ p > 2.$$

Prova:

1) $x^2 \equiv n$ (mod 2) tem uma raiz $x^2 \equiv 1$ (mod 2) se $2 \nmid n$.

2) $x^2 \equiv 3$ (mod 4) não tem raiz.

3) $x^2 \equiv 1$ (mod 4) tem duas raízes $x \equiv \pm 1$ (mod 4).

4) Seja $p = 2, l > 2, 2 \nmid n$, e $n \not\equiv 1 (\text{mod } 8)$. Se

$$x^2 \equiv n\ (\text{mod } 2^l\ )$$

tivesse soluções então x seria ímpar e teríamos

$$x^2 \equiv n\ (\text{mod } 8),$$

de modo que

$$x^2 \not\equiv 1\ (\text{mod } 8).$$

Contudo, o quadrado de qualquer número ímpar é $\equiv 1$ (mod 8).

5) Seja $p = 2, l > 2,$ e $n \equiv 1\ (mod\ 8)$. Sem perda de generalidade, seja $0 < n < 2^l$. As soluções devem ser procuradas apenas entre os 2^{l-1} números ímpares x satisfazendo $0 < x < 2^l$.

Para cada x assim, certamente temos

$$x^2 \equiv m\ (\text{mod}\ 2^l)$$

para $m \equiv 1\ (\text{mod}\ 8)$ escolhido apropriadamente no intervalo $0 < m < 2^l$.
Cada um destes 2^{l-1} números m ocorre no máximo quatro vezes. Pois de

$$x^2 \equiv x_0^2 (\text{mod}\ 2^l), \qquad 2 \nmid x_0$$

segue que

$$2^l | (x - x^0)(x + x^0);$$

como x e x^0 são ímpares, de modo que $x - x^0$ e $x + x^0$ são pares, temos

$$2^{l-2} \left| \frac{x - x^0}{2} \cdot \frac{x + x^0}{2} \right.$$

2 não divide ambos os fatores $\frac{x-x^0}{2}$ e $\frac{x+x^0}{2}$, já que a soma deles é ímpar:
assim

$$2^{l-2} \left| \frac{x-x^0}{2} \right. \text{ ou } 2^{l-2} \left| \frac{x+x^0}{2} \right.,$$

isto é,

$$x^2 \equiv \mp x_0 (\text{mod}\ 2^{l-1}),$$

resultando em no máximo quatro valores para x.

Como os $2^{l-1} = 4.2^{l-3}$ números x estão distribuídos entre 2^{l-3} posições ("escaninhos") de tal maneira que existem no máximo quatro deles em cada um, segue que existem exatamente quatro em cada um, e, portanto a posição n dada contém exatamente quatro soluções.

6) Seja $p > 2$.

6.1) Seja $\left(\frac{n}{p}\right) = -1$. Já temos que

$$x^2 \equiv n (\text{mod}\ p)$$

é insolúvel, de modo que

$$x^2 \equiv n(\text{mod } p^1)$$

é certamente insolúvel, e o número de soluções de (28) é

$$0 = 1 + \left(\frac{n}{p}\right).$$

6.2) Seja $\left(\frac{n}{p}\right) = 1$. Sem perda de generalidade seja $0 < n < p^1$. As soluções devem ser procuradas somente entre os $\varphi(p^1)$ números x no intervalo $0 < x < p^1$ que não são divisíveis por p.

Para cada x assim certamente temos

$$x^2 \equiv m(\ mod\ p^l)$$

para m apropriado com $\left(\frac{m}{p}\right) = 1, 0 < m < p^l \cdot$. Cada qual destes $\frac{p-1}{2}\ p^{l-1} = \frac{1}{2}\varphi\ (p^l)$ números ocorre no máximo duas vezes. Pois de

$$x^2 \equiv x_0^2(\text{mod } p^l), \qquad p \nmid x_0$$

segue que

$$p^l | (x - x_0\ )(x + x_0).$$

p não divide ambos os fatores $\frac{x-x_0}{2}$ e, já que a soma deles $2x$ não é divisível por p; assim

$$x^2 \equiv \pm\, x_0\ (\text{mod } p^{l-1})$$

resultando em no máximo dois valores para x.

Uma vez que os $\varphi(p^l\ )$ números estão distribuídos entre $\frac{1}{2}\ \varphi(p^l)$ posições ("escaninhos") de tal maneira que existem no máximo dois deles em cada um, segue que existem exatamente quatro em cada um, e, portanto a posição n dada contém exatamente duas soluções. Assim o número de soluções é

$$2 = 1 + \left(\frac{n}{p}\right).$$

■

TEOREMA 1.28. Seja $m > 0$ e $(n, m) = 1$. Então o número de soluções de

$$x^2 \equiv n\ (\text{mod } m)$$

Tem o seguinte valor

0 se $4|m, 8 \nmid m$ e $n \not\equiv 1 \pmod 4$;

0 se $8|m$ e $n \not\equiv 1 \pmod 4$

0 se um primo $p > 2$ para o qual $\left(\frac{n}{p}\right) = -1$ divide m.

Caso contrário, se s for o número de primos ímpares distintos $p|m$ então o número de soluções é

$$2^8 \text{ para } 4 \nmid m,$$
$$2^{8+1} \text{ para } 4|m, 8 \nmid m,$$
$$2^{8+2} \text{ para } 8|m.$$

Prova: Para $m = 1$ afirmação é verdadeira (o número de soluções é 1); para $m > 1$ o número de soluções para os vários primos $p|m$ e suas respectivas multiplicidades l aparecendo na decomposição canônica de m é multiplicativo, pelo teorema 71. Os enunciados então seguem. Porque se $p = 2$ então 0 é o número de soluções quando $4|m$, a não ser que ou $l = 2\ e\ n \equiv 1\ (mod\ 4)\ ou\ l > 2\ e\ n \equiv 1\ (mod\ 8)$ ·; $se\ p > 2$ é 0 quando $\left(\frac{n}{p}\right) = -1$. Caso contrário, a potencia de 2 se houver alguma, fornece o fator de um na última forma se $l = 1;\ 2\ se\ l = 2;\ e\ 4\ se\ l \geq 3$; e cada primo ímpar $p|m$ que ocorre fornecer um fator de 2.

