Decomposição dum Número Natural em Somas de Quadrados

Owen John Brison Egídio Gonçalves Pereira

Outubro de 2007

Conteúdo

Prefácio

O presente texto tem por base a *Dissertação de Mestrado*, do 2^o Ano do Curso de Mestrado em Matemática (Área de especialização de Matemática para o Ensino), da Faculdade de Ciências de Lisboa, apresentada em 1999.

O texto inicial foi ligeiramente alterado, tendo-se procurado corrigir as gralhas existentes.

Apresento os meus agradecimentos às seguintes entidades, pelo apoio concedido:
Magnífico Reitor da Universidade da Madeira
Presidente do Departamento de Matemática da Universidade da Madeira
Conselho Directivo da Escola Secundária do Funchal
Pelo apoio concedido, apresento os meus agradecimentos a:
Professor Doutor José Manuel Castanheira da Costa
Professor Doutor Owen John Brison
Professora Doutora Rita Vasconcelos
Professor Doutor Vítor Lopes
Mestre Elias Rodrigues
Mestre Sandra Mendonça, actualmente Professora Doutora
Dr. Jorge Moreira de Sousa
Meus alunos em 1997/1998 e 1998/1999
Todos aqueles que manifestaram o seu apoio

Introdução

O tema deste trabalho, *Decomposição de um número natural em somas de quadrados*, foi proposto pelo orientador, professor Doutor Owen John Brison e veio de encontro às minhas preferências, uma vez que pretendia um tema da área de Teoria dos Números e, até já tinha escrito um pequeno artigo na revista *Educação e Matemática*, da APM (Associação de Professores de Matemática) sobre ternos Pitagóricos. Esse tema foi retomado e desenvolvido.

Os vários Capítulos foram organizados por temas, de modo a apresentar os assuntos que eram necessários para a demonstração dos *teoremas essenciais* deste trabalho e que são os *Teoremas dos Dois Quadrados, dos Quatro Quadrados e dos Três Quadrados.*

Assim, no primeiro Capítulo, estão alguns resultados sobre *Congruências Lineares e Congruências Quadráticas.* Algumas proposições (elementares) foram apresentadas sem demonstração, podendo essa demonstração ser encontrada em qualquer livro elementar de *Teoria dos Números.*

No segundo Capítulo, estão algumas proposições sobre grupos Cíclicos relacionadas com alguns dos assuntos do primeiro Capítulo.

No terceiro Capítulo, temos alguns resultados sobre o *Anel dos Inteiros Gaussianos*, sendo de destacar o papel da chamada *Norma de um Inteiro Gaussiano.*

No qurto Capítulo, está desenvolvido o tema dos *Ternos Pitagóricos*, relacionando-o com três temas do Ensino Secundário: *Trigonometria, Números Complexos e Sucessões Definidas por Recorrência.*

No quinto Capítulo, estão alguns resultados sobre o *Anel dos Quaterniões* que simplificam algumas demonstrações, voltando a destacar-se o papel da aplicação *Norma.*

No sexto Capítulo, temos, finalmente, a parte mais interessante desta dissertação: O *Teorema dos Três Quadrados.* A demonstração deste Teorema é bastante longa e utiliza um Teorema de Dirichlet que afirma que, dados a e b, primos entre si, há infinitos primos na progressão aritmética de temo geral $an + b$. Este muito importante Teorema foi apresentado sem demonstração, uma vez que ele, por si só, é bem capaz de ser um tema para uma outra dissertação de Mestrado.

Para ilustrar a demonstração do *Teorema dos Três Quadrados*, está apresentado o modo decompor 30 e 33 em somas de três quadrados, sedo que é muito mais fácil conseguir essa decomposição por tentativas. No entanto, o objectivo é ilustrar a demonstração do referido *Teorema dos Três Quadrados* e não, obter a decomposição de 30 e 33 em somas de três quadrados.

No sétimo Capítulo, temos alguns resultados bastante curiosos sobre *Quadrados Não Nulos.*

Estes dois últimos Capítulos foram escritos com base na obra de Emil Grosswald, *Representation of Integers as Sums of Squares.*

Refira-se que o *Teorema dos Dois Quadrados* foi enunciado e demonstrado várias vezes, consoante o contexto, sendo uma das demonstrações da minha autoria. Outra demonstração da minha autoria e análoga a essa é sobre a proposição "Todo o número primo da forma $8n + 3$ é soma de três quadrados". Repare-se que a decomposição pode ser feita com duas parcelas iguais.

Funchal, Outubro de 2007
Egídio Gonçalves Pereira

Capítulo 1

Congruências Lineares e Congruências Quadráticas

1.1 Congruências Lineares

Definição 1 *Sejam $a, b, m \in \mathbb{Z}$, tais que $m \geq 1$. Diz-se que a é congruente com b, módulo m, e escreve-se $a \equiv b \pmod{m}$, se m divide $b - a$.*

Proposição 2 *Sejam $a, x, y \in \mathbb{Z}$, com $a \neq 0$, tais que a divide x e a divide y. Então, a divide $x + y$ e a divide $x - y$.*

Demonstração
Se a divide x e a divide y, então existem inteiros q_1 e q_2, tais que $x = aq_1$ e $y = aq_2$.
Então, $x + y = aq_1 + aq_2 = a(q_1 + q_2)$, pelo que a divide $x + y$.
E, de $x - y = aq_1 - aq_2 = a(q_1 - q_2)$, vem que a divide $x - y$.

Proposição 3 *Sejam $a, x, y \in \mathbb{Z}$, com $a \neq 0$, tais que a divide x. Então, a divide xy.*

Demonstração
Se a divide x, então existe um inteiro q, tal que $x = aq$. Então, $xy = (aq)y = a(qy)$.
Logo, a divide xy.

Proposição 4 *Sejam $a, b, c, d, m, n \in \mathbb{Z}$, com $m \geq 1, n \geq 0$. A relação binária acima definida é uma relação de equivalência com as seguintes propriedades:*

1. *Se $a \equiv b \pmod{m}$, então $a + c \equiv b + c \pmod{m}$*
2. *Se $a \equiv b \pmod{m}$, então $ac \equiv bc \pmod{m}$*
3. *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$*
4. *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$*
5. *Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.*

Demonstração
A propriedade reflexiva resulta do facto de m dividir zero .
Se m divide $b - a$, então m divide $a - b$, pelo que a relação é simétrica.

Se m divide $b-a$ e m divide $c-b$, então m divide $(b-a)+(c-b)$, ou seja, m divide $c-a$, pelo que a relação é transitiva.

Então, a relação considerada é uma relação de equivalência.

Além disso:

1. Se $a \equiv b \pmod m$, então m divide $b-a$. Mas, $b-a = (b+c)-(a+c)$. Logo, m divide $(b+c)-(a+c)$, donde se conclui que $a+c \equiv b+c \pmod m$.

2. Se $a \equiv b \pmod m$, então m divide $b-a$. Logo, m divide $(b-a)\,c$, donde se conclui que m divide $bc-ac$. Então, $ac \equiv bc \pmod m$.

3. Se m divide $b-a$ e m divide $d-c$, então m divide $(b-a)+(d-c)$, ou seja, m divide $(b+d)-(a+c)$. Então, $a+c \equiv b+d \pmod m$.

4. Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $ac \equiv bc \pmod m$ e $bc \equiv bd \pmod m$. Então, por transitividade, $ac \equiv bd \pmod m$.

   (a) $a^0 \equiv b^0 \pmod m$

   (b) Hipótese de indução: $a^n \equiv b^n \pmod m$

   (c) Tese: $a^{n+1} \equiv b^{n+1} \pmod m$
   Se $a^n \equiv b^n \pmod m$ e $a \equiv b \pmod m$, então $a^n \times a \equiv b^n \times b$, donde vem $a^{n+1} \equiv b^{n+1} \pmod m$.