A introdução a seguir do chamado símbolo de Jacobi, uma generalização do de Legendre, irá entre outras coisas tornar a decomposição prima de $|n|$ desnecessária para a análise completa de $\left(\frac{n}{p}\right)$, onde $p > 2\ e\ p \nmid n$. Em particular as cinco propriedades mais importantes (Teoremas 1.18, 1.21, 1.23, 1.25 e 1.26) do símbolo de Legendre serão válidas também para o símbolo de Jacobi. ■

1.5 FRAÇÕES DE FAREY

Este assunto, que é velho de mais de um século, mostrou-se recentemente ser de extraordinária utilidade no desenvolvimento da aritmética. O leitor encontrará suas aplicações principais nas partes quinta e sexta de Vorlesungen Über Zahlentheorie.

Definição 1.29. para um número fixo $n > 0$, sejam todas as frações reduzidas com denominadores positivos $\leq n$, ou seja, todos os racionais

$$\frac{a}{b}, \quad (a, b) = 1, \quad 0 < b \leq n,$$

arranjadas em rodem crescente; a sequência assim obtida é dita a sequência de Farey pertencente a n.

Incidentalmente, existem exatamente $\sum_{b=1}^{n} \varphi(b)$ frações assim em cada intervalo $g \leq \varepsilon < g + 1$ (pois para b fixo os valores de a que resultam de $g \leq \frac{a}{b} < g + 1$ constituem um conjunto de resíduos reduzido mod b no intervalo $gb \leq a < gb \leq + b$); como a sequencia de Farey é afinal transformadora em si própria por translação por 1, nos a conhecemos completamente se restringirmos simplesmente ao intervalo $0 \leq \varepsilon \leq 1$. Isto, contudo, não me importa no momento.

Exemplo: A seção da sequencia Farey petencente a $n = 7$ que está no intervalo $0 \leq \varepsilon \leq 1$ é

$$\frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}.$$

TEOREMA 1.30 Sejam $\frac{a}{b}$ e $\frac{a'}{b'}$ dois termos sucessivos da sequencia de Farey pertencente a n. Então em primeiro lugar temos

$$b + b' \geq n + 1,$$

e, além disso, temos

$$ba' - ab' = \pm 1 \text{ dependendo se } \frac{a}{b} \gtrless \frac{a'}{b'}.$$

Prova: por simetria podemos supor

$$\frac{a}{b} < \frac{a'}{b'}.$$

Então podemos determinar os números x e y correspondendo à a e a b para os quais

$$bx - ay = 1, \quad n - b < y \leq n,$$

pois temos $(b, -a) = 1$ e $b > 0$, de modo que existe um número y no conjunto completo de resíduos mod b indicando acima e então um x apropriado correspondente a y. Então temos

$$y > 0, \quad (x, y) = 1, \quad \frac{x}{y} = \frac{a}{b} + \frac{1}{by} > \frac{a}{b}.$$

Se puder mostrar que

$$\frac{x}{y} = \frac{a'}{b'}$$

então terei provado. Porque então

$$b'x = a'y, \quad y|b', \quad b'|y,$$
$$b' = y, \quad a' = x,$$

e, portanto, temos,

$$ba' - ab' = 1, \quad b + b' \geq n.$$

Suponha que

$$\frac{x}{y} \neq \frac{a'}{b'}.$$

Então, como $\frac{a'}{b'}$ é vizinha da direita de $\frac{a}{b}$ e como $\frac{x}{y}$ também pertence à sequência de Farey porque $(x, y) = 1$ e $0 < y \leq n$, seria que

$$\frac{x}{y} > \frac{a'}{b'},$$

de modo que na fórmula

$$\frac{x}{y} - \frac{a'}{b'} = \frac{xb' - ya'}{yb'}$$

o numerador a direita seria > 0 e logo ≥ 1. Teríamos com isso

$$\frac{x}{y} - \frac{a'}{b'} \geq \frac{1}{yb'}.$$

Da mesma forma $\left(\text{como } \frac{a'}{b'} > \frac{a}{b}\right)$ teríamos

$$\frac{a'}{b'} - \frac{a}{b} = \frac{ba' - ab'}{bb'} \geq \frac{1}{bb'}$$

somando e usando o fato que $b' \leq n$ obteríamos

$$\frac{1}{by} = \frac{bx - ay}{by} = \frac{x}{y} - \frac{a}{b} \geq \frac{1}{yb'} + \frac{1}{bb'} = \frac{b + y}{ybb'} > \frac{n}{ybb'} \geq \frac{1}{by},$$

o que é uma contradição. ■

TEOREMA 1.31. A mediante $\frac{a+a'}{b+b'}$ está entre $\frac{a}{b}$ e $\frac{a'}{b'}$ (e logo certamente não é um termo da sequência de Farey); sua distância de $\frac{a}{b}$ e $\frac{a'}{b'}$ é $\frac{1}{b(b+b')}$ e $\frac{1}{b'(b+b')}$, respectivamente.

Prova: Sem perda de generalidade, seja $ab < \frac{a'}{b'}$; então pelo teorema 1.31 temos

$$\frac{a'}{b'} - \frac{a + a'}{b + b'} = \frac{ba' - ab'}{b'(b + b')} = \frac{1}{b'(b + b')} > 0,$$

$$\frac{a + a'}{b + b'} - \frac{a}{b} = \frac{ba' - ab'}{b(b + b')} = \frac{1}{b(b + b')} > 0$$

■

TEOREMA 1.32. Dado qualquer número $n > 0$ e qualquer real ε existe uma fração $\frac{a}{b}$ para qual

$$(a, b) = 1, \quad 0 < b, \leq n, \quad \left|\varepsilon - \frac{a}{b}\right| \leq \frac{1}{b(n + 1)}.$$

Prova: Se considerarmos todas as frações de Farey pertencentes a n e as mediantes de cada par então ε está certamente contido em pelo menos um intervalo entre uma fração de Farey $\frac{a}{b}$ (inclusive) e uma das duas mediantes $\frac{a+a'}{b+b'}$ (inclusive) que pertencem ela. Assim pelos teoremas 1.30 e 1.32 temos

$$\left|\varepsilon - \frac{a}{b}\right| \leq \left|\frac{a + a'}{b + b'} - \frac{a}{b}\right| = \frac{1}{b(b + b')} \leq \frac{1}{b(n + 1)}.$$

■

TEOREMA 1.33. Dado $\mu \geq 1$ e $\varepsilon \gtreqless 0$ existe uma fração $\frac{a}{b}$ para a qual

$$(a, b) = 1, \quad 0 < b, \leq \mu, \quad \left|\varepsilon - \frac{a}{b}\right| \leq \frac{1}{b\mu}.$$

Prova: Pelo teorema 1.32 com $n = [\mu]$. ■

CAPITULO II

2 DECOMPOSIÇÃO EM DOIS QUADRADOS

As letras n, n_1, n_2, d, d_1 e d_2 neste capítulo sempre representarão números positivos.

TEOREMA 2.1: Se

$$n > 1,\ l^2 \equiv -1 \ (\text{mod n}),$$

Então

(1) $n = x^2 + y^2, x > 0, y > 0\ (x, y) = 1,\ y \equiv lx\ (\text{modn})$ é sempre solúvel, e a solução é única prova: (Solubilidade) pelo teorema 1.33, temos dado $\mu \geq 1$ e $\varepsilon \gtrless 0$ existe uma fração $\frac{a}{b}$ para a qual

$$(a, b) = 1, 0 < b, \leq \mu, \left|\varepsilon - \frac{a}{b}\right| \leq \frac{1}{b\mu}$$

Daí temos que $\left(com\ \mu = \sqrt{n}, \varepsilon = -\frac{l}{n}\right)$, correspondendo ao n e l dados existem dois números a e b para os quais

$$(a, b) = 1, 0 < b, \leq \sqrt{n}, \left|-\frac{l}{n} - \frac{a}{b}\right| \leq \frac{1}{b\sqrt{n}}$$

Se fizermos

$$lb + na = c$$

Então segue que

$$\left|-\frac{l}{n} - \frac{a}{b}\right| \leq \frac{1}{b\sqrt{n}} \Rightarrow \left|\frac{-lb-na}{nb}\right| \leq \frac{1}{b\sqrt{n}}$$

$$\left|\frac{-lb-na}{|nb|}\right| \leq \frac{1}{b\sqrt{n}} \Rightarrow \left|\frac{lb+na}{nb}\right| \leq \frac{1}{b\sqrt{n}}$$

$$|lb + na| \leq \frac{nb}{b\sqrt{n}} \Rightarrow |lb + na| \leq \frac{n}{\sqrt{n}}$$

$$|lb + na| \leq \sqrt{n} \Rightarrow |c| < \sqrt{n}$$

Daí vem

$$c \equiv lb\ (\text{modn}), |c| < \sqrt{n}$$

De modo que:

$$0 < b < \sqrt{n}$$

Elevando-se ambos os lados da desigualdade ao quadrado, temos

$$0 < b^2 < n \qquad \text{(I)}$$

Com isso, temos que

$$|c| < \sqrt{n}$$

Elevando-se ao quadrado, temos

$$c^2 < n \qquad \text{(II)}$$

Somando-se (I) e (II), vem

$$0 < b^2 + c^2 < 2n$$

Como:

$$b^2 + c^2 \equiv b^2 + l^2b^2 \equiv (1 + l^2)b^2 \equiv 0 \ (\text{mod}n)$$

Segue que

$$b^2 + c^2 = n$$

Além disso, temos $(b, c) = 1$; pois de

$$n = b^2 + (lb + na)^2 \rightarrow n = b^2 + l^2b^2 + 2lbna + n^2a^2$$

$$\Rightarrow 1 = \frac{b^2 + l^2b^2}{n} + 2lba + na^2 \Rightarrow 1 = \frac{(1 + l^2)b^2}{n} + 2lba + na^2$$

$$\Rightarrow 1 = \frac{(b^2 + l^2)b^2}{n} + lba + lba + na^2$$

$$\Rightarrow 1 = \left[\frac{(1 + l^2)b}{n} + la\right]b + a(lb + na)$$

Então existem u e c tais que:

$$1 = ub + ac \Rightarrow ub + ac = 1$$

$c \neq 0$; pois caso contrário teríamos

$$b^2 = n > 1 \text{ e } (b, c) > 1$$

No caso $c > 0$ a escolha

$$x = b, y = c$$

Faz isso, pois

$$n = (-c^2) + b^2, -c > 0, b > 0, (-c, b) = 1,$$

$$b \equiv -l^2b \equiv -lc \equiv l(-c) \ (\text{mod}n).$$

2°) (Unidade) Sejam x_1, y_1 e $x_2\ y_2$ Satisfazendo as condições un (1).

Então temos:

$$n = x_1^2 + y_1^2 \therefore n = x_2^2 + y_2^2$$

$$n \,.\, n = (x_1^2 + y_1^2)(x_2^2 + y_2^2)$$

$$n^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - y_1 x_2)^2$$

Prova:

Como $n = x_1^2 + y_1^2$ e $n = x_2^2 + y_2^2$

$$n^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2)$$

$$n^2 = x_1^2 x_2^2 + x_1^2 y_2^2 + y_1^2 x_2^2 + y_1^2 y_2^2$$

$$n^2 = \underbrace{x_1^2 x_2^2 + y_1^2 y_2^2}_{(I)} + \underbrace{x_1^2 y_2^2 + y_1^2 x_2^2}_{(II)}$$

Mudamos do à ordem das parcelas.

Observe que: $x_1^2 x_2^2 + y_1^2 y_2^2$, pela relação $a^2 + b^2 = (a + b)^2 - 2ab$, temos que:

$$x_1^2 x_2^2 + y_1^2 y_2^2 = (x_1 x_2 + y_1 y_2)^2 - 2x_1 x_2 y_1 y_2;$$

Portanto usaremos para as 2 últimas parcelas, temos; $x_1^2 y_2^2 + y_1^2 x_2^2 = (x_1 y_2 + y_1 x_2) - 2x_1 y_2 y_1 x_2$ teremos 2 termos iguais sobrando $-2x_1 x_2 y_1 y_2$, e $-2x_1 y_2 y_1 x_2$