Está, assim terminada a demonstração.

Definição 5 *Sejam $a, b \in \mathbb{Z}$ dois números não simultaneamente nulos. Máximo dividor comum entre a e b, que se escreve* $\operatorname{mdc}(a,b)$*, é um número natural d, tal que d divide a, d divide b e todo o número inteiro que seja divisor comum de a e de b divide d.*

Proposição 6 *Sejam $a, b \in \mathbb{Z}$ dois números não simultaneamente nulos. Máximo dividor comum entre a e b é o menor número positivo pertencente ao conjunto $S = \{ax+by \colon x, y \in \mathbb{Z}\}$.*

Demonstração

Suponhamos, sem perda de generalidade, que $a \neq 0$. Então, a e $-a$ pertencem a S, sendo que um desses dois números é positivo. Então, existe o menor elemento positivo de S. Seja d tal elemento mínimo. Então, $d = ax_0 + by_0$, para certos inteiros x_0 e y_0, uma vez que d pertence a S.

Seja u um número natural que divide a e divide b. Então, u divide ax_0 e u divide by_0, pelo que u divide $ax_0 + by_0$, ou seja, u divide d.

Falta provar que d divide a e divide b. Dividindo a por d, obtemos $a = dq + r$, com $q \in \mathbb{Z}$ e $0 \leq r < d$.

Então, $r = a - dq = a - (ax_0 + by_0)\,q = a\,(1 - qx_0) - bqy_0$, pelo que $r \in S$. Então, $r = 0$, pelo que d divide a.

Analogamente se mostra que d divide b.

A igualdade $d = ax_0 + by_0$ é conhecida por igualdade de Bézout e pode ser obtida pelo algoritmo de Euclides do qual se apresenta um exemplo:

Exemplo 7 *Calcule* $\operatorname{mdc}(146, 19)$*, aplicando o algoritmo de Euclides*

1. Dividimos 146 por 19: $146 = 7 \times 19 + 13$

2. Dividimos 19 por 13: $19 = 1 \times 13 + 6$

3. Dividimos 13 por 6: $13 = 2 \times 6 + 1$

4. Dividimos 6 por 1: $6 = 6 \times 1 + 0$

5. O último resto não nulo foi 1. Então, $\text{mdc}(146, 19) = 1$.

6.

$$\begin{aligned} 1 &= 13 - 2 \times 6 = 13 - 2 \times (19 - 13) = 3 \times 13 - 2 \times 19 \\ &= 3 \times (146 - 7 \times 19) - 2 \times 19 = 3 \times 146 - 21 \times 19 - 2 \times 19 \\ &= 3 \times 146 - 23 \times 19 \end{aligned}$$

Igualdade de Bézout: $1 = \text{mdc}(146, 19) = 3 \times 146 - 23 \times 19$.

Proposição 8 *Sejam a, b, c três números inteiros não nulos.*
Então, $\text{mdc}(\text{mdc}(a, b), c) = \text{mdc}(a, \text{mdc}(b, c))$.

Demonstração
Sejam $d_1 = \text{mdc}(\text{mdc}(a, b), c)$ e $d_2 = \text{mdc}(a, \text{mdc}(b, c))$.
Então, d_1 divide $\text{mdc}(a, b)$ e d_1 divide c. Logo, d_1 divide a, d_1 divide b e d_1 divide c.
Então, d_1 divide a e d_1 divide $\text{mdc}(b, c)$.
Então, d_1 divide $\text{mdc}(a, \text{mdc}(b, c))$. Logo, d_1 divide d_2.
Analogamente, se mostra que d_2 divide d_1.
E como estamos a considerar que o máximo divisor comum entre dois números inteiros é um número positivo, então $d_1 = d_2$, ou seja, $\text{mdc}(\text{mdc}(a, b), c) = \text{mdc}(a, \text{mdc}(b, c))$.
Observe-se que o resultado permanece válido, no caso de, apenas, um dos três números a, b, c ser nulo.