Usaremos então que:

$$x_1^2 y_2^2 + y_1^2 x_2^2 = (x_1 y_2 - y_1 x_2)^2 + 2x_1 y_2 y_1 x_2$$

Então votando a expressão, temos

$$n^2 = x_1^2 x_2^2 + y_1^2 y_2^2 + x_2^2 y_2^2 + y_1^2 x_2^2$$

Substituindo agora, temos que:

$$n^2 = [(x_1 x_2 + y_1 y_2)^2 - 2x_1 x_2 y_1 y_2] + [(x_1 y_2 - y_1 x_2)^2 + 2x_1 y_2 y_1 x_2]$$

$$n^2 = (x_1 x_2 + y_1 y_2)^2 - 2x_1 x_2 y_1 y_2 + (x_1 y_2 - y_1 x_2)^2 + 2x_1 y_2 y_1 x_2$$

$$n^2 = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - y_1 x_2)^2$$

Portanto

$$n^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - y_1 x_2)^2,$$

$$x_1 x_2 + y_1 y_2 \equiv x_1 x_2 + l x_1 l x_2 \equiv (1 + l^2) x_1 x_2 \equiv 0 \,(\text{mod} n)$$

Observe as congruências abaixo

$$y_1 \equiv l x_1 \,(\text{mod} n)$$

$$y_2 \equiv l x_2 \,(\text{mod} n),$$

Multiplicando-se as congruências temos

$$y_1y_2 \equiv lx_1lx_2 \quad y_1 \equiv lx_1 \text{ (mod}n\text{)}$$

De modo que como $x_1x_2 + y_1y_2 > 0$, se tivermos

$$x_1x_2 + y_1y_2 = n,$$

Obtemos

$$n^2 = n^2 + (x_1y_2 - y_1x_2)^2,$$

Daí

$$x_1y_2 + y_1x_2 = 0,$$

Logo

$$x_1x_2 + y_1y_2 = n \qquad\qquad x_1y_2 - y_1x_2 = 0$$

E daí

$$x_1x_2 = y_1y_2$$

Logo temos

$$\begin{cases} x_1y_2 = y_1x_2 \\ \text{ou} \\ x_1x_2 = y_1y_2 \end{cases}$$

A segunda opção não ocorre, pois de

$$\begin{cases} x_1 < y_1, \\ x_2 < y_2. \end{cases}$$

Segue $x_1x_2 < y_1y_2$, temos então $x_1y_2 = y_1x_2$. De $x_1 | y_1x_2$ e mdc $(x_1, y_1) = 1$ concluimos $x_1 | x_2$, $x_2 = kx_1$. Então $x_1y_2 = y_1x_2 \Rightarrow$

$$\Rightarrow x_1y_2 = y_1kx_1 \Rightarrow x_2 = ky_1$$

Agora, $n = x_2^2 + y_2^2$

$$\Rightarrow n = (kx_1)^2 + (ky_1)^2 \Rightarrow n = k^2x_1^2 + k^2y_1^2$$
$$\Rightarrow n = k^2(x_1^2 + y_1^2) \Rightarrow n = k^2n \Rightarrow$$
$$\Rightarrow k^2 = 1 \Rightarrow k = 1, \text{ daí}$$
$$x_1 = x_2 \text{ e } y_1 = y_2$$

■

TEOREMA 2.2. Seja $V(n)$ o número de soluções de

(2)

$$l^2 \equiv -1 \pmod{n}$$

Então o número de soluções de

(3)

$$n = x^2 + y^2,\ (x, y) = 1,$$

É $4V(n)$.

Observação: O valor de $V(n)$ foi determinado no Teorema 5 (o n daquele teorema é $= -1$ aqui e o m daquele teorema é n aqui):

$$V(n) = \begin{cases} 0, & \text{se } 4|n \text{ ou se um primo } p \equiv 3 \pmod 4 \text{ divide } n, \\ 2^s, & \text{se } 4 \nmid n, \text{nenhum primo } p \equiv 3 \pmod 4 \text{ divide } n, \\ \text{e } s, & \text{é o número de primos ímpares distintos } p|n. \end{cases}$$

Prova: 1) Para $n = 1$ o enunciado é trivial; temos

$$V(1) = 1,$$

E as quatro decomposições são

$$1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2.$$

2) Para $n > 1$ temos necessariamente $x \neq 0$ e $y \neq 0$ (uma vez que $(x, y) = 1$), e, portanto o número de soluções de (3) deve ser quatro vezes o número de soluções com as condições suplementares $x > 0$ e $y > 0$. Segue do Teorema 2.1 que para cada l satisfazendo (2) existe uma solução de (3) para o qual

$$x > 0, y > 0, \text{e } y \equiv lx \pmod{n}.$$

Reciprocamente, cada solução de (3) para qual $x > 0$ e $y > 0$ fornece exatamente um l satisfazendo (2) para o qual

(4)

$$y \equiv lx \pmod{n}.$$

Pois como $(x, y) = 1$ temos $(x, n) = 1$, e, portanto pelo teorema (1.27) é unicamente solúvel para $l \pmod{n}$, de modo que

$$0 \equiv n \equiv x^2 + y^2 \equiv x^2 + l^2x^2 \equiv (1 + l)^2x^2 \pmod{n},$$

$$0 \equiv 1 + l^2 \pmod{n}.$$

■

TEOREMA 2.3. O número $U(n)$ de soluções de

(4)

$$n = x^2 + y^2$$

É dado pela fórmula

$$U(n) = 4\sum_{d^2|n} V\left(\frac{n}{d^2}\right).$$

(Ou seja, d percorre todos os números positivos cujos quadrados dividem n).

Prova: Se os pares x, y forem classificados de acordo com os valores de $(x, y) = d$, onde $d^2|n$, então claramente nosso teorema segue do Teorema 2.2, uma vez que para $(x, y) = d$ (5) é equivalente à afirmação

$$\frac{n}{d^2} = x_1^2 + y_1^2, \qquad x_1 = \frac{x}{d}, \qquad y_1 = \frac{y}{d}, \qquad (x_1, y_1) = 1.$$

■

TEOREMA 2.4.

(6)

$$U(n) = 4\sum_{d|n} x(d),$$

Onde $x(d)$ é o caráter não principal mod 4, isto é,

$$x(d) = \begin{cases} 0, \text{ para } d \equiv 0 \pmod 2; \\ 1, \text{ para } d \equiv 1 \pmod 4; \\ -1, \text{ para } d \equiv 3 \pmod 4. \end{cases}$$

Escrito de outra forma,

$$U(n) = 4\sum_{u|n \; u \text{ ímpar}} (-1)^{\frac{u-1}{2}}.$$

Observação: Assim este teorema justifica o enunciado da resposta à segunda das questões da introdução.

Prova: Se $(n_1, n_2) = 1$ então temos,

$$V(n_1 n_2) = V(n_1)V(n_2),$$

De modo que pelo Teorema 2.3 temos

$$\frac{U(n_1 n_2)}{4} = \sum_{d^2|n_1 n_2} V\left(\frac{n_1 n_2}{d^2}\right)$$

$$= \sum_{d_1{}^2|n_1 d_2{}^2|n_2} V\left(\frac{n_1 n_2}{d_1^2 d_2^2}\right)$$

$$= \sum_{d_1{}^2 | n_1 d_2{}^2 | n_2} V\left(\frac{n_1}{d_1^2}\right) V\left(\frac{n_2}{d_2^2}\right)$$

(já que os números d para os quais $d^2 | n_1 n_2$ estão em correspondência unívoca com os produtos $d_1 d_2$ para os quais $d_1^2 | n_1$ e $d_2^2 | n_2$)

(7)

$$= \sum_{d_1^2} V\left(\frac{n_1}{d_1^2}\right) \cdot \sum_{d_2^2 | n_2} V\left(\frac{n_2}{d_2^2}\right) = \frac{U(n_1)}{4} \cdot \frac{U(n_2)}{4}.$$

Fazendo

$$\sum_{d|n} X(d) = W(n),$$

Então $W(n)$ tem também a propriedade que

$$W(n_1 n_2) = W(n_1) W(n_2), \text{ para } (n_1, n_2) = 1;$$

Pois

$$\sum_{d | n_1 n_2} X(d) = \sum_{d_1^2 | n_1 \, d_2^2 | n_2} X(d_1 d_2) = \sum_{d_1 | n_1} X(d_1) \sum_{d_2 | n_2} X(d_2).$$

Basta, portanto, já que (6) é obvio para $n = 1$ ($4 = 4.1$), provar que $n = p^1, l > 0$, quando então o enunciado fica

$$\frac{U(p^1)}{4} = X(p^1) + \cdots + X(p) + 1.$$

De fato temos que $V(1) = 1$, e pelo Teorema 1.27 (o valor de n lá sendo -1 aqui), ou então pela observação do Teorema 2.2, temos também

$$V(p^m) = \begin{cases} 1, & \text{para } p = 2, m = 1, \\ 0, & \text{para } p = 2, m > 1, \\ 0, & \text{para } p \equiv 3 \pmod 4, m > 0 \\ 2, & \text{para } p \equiv 1 \pmod 4, m > 0. \end{cases}$$

Segue do Teorema 2.5 que, para l par

(8)

$$\frac{U(p^l)}{4} = V(p^l) + V(p^{l-2}) + \ldots + V(p^2) + 1 =$$

$$= \begin{cases} 1, & \text{para } p = 2, \\ \frac{1}{2}\,2 + 1 = l + 1, & \text{para } p \equiv 1 \pmod 4, \\ 1, & \text{para } p \equiv 3 \pmod 4, \end{cases}$$

E que é ímpar

(9)

$$\frac{U(p^l)}{4} = V(p^l) + V(p^{l-2}) + \ldots + V(p^2) + 1 =$$

$$= \begin{cases} 1, & \text{para } p = 2 \\ 2\,\frac{l+1}{2}\,2 + 1 = l + 1, & \text{para } p \equiv 1 \pmod 4 \\ 0, & \text{para } p \equiv 3 \pmod 4 \end{cases}$$

Por outro lado, segue da definição que

$$X(p^l) + \ldots + X(p) + 1 = \begin{cases} 0 + \cdots + 0 + 1 = 1, & \text{para } p = 2, \\ 1 + \cdots + 1 + 1 = l + 1, & \text{para } p \equiv 1 \pmod 4, \\ 1 - 1 + \cdots + 1 = 1, & \text{para } p \equiv 3 \pmod 4, 2 - 1, \\ 1 + 1 - \cdots + 1 = 0, & \text{para } p \equiv 3 \pmod 4, 2|l. \end{cases}$$

(Estou plenamente consciente de ter repetido vários cálculos que ocorreram no começo da prova desta demonstração). ■

TEOREMA 2.5

$$\frac{U(n)}{4} = \begin{cases} 0, & \text{se existir um primo } p \equiv 3 \pmod 4 \text{ que divide } n, \\ & \text{com multiplicidade ímpar (precisamente),} \\ T(m), & \text{caso contrário, onde } m \text{ é o produto das potências} \\ & \text{de primos } p|n \text{ da forma } p \equiv 1 \pmod 4 \\ & \text{ocorrendo na decomposição canônica de } n. \end{cases}$$

Prova: Para $n = 1$ a afirmação é óbvia (1 = 1). Para $(n_1 n_2) = 1$ a equação

$$F(n_1 n_2) = F(n_1)F(n_2)$$

Vale para $\frac{U(n)}{4}$ (por (7)) como também (obviamente) para o lado direito da afirmação a ser provada. É, portanto suficiente provar a afirmação para $n = p^l, l > 0$. Neste caso segue de (8) que de fato temos

$$\frac{U(n)}{4} = \begin{cases} 1 = T(1), & \text{para } p = 2 \\ l + 1 = T(p^l), & \text{para } p \equiv 1 \pmod 4, \\ 1 = T(1), & \text{para } p \equiv 3 \pmod 4, 2|l, \\ 0 = 0, & \text{para } p \equiv 3 \pmod 4, 2 \nmid l \end{cases}$$

■

Teorema 2.6 Todo primo $p \equiv 1 \pmod 4$ pode ser escrito como uma soma de dois quadrados e, além disso, isso pode ser escrito de oito maneiras.

Prova: Do Teorema 2.4 ou do Teorema 2.5 $U(p) = 4.2 = 8$. (Mesmo Teorema 2.2 basta, já que $V(p) = 2$ e na equação $p = x^2 + y^2$ certamente temos $(x, y) = 1$.)