Proposição 9 *Sejam a, b, m três números inteiros, tais que $m > 0$ e $\text{mdc}(a, m) = 1$. Então, a congruência $ax \equiv b \pmod{m}$ tem solução e a solução é única, módulo m.*

Demonstração
Como $\text{mdc}(a, m) = 1$, existem inteiros x_0, y_0, tais que $ax_0 + my_0 = 1$.
Então, $a(bx_0) + m(by_0) = b$, donde se conclui que $a(bx_0) \equiv b \pmod{m}$. Logo, bx_0 é solução de $ax \equiv b \pmod{m}$. Seja u tal que $u \equiv bx_0 \pmod{m}$. Então, $au \equiv abx_0 \equiv b \pmod{m}$, pelo que u é solução de $ax \equiv b \pmod{m}$.
Falta provar que não há mais soluções. Sejam x_1 e x_2 duas soluções de $ax \equiv b \pmod{m}$.
Então, $ax_1 \equiv b \equiv ax_2 \pmod{m}$, pelo que $ax_1 \equiv ax_2 \pmod{m}$.
Logo, $ax_1 \equiv ax_2 \pmod{m}$, pelo que m divide $ax_2 - ax_1$, ou seja, m divide $a(x_2 - x_1)$.
Então, m divide $x_2 - x_1$, uma vez que $\text{mdc}(a, m) = 1$.
Então, $x_2 \equiv x_{12} \pmod{m}$, pelo que a solução é única, módulo m, uma vez que quaisquer duas soluções são congruentes, módulo m.
Sejam a, b, m três números inteiros, tais que $m > 0$ e $\text{mdc}(a, m) = d$. Então, a congruência $ax \equiv b \pmod{m}$ tem solução se e só se d divide b. Mais, se houver souver solução, então ela é única, módulo $\frac{m}{d}$.
Demonstração
Como $\text{mdc}(a, m) = d$, existem inteiros x_0, y_0, tais que $ax_0 + my_0 = d$. Suponhamos que d divide b. Então, $b = dq$, para certo inteiro q.
Então, $b = dq = ax_0q + my_0q$, donde se conclui que $a(x_0q) \equiv b \pmod{m}$. Logo, x_0q é solução de $ax \equiv b \pmod{m}$.
Reciprocamente, suponhamos que a congruência $ax \equiv b \pmod{m}$ tem solução z. Então, $az \equiv b \pmod{m}$, pelo que m divide $az - b$.

Mas, como d divide m, temos que d divide $az - b$. Logo, d divide b, uma vez que d divide a.

Falta provar que a solução e única, módulo $\frac{m}{d}$. Sejam x_1 e x_2 duas soluções de $ax \equiv b \pmod{m}$.

Então, $ax_1 \equiv ax_2 \pmod{m}$. Logo, m divide $ax_1 - ax_2$, pelo que existe um inteiro q tal que $mq = ax_1 - ax_2$.

Então, $\frac{m}{d}q = \frac{a}{d}x_1 - \frac{a}{d}x_2$. Então, $\frac{a}{d}x_1 \equiv \frac{a}{d}x_2 \left(\mathrm{mod}\, \frac{m}{d}\right)$.

Mas, $\mathrm{mdc}\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, pois, caso contrário, d não seria o máximo divisor comum entre a e m. Então, como $\frac{m}{d}$ divide $\frac{a}{d}(x_1 - x_2)$ e $\frac{m}{d}$ é primo com $\frac{a}{d}$, então $\frac{m}{d}$ divide $x_1 - x_2$, ou seja, $x_1 \equiv x_2 \left(\mathrm{mod}\, \frac{m}{d}\right)$.