$p \equiv 1 \pmod 4$ pode ser escrito "essencialmente" de uma única maneira como uma soma de dois quadrados, pois as oito representações podem ser obtidas de qualquer uma delas trocando os sinais de x e de y e trocando as parcelas. Enunciado precisamente,

$$p \equiv x^2 + y^2, \quad x > 0, \quad y > 0, \quad 2|x$$

tem exatamente uma solução para $p \equiv 1 \pmod 4$. ■

CAPITULO III

3 DECOMPOSIÇÃO EM QUATRO QUADRADOS

Teorema 3.1 (Identidade de Euler)

(10)

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^1 + y_2^2 + y_3^2 + y_4^2) =$$
$$(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2$$
$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$$

Daí, temos que:

$$[(x_1y_1 + x_2y_2) + (x_3y_3 + x_4y_4)]^2 +$$
$$[(x_1y_2 - x_2y_1) + (x_3y_4 - x_4y_3)]^2 + [(x_1y_3 - x_3y_1) + (x_4y_2 - x_2y_4)]^2 +$$
$$+ [(x_1y_4 - x_4y_1) + (x_2y_3 - x_3y_2)]^2 \Rightarrow$$
$$\Rightarrow (x_1y_1 + x_2y_2)^2 + 2(x_1y_1 + x_2y_2)(x_3y_3 + x_4y_4) +$$
$$(x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1)^2 + 2(x_1y_2 - x_2y_1)(x_3y_4 - x_4y_3)$$
$$+ (x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_3y_1)^2 + 2(x_1y_3 - x_3y_1)(x_4y_2 - x_2y_4)$$
$$+ (x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1)^2 + 2(x_1y_4 - x_4y_1)(x_2y_1 - x_3y_2)$$
$$+ (x_2y_3 - x_3y_2)^2 \rightarrow (x_1y_1)^2 + 2(x_1y_1)(x_2y_2) + (x_2y_2)^2 \Rightarrow$$
$$2(x_1y_1 + x_2y_2)(x_3y_3 + x_4y_4) + (x_3y_3)^2 + 2(x_3y_3)(x_4y_4) +$$
$$+ (x_4y_4)^2 + (x_1y_2)^2 - 2(x_1y_2)(x_2y_1) + (x_2y_1)^2 +$$
$$2(x_1y_2 - x_2y_1)(x_3y_4 - x_4y_3) + (x_3y_4)^2 - 2(x_3y_4)(x_4y_3)^2$$
$$(x_4y_3)^2 + (x_1y_3)^2 - 2(x_1y_3)(x_3y_1) + (x_3y_1)^2 + 2(x_1y_3 - x_3y_1)(x_4y_2 - x_2y_4)$$
$$+ (x_4y_2)^2 - 2(x_4y_2)(x_2y_4) + (x_2y_4)^2 + (x_1y_4)^2 -$$
$$2(x_1y_4)(x_4y_1) + (x_4y_1)^2 + 2(x_1y_4 - x_4y_1)(x_2y_1 - x_3y_2)$$
$$+ (x_2y_3)^2 - 2(x_2y_3)(x_3y_2) + (x_3y_2)^2$$

Observe que depois de conferir as contas à esquerda depois de efetuadas as multiplicações, temos dezesseis expressões da forma $x_a^2 y_b^2$ $(a = 1, \dots, 4;\ b = 1, \dots, 4)$. Estes termos também aparecem à direita observe que:

$$(x_1^2 + x_2^2 + x_3^3 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \Rightarrow$$
$$\Rightarrow x_1^2 y_1^2 + x_1^2 y_2^2 + x_1^2 y_3^2 + x_1^2 y_4^2 + x_2^2 y_1^2 + x_2^2 y_2^2$$
$$\Rightarrow x_2^2 y_3^2 + x_2^2 y_4^2 + x_3^2 y_1^2 + x_3^2 y_2^2 + x_3^2 y_3^2 + x_3^2 y_4^2 + x_4^2 y_1^2 + x_4^2 y_2^2 + x_4^2 y_3^2 + x_4^2 y_4^2$$

Estes termos também aparecem à direita entre outros termos, pois entre os quatro parênteses à direita cada x_a é combinado com cada y_b com um coeficiente ± 1. Os outros vinte e quatro termos à direita, que são todos da forma $\pm 2x_a y_b x_c y_d, a < b, c < d$ cancelam mutuamente, pois à direita o coeficiente de

$$2x_1x_2 \text{ é } y_1y_2 - y_1y_2 - y_3y_4 + y_3y_4 = 0$$
$$2x_1x_3 \text{ é } y_1y_3 + y_2y_4 - y_1y_3 - y_2y_4 = 0$$
$$2x_1x_4 \text{ é } y_1y_4 - y_2y_3 + y_2y_3 - y_1y_4 = 0$$
$$2x_2x_3 \text{ é } y_2y_3 - y_1y_4 + y_1y_4 - y_2y_3 = 0$$
$$2x_2x_4 \text{ é } y_2y_4 + y_1y_3 - y_2y_4 - y_1y_3 = 0$$
$$2x_3x_4 \text{ é } y_3y_4 - y_3y_4 - y_1y_2 + y_1y_2 = 0$$

Teorema 3.2: para todo $p > 2$ existe um m para o qual

$$1 \leq m < p$$

e

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

é solúvel.

Observação: Sem a condição $m < p$ isto seria trivial

$$pp = p^2 + 0^2 + 0^2 + 0^2;$$

Mas seria também inútil.

Prova: os $\frac{p+1}{2}$ números $x^2, 0 \leq x \leq \frac{p-1}{2}$, são mutuamente incongruentes $(\text{mod } p)$, pois de $x_1^2 \equiv x_2^2$ segue que.

$x_1^2 x_2^2 \ (\text{mod } p)$, ou seja,

$p | x_1^2 - x_2^2 \rightarrow p | (x_1 - x_2)(x_1 + x_2)$

$\rightarrow p|x_1 - x_2\ e\ p|x_1x_2$, portanto $\rightarrow\ x_1 \equiv \pm\ x_2\ (\mathrm{mod}\ p)$, o mesmo se passa com os $\frac{p+1}{2}$ números $-1 - y^2, 0 \leq y \leq\ \frac{p-1}{2}$. Portanto como estes totalizam $p + 1$ números, e como existem apenas p classes residuais mod p, segue
(principio da casa dos pombos) que existe um par x, y para o qual.

$$x^2 \equiv -1 - y^2(\mathrm{mod}\ p), |\ x| < \frac{p}{2}, |y| < \frac{p}{2}$$

De fato:

$$p|x^2 - (-1 - y^2) \Rightarrow p|x^2 + 1 + y^2|$$
$$\Rightarrow x^2 + y^2 + 1 = mp, \text{com}\ m\ \in \mathbb{Z}$$

Mas $|x|, |y| < \frac{p}{2}$, então

$$mp = |x|^2 + |y|^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1$$
$$\Rightarrow \frac{p^2}{4} + \frac{p^2}{4} + 1 \Rightarrow 2\frac{p^2}{4} + 1 \rightarrow \frac{p^2}{2} + 1$$
$$\Rightarrow |x|^2 + |y|2 + 1 < \frac{p^2}{2} + 1 < \frac{p^2}{2} + \frac{p^2}{2} = 2\frac{p^2}{2} = p^2$$
$$\Rightarrow 0 < mp < p^2 \Rightarrow 0 < m < p$$

Teorema 3.3: para todo primo p

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

É solúvel.

Prova: para $p = 2 \Rightarrow 2 = 1^2 + 1^2 + 0^2 + 0^2$, ok, portanto, seja $p < 2$. Seja $m = m(p)$ o menor positivo para o qual
(11)

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

é solúvel. Pelo teorema 2.9, $m < p$ afirmamos que.

$$m = 1$$

De qualquer maneira, m é impar; caso contrário seguiria de (11) que

$$x_1 + x_2 + x_3 + x_4 \equiv 0\ (\mathrm{mod}\ 2)$$

Observe que;

$$(x_1 + x_2 + x_3 + x_4)^2 = (x_1 + x_2 + x_3 + x_4)(x_1 + x_2 + x_3 + x_4)$$

$$\Rightarrow x_1^2 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_2 + x_2^2 + x_2x_3 + x_2x_4 + x_1x_3 +$$

$$\Rightarrow x_2x_3 + x_3^2x_3x_4 + x_1x_4 + x_2x_4 + x_3x_4 + x_4^2$$

$$(x_1 + x_2 + x_3 + x_4)^2 = x_1^2x_2^2x_3^2x_4^2 + 2x_1x_2$$

$$+ 2x_1x_3 + 2x_1x_4 + 2x_2x_3 + 2x_2x_4 + 2x_3x_4$$

$$\Rightarrow (x_1 + x_2 + x_3 + x_4)^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2\underbrace{(x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4)}_{\| \; k\in\mathbb{Z}}$$

$$\Rightarrow (x_1 + x_2 + x_3 + x_4)^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2k$$

$$\Rightarrow (x_1 + x_2 + x_3 + x_4)^2 = 2k_1 + 2k$$

$$\Rightarrow (x_1 + x_2 + x_3 + x_4)^2 = 2(k_1 + k)$$

$$\Rightarrow (x_1 + x_2 + x_3 + x_4)^2 = 2k_3 \qquad k_3 \in \mathbb{Z}$$

Portanto, temos que:

$$(x_1 + x_2 + x_3 + x_4) \equiv 0 \pmod 2$$

De modo que, sem perda de generalidade,

$$x_1 + x_2 \equiv 0, \qquad x_3 + x_4 \equiv 0 \pmod 2$$

Isto é, se os x_k fossem todos ímpares ou todos pares, isto seria certamente verdade; se dois fossem pares e dois ímpares, será verdade depois de uma renumeração apropriada, portanto

$$\frac{m}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

Mas sabemos que $x_1 + x_2$ é múltiplo de 2, ou seja, $2|x_1 + x_2$ resta saber que $x_1 - x_2$ é múltiplo de 2 observe que:

$$a|b + c \qquad \text{e} \qquad a|b \qquad \text{então } a|c$$

Seja $a = 2 \; \therefore b = x_1 + x_2 \; \therefore c = x_1 - x_2$

$2|(x_1 + x_2) + (x_1 - x_2)|$ e $2|x_1 + x_2$, então $2|x_1 - x_2$.

Observe que:

$$\begin{cases} (x_1 + x_2) + (x_1 - x_2) = 2k_1 \\ x_1 + x_2 = 2k_2 \end{cases}$$

Subtraindo-se (I) de (II), temos,

$$(x_1 + x_2) + (x_1 - x_2) - (x_1 + x_2) = 2k_1 - 2k_2$$

$$x_1 - x_2 = 2\left(\frac{k_1 - k_2}{k_3}\right); k_3 \in \mathbb{Z}$$

$$x_1 - x_2 = 2k_3$$

Portanto, $2|x_1 - x_2$

Onde os quatro termos entre parênteses à direita serão inteiros em contradição com a minimalidade de m.

O Teorema 3.3**:** Será agora provado indiretamente. Suponhamos que $m > 1$ e logo ímpar e ≥ 3.

Sejam escolhidos, para $k = 1, 2, 3, 4$ de tal maneira que

$$y_k \equiv x_k \pmod{m}, \quad |y_k| < \frac{m}{2}$$

Isto pode ser feito, uma vez que $-\frac{m-1}{2} \leq y \leq \frac{m-1}{2}$ é um conjunto completo de resíduos,

Então temos:

De fato

$$\begin{cases} y_1 \equiv x_1 \ (mod\ m) \\ y_2 \equiv x_2 \ (mod\ m) \\ y_3 \equiv x_3 \ (mod\ m) \\ y_4 \equiv x_4 \ (mod\ m) \end{cases}, \Rightarrow y_1 + y_2 + y_3 + y_4 \equiv x_1 + x_2 + x_3 + x_4 \pmod{m}$$

$$\sum_k y_k^2 \equiv \sum_k x_k^2 \pmod{m}$$

$$\sum_k y_k^2 \equiv \sum_k x_k^2 \equiv mp \equiv 0 \pmod{m}$$

Então, temos que

$$m|\sum_k y_k^2 \Rightarrow \sum_k x_k^2 = mn\ n \in \mathbb{Z}$$

Se

$$n = \ \Rightarrow \sum_k y_k^2 = 0$$

$$\Rightarrow y_1^2 + y_2^2 + y_3^2 + y_4^2 = 0$$

cada y_i é zero $y_k \equiv x_k$ (mod m) $0 \equiv x_k$ (mod m)$\Rightarrow m|x_k$ para cada k, se $m|x_k$, então $m^2|(x_k)^2 \Rightarrow (x_k^2) = m^2t^2$, $t \in \mathbb{Z}$ logo $m^2|\sum_k x_k \Rightarrow m^2|mp \Rightarrow mp = m^2k \Rightarrow p = mk$, ou seja, $m|p$, contradição, pois $1 \leq m \leq p$.

Além disso $n < m$, pois por (12) $m.n < 4\frac{m^2}{4}$, observe que

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mn, \text{ daí}$$

$$|y_k| < \frac{m}{2} | \Rightarrow {y_k}^2 < \frac{m^2}{4} \Rightarrow {y_k}^2 < \frac{m^2}{4}$$

$$\Rightarrow m \cdot n < \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4}$$

$\Rightarrow m \cdot n < 4\frac{m^2}{4}$, ou seja.

$$\Rightarrow m \cdot n < m^2 \Rightarrow n < m$$

De (11) e (12) segue, por (10), que

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

$$mn = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

Multiplicando-se temos que.