Proposição 10 *Sejam p um número primo e $P(x)$, um polinómio na indeterminada x, de grau n e coeficientes em $\mathbb{Z}$, cujo coeficiente director (coeficiente do termo de maior grau) é um número primo com p. Então, a congruência $P(x) \equiv 0 \pmod{p}$, não tem mais do que n soluções, mutuamente incongruentes, módulo p.*

Demonstração

Já sabemos que a propriedade é válida para $n = 1$.

Hipótese de indução: a propriedade verifica-se para um certo inteiro n.

Tese: a propriedade verifica-se para o número inteiro $n + 1$, isto é, se $\mathrm{mdc}(a_{n+1}, p) = 1$, então $a_{n+1}x^{n+1} + a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$ não tem mais de $n + 1$ soluções.

Demonstração da Tese:

Se uma congruência polinomial de grau $n + 1$ não tiver solução, não terá mais de $n + 1$ soluções.

Seja $a_{n+1}x^{n+1} + a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$, uma congruência polinomial de grau $n + 1$, com $\mathrm{mdc}(a_{n+1}, p) = 1$.

Suponhamos que a congruência anterior tem uma solução α.

Então, a congruência será equivalente a $(x - \alpha)(b_n x^n + \cdots + b_1 x + b_0) + r \equiv 0 \pmod{p}$, com os novos coeficientes dados pela regra de Rufinni, tendo-se que p divide r e $b_n = a_{n+1}$.

Então, a congruência inicial (de grau $n + 1$) é equivalente a $(x - \alpha)(b_n x^n + \cdots + b_1 x + b_0) \equiv 0 \pmod{p}$.

Então, $x \equiv \alpha \vee b_n x^n + \cdots + b_1 x + b_0 \equiv 0 \pmod{p}$.

Ora, por hipótese de indução, $b_n x^n + \cdots + b_1 x + b_0 \equiv 0 \pmod{p}$ não tem mais de n soluções, porque $b_n = a_{n+1}$ e $\mathrm{mdc}(a_{n+1}, p) = 1$.

Então, uma congruência polinomial de grau $n + 1$ não tem mais de $n + 1$ soluções, mutuamente incongruentes, módulo p.

Proposição 11 *Sejam m, n dois números naturais. Um número inteiro x é primo com mn se e só se, tal número x é primo com m e é primo com n.*

Demonstração

Seja x um número inteiro, primo com mn. Então, existem inteiros u e v, tais que $1 = (mn)u + xv = m(nu) + xv = n(mu) + xv$.

Então,

Definição 12 *Seja $m \in \mathbb{Z}$, com $m \geq 1$. Sistema residual completo (SRC), módulo m, é um conjunto maximal de inteiros mutuamente incongruentes, módulo m.*

Sistema residual reduzido (SRR), módulo m, é um conjunto maximal de inteiros primos com m e mutuamente incongruentes, módulo m.

Função φ de Euler é a aplicação de $\mathbb{N}$ em $\mathbb{N}$, tal que $\varphi(n)$ é o número de elementos de $\{1, 2, \ldots, n\}$ que são primos com n, ou seja, $\varphi(n)$ é o número de elementos de um sistema residual reduzido, módulo n.

Proposição 13 *A função φ de Euler é uma aplicação multiplicativa, isto é, se m e n são números naturais primos entre si, então $\varphi(mn) = \varphi(m) \times \varphi(n)$.*

Demonstração

Se $m = 1$ ou $n = 1$, a afirmação é verdadeira, porque $\varphi(1) = 1$. Suponhamos que m e n são maiores que 1 e consideremos os números naturais de 1 a nm, colocados na seguinte tabela:

1	2	$\cdots$	$m-1$	m
$m+1$	$m+1$	$\cdots$	$2m-1$	$2m$
$2m+1$	$2m+1$	$\cdots$	$3m-1$	$3m$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(n-1)m+1$	$(n-1)m+2$	$\cdots$	$nm-1$	nm

Na primeira linha desta tabela, há $\varphi(m)$ números primos com m. E o mesmo acontece com as restantes linhas.