(13)

$$m^2np = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

$$\Rightarrow m^2np = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 + x_4y_3)^2$$

$$\Rightarrow (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$$

Cada termo entre parênteses é $\equiv 0 \pmod m$, pois o 1º é:

$$\sum_i x_iy_i \equiv \sum {x_i}^2 \equiv 0 \pmod m$$

Observe que:

$$y_i \equiv x_i (mod\ m) \Rightarrow x_iy_i \equiv x_i^2 \pmod m$$

De fato temos

$$x_1y_1 \equiv x_1^2 \pmod m$$

$$x_2y_2 \equiv x_2^2 \pmod m$$

$$x_3y_3 \equiv x_3^2 \pmod m$$

$$x_4y_4 \equiv x_4^2 \pmod m$$

Portanto que somando-se todas essas congruências, temos

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod m$$

$\sum_i x_iy_i \equiv \sum_i x_i^2$, $(mod\ m)$, portanto

$$\sum_i x_iy_i \equiv \sum_i x_i^2 \equiv 0 \pmod m$$

Observamos ainda que:

$$x_ky_l - x_ly_k \equiv x_kx_l - x_lx_k \equiv 0\ (mod\ m)$$

De fato,

$$y_k \equiv x_k (\text{mod } m) \quad e \quad y_l \equiv x_l \ (\text{mod } m)$$

Multiplicando-se (I) por x_l, temos

$$x_l y_l \equiv x_k x_l \ (\text{mod } m) \qquad (III)$$

Multiplicando-se (II) por x_k, temos

$$x_k y_l \equiv x_k x_l \ (\text{mod } m) \qquad (IV)$$

Subtraindo-se (IV) de (III), vem

$$x_k y_l - x_l y_k \equiv x_k x_l - x_l x_k \ (\text{mod } m)$$

$x_k y_l - x_l y_k \equiv 0 \ (\text{mod } m)$, então

$$x_k y_l - x_l y_k \equiv x_k x_l - x_l x_k \equiv 0 \ (\text{mod } m)$$

De (13) segue, portanto que

$$np = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

Observe (13) que:

$$m^2 np = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

$$m^2 np = (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 + (x_1 y_2 - x_2 y_1 + x_3 y_4 + x_4 y_3)^2 +$$

$$(x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 x_4)^2 + (x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2)^2$$

Mas sabemos que m divide o 1º parênteses ao quadrado, então m^2 também divide, portanto

$$m^2 np = (mz_1)^2 + (mz_2)^2 + (mz_3)^2 + (mz_4)^2$$

$$m^2 np = m^2 (z_1^2 + z_2^2 + z_3^2 + z_4^2)$$

$$np = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

O que como $0 < n < m$, contradiz a minimalidade de m

3.1 TEOREMA DE LAGRANGE:

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

É solúvel para todo $n \geq 0$

Demo: para $n = 0$ e $n = 1$ ok

Seja $n > 1$, pelo **T.F.A.**, temos que $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$ pelo teorema 3.3 cada π pode ser escrito como soma de 4 quadrados de inteiros e pela identidade de Euler o resultado segue.

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

é solúvel para todo $n \geq 0$

Prova: para $n = 0$ e $n = 1$ ok

Observe que

Para $n = 0 \Rightarrow 0 = 0^2 + 0^2 + 0^2 + 0^2$ ok

Para $n = 1 \Rightarrow 1 = 1^2 + 0^2 + 0^2 + 0^2$ ok

Seja $n > 1$, pelo **T.F.A.**, temos

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_n$$

Pelo teorema (3.3), temos que:

Cada p_i pode ser escrito como soma de quatro quadrados de inteiros, ou seja,

$$p_i = \propto_{i,1}^2 + \propto_{i,2}^2 + \propto_{i,3}^2 + \propto_{i,4}^2, \text{ com } i = 1,\ldots, n,$$

então

$$n = \left(\propto_{1,1}^2 + \cdots + \propto_{1,4}^2\right)\left(\propto_{2,1}^2 + \cdots + \propto_{2,4}^2\right) \cdot \ldots \cdot \left(\propto_{n,1}^2 + \cdots + \propto_{n,4}^2\right)^2,$$

portanto, aplicando Euler $n - 1$ vezes chega-se ao resultado.

4 CONSIDERAÇÕES FINAIS

Ao término desse trabalho passamos a perceber e compreender de forma mais nítida uma interessante e importante propriedade dos números inteiros e particularmente dos inteiros não negativos, a qual está primordialmente fundamentada no Teorema de Lagrange. Tal propriedade possui inúmeras aplicações servindo de ferramenta na demonstração de resultados algébricos mais aprofundados.

O nosso desejo é que cada leitor desse trabalho, bem como os atuais e futuros professores de matemática se interessem pelo estudo da álgebra e de suas inúmeras particularidades a fim de que percebam sua beleza e suas aplicações nos diversos ramos da ciência.

5 BIBLIOGRAFIA

GONÇALVES. Adilson**. Introdução a Álgebra**. Rio de Janeiro: IMPA, 2003.

IEQUAIN, Arnaldo Garcia Yves. **Elementos de Álgebra**. Rio de Janeiro: IMPA, 2008.

LANDAU, Edmund Georg Hermann. **Teoria Elementar dos Números**. Rio de Janeiro: Ed. Ciência Moderna, 2002.

LEMOS, M. Criptografia, **Números Primos e Algoritmos**. 17º Colóquio Brasileiro de Matemática. Revistas do Professor de Matemática - SBM.

NIVEN, I., Zuckerman, H.S. and Montgomery, H.L. **An Introduction to the Theory of Numbers**. New York: Wiley, 1991.

SANTOS, José Plínio de Oliveira. **Introdução a Teoria dos Números**. São Paulo: IMPA, 1998.

SIDKI, S. **Introdução à Teoria dos Números**. 10º Colóquio Brasileiro de Matemática, IMPA, 1975.

SIERPINSKI, W. **A Selection of Problems in the Theory of Numbers**. Pergamon Press, 1964.

SILVA, Antônio de Andrade e. **Mutação**. XI Semana de Matemática: UFMT, 2006.