Quanto a cada coluna, temos que todos os elementos são primos com m ou nehum elemento é primo com m.

Então, temos $\varphi(m)$ colunas em que todos os elementos são primos com m e temos $m-\varphi(m)$ colunas em que nenhum elemento é primo com m.

Então, na tabela anterior, há $n\varphi(m)$ números primos com m.

Mas, em cada coluna, todos os elementos são incongruentes, módulo n. Então, em cada coluna, há $\varphi(n)$ números primos com n e há $n - \varphi(n)$ números que não são primos com n.

Logo, dos $n\varphi(m)$ números primos com m, há que descontar os $\varphi(m)(n - \varphi(n))$ números que não são primos com n e que se encontram nas $\varphi(m)$ colunas referidas.

Então,

$$\varphi(mn) = n\varphi(m) - \varphi(m)(n - \varphi(n)) = n\varphi(m) - n\varphi(m) + \varphi(m)\varphi(n) = \varphi(m)\varphi(n)$$

Ainda há um processo mais fácil:

Os números primos com m são todos os elementos de $\varphi(m)$ colunas.

Os números primos com n são todos os elementos de $\varphi(n)$ colunas.

Então, os elementos primos com m e com n são os $\varphi(m)\varphi(n)$ elementos que estão simultaneamente em tais linhas e colunas.

Proposição 14 *Sejam φ a função de Euler, p um número primo e n um número natural. Então, $\varphi(p^n) = p^{n-1}(p-1)$.*

Demonstração

Se p é um número primo, então $\varphi(p) = p - 1 = p^0(p-1)$.

Se $p = 2$, então $\varphi(p^n) = \varphi(2^n) = 2^{n-1} = 2^{n-1}(2-1)$, porque os números menores que 2^n e primos com 2^n são todos os números ímpares menores que 2^n $(1, 3, \ldots, 2^n - 1)$.

Se p é um número primo ímpar e n maior que 1, os números pertencentes ao conjunto $\{1, 2, \ldots, p^n\}$ que não são primos com p^n são $p, 2p, \ldots, p^{n-1} \times p$. Então, há p^{n-1} números pertencentes ao conjunto $\{1, 2, \ldots, p^n\}$ que não são primos com p^n.

Então, $\varphi(p^n) = p^{n-1}(p-1)$.

Está, pois, terminada a demonstração.

Corolário 15 *Sejam a função de Euler, $p_1, \ldots, p_k$, k primos distintos dois a dois e $\alpha_1, \ldots, \alpha_k$, k números naturais. Então,*

$$\varphi\left(p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}\right) = p_1^{\alpha_1 - 1}(p_1 - 1) \times \cdots \times p_k^{\alpha_k - 1}(p_k - 1)$$

Demonstração
Os números $p_1, \ldots, p_k$ são primos distintos dois a dois. Então, $p_1^{\alpha_1}$,...,$p_k^{\alpha_k}$ são primos entre si.
Então,

$$\begin{aligned}\varphi\left(p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}\right) &= \varphi\left(p_1^{\alpha_1}\right) \times \cdots \times \varphi\left(p_k^{\alpha_k}\right) \\ &= p_1^{\alpha_1 - 1}\left(p_1 - 1\right) \times \cdots \times p_k^{\alpha_k - 1}\left(p_k - 1\right)\end{aligned}$$

Proposição 16 *Sejam φ a função de Euler, p um número primo e n um número natural. Então, $\varphi\left(p^n\right) = p^{n-1}\left(p-1\right)$.*

Demonstração
Se p é um número primo, então $\varphi\left(p\right) = p - 1 = p^0\left(p-1\right)$.
Se $p = 2$, então $\varphi\left(p^n\right) = \varphi\left(2^n\right) = 2^{n-1} = 2^{n-1}\left(2-1\right)$, porque os números menores que 2^n e primos com 2^n são todos os números ímpares menores que 2^n (ou seja, $1, 3, \ldots, 2^n - 1$).
Se p é um número primo ímpar e n maior que 1, os números pertencentes ao conjunto $\{1, 2, \ldots, p^n\}$ que não são primos com p^n são $p, 2p, \ldots, p^{n-1} \times p$. Então, há p^{n-1} números pertencentes ao conjunto $\{1, 2, \ldots, p^n\}$ que não são primos com p^n.
Então, $\varphi\left(p^n\right) = p^{n-1}\left(p-1\right)$.

Proposição 17 *Sejam φ a função de Euler, p um número primo e n um número natural. Então, $\sum\limits_{d|p^n} \varphi\left(d\right) = p^n$.*

Demonstração
Os divisores de p^n são $1, p, \ldots, p^n$.
Então,

$$\begin{aligned}\sum_{d|p^n} \varphi\left(d\right) &= \sum_{k=0}^{n} \varphi\left(p^k\right) = \varphi\left(1\right) + \varphi\left(p\right) + \cdots + \varphi\left(p^n\right) \\ &= 1 + 1\left(p-1\right) + \cdots + p^{n-1}\left(p-1\right) \\ &= 1 + \left(p-1\right)\left(1 + p + \cdots + p^{n-1}\right) \\ &= 1 + \left(p-1\right) \times \frac{p^n - 1}{p-1} = 1 + p^n - 1 \\ &= p^n\end{aligned}$$

Nesta demonstração utilizamos o facto de, excluída a primeira parcela, termos uma soma de termos consecutivos duma progressão geométrica de primeiro termo 1 e razão p.
A demonstração podia ter sido feita por indução em n.

Proposição 18 *Sejam φ a função de Euler, k um número natural, $p_1, \ldots, p_k$ k primos distintos dois a dois, $\alpha_1, \ldots, \alpha_k$, k números naturais e $m_k = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$. Então, $\sum\limits_{d|m_k} \varphi\left(d\right) = m_k$.*

Demonstração
Pela proposição anterior, sabemos que a presente proposição é válida para $k = 1$. Suponhamos que a mesma é válida para um natural k. Pretendemos mostrar que a afirmação é válida para $k+1$.
Seja $m_{k+1} = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} \times p_{k+1}^{\alpha_{k+1}}$.
Os divisores do número m_{k+1} são os divisores de m_k multiplicados pelos divisores de $p_{k+1}^{\alpha_{k+1}}$, sendo estes últimos $1, p_{k+1}, \ldots, p_{k+1}^{\alpha_{k+1}}$, os quais são primos com os divisores de m_k.

Então,

$$\begin{aligned}
\sum_{d|m_{k+1}} \varphi(d) &= \sum_{d_1|m_k \wedge d_2|p_{k+1}^{\alpha_{k+1}}} \varphi(d_1 \times d_2) \\
&= \sum_{d_1|m_k \wedge d_2|p_{k+1}^{\alpha_{k+1}}} (\varphi(d_1) \times \varphi(d_2)) \\
&= \sum_{d_1|m_k} \varphi(d_1) \times \sum_{dd_2|p_{k+1}^{\alpha_{k+1}}} \varphi(d_2) \\
&= p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} \times \sum_{dd_2|p_{k+1}^{\alpha_{k+1}}} \varphi(d_2) \\
&= p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} \times p_{k+1}^{\alpha_{k+1}} \\
&= m_{k+1}
\end{aligned}$$

Está, assim, terminada a demonstração.

Corolário 19 *Seja m um número natural. Então, $\sum_{d|m} \varphi(d) = m$.*

Demonstração

O único caso que falta demonstrar é $m = 1$. Mas este caso é trivial, porque o único divisor natural de 1 é 1 e $\varphi(1) = 1$.

Proposição 20 *(Teorema de Wilson)*

Seja $p \in \mathbb{N}$, um número primo. Então, $(p-1)! \equiv -1 \pmod{p}$.

Demonstração

Se $p = 2$, temos $(p-1)! = (2-1)! = 1! = 1 \equiv -1 \pmod{2}$.

Se $p = 3$, temos $(p-1)! = (3-1)! = 2! = 2 \equiv -1 \pmod{3}$.

Se $p > 3$, associamos os factores 1 e $p-1$ e procuramos associar os restantes factores de $(p-1)!$, dois a dois, de modo que o produto de cada par de factores seja congruente com 1, módulo p. Se tal for possível, teremos que $(p-1)! \equiv -1 \pmod{p}$.

Vejamos que essa associação pode ser feita:

Consideremos um número inteiro a, tal que $1 < a < p-1$. Como $\operatorname{mdc}(a, p) = 1$, a congruência linear $ax \equiv 1 \pmod{p}$ tem solução única, pelo que existe um único natural b, tal que $1 < b < p-1$ e $ab \equiv 1 \pmod{p}$. Tal b tem de ser diferente de a, pois se fosse $b = a$, teríamos $a^2 \equiv 1 \pmod{p}$, congruência esta que só tem as soluções 1 e $p-1$. Tal b tem de ser diferente de $p-1$, pois se fosse $b = p-1$, teríamos $ab = a(p-1) \equiv -a \pmod{p}$. Então, teríamos $a \equiv -1 \pmod{p}$ o que é falso.

Então, associamos a com b. Se $p = 5$, nada mais temos a fazer. Se $p > 5$, então escolhemos um elemento a_1, tal que $1 < a_1 < p-1$, $a_1 \neq a$ e $a_1 \neq b$. E, novamente, existe um único natural b_1, diferente de a_1, tal que $1 < b_1 < p-1$ e $a_1 b_1 \equiv 1 \pmod{p}$. Note-se que $b_1 \neq a$ e $b_1 \neq b$, pois caso contrário, a congruência linear $ax \equiv 1 \pmod{p}$ não teria solução única. Por isso os novos números a serem associados são distintos dos anteriores.

Como $p-1$ é um número par, o processo continua até esgotarmos todos os factores de $(p-1)!$.

Finalmente, temos que $(p-1)! \equiv -1 \times 1 \times 1^{\frac{p-3}{2}} \equiv -1 \pmod{p}$.

Observação

$$\begin{aligned}
a^2 \equiv 1 \pmod{p} &\iff p \,|\, a^2 - 1 \iff p \,|\, (a+1)(a-1) \\
&\iff p \,|\, a+1 \vee p \,|\, a+1 \\
&\iff a \equiv -1 \pmod{p} \vee a \equiv 1 \pmod{p}
\end{aligned}$$

Proposição 21 *(Recíproco do Teorema de Wilson)*
Seja $m \in \mathbb{N}$, tal que $m > 1$ e $(m-1)! \equiv -1 \pmod{m}$. Então, m é primo.

Demonstração
Suponhamos que $m > 1$ e que m não é primo e que $(m-1)! \equiv -1 \pmod{m}$. Então, existe um número primo p, tal que p divide m. Tal p é menor que m, pelo que p é um dos factores de $(m-1)!$. Além disso m divide $(m-1)!+1$ e p será um divisor de $(m-1)!+1$. Logo, p dividiria 1, o que não pode acontecer. Então, se $m > 1$ e $(m-1)! \equiv -1 \pmod{m}$, é absurdo supor que m não é primo.

Corolário 22 *Seja p um número primo tal que $p \equiv 1 \pmod{4}$. Então a congruência $x^2 \equiv -1 \pmod{p}$ admite a solução $\frac{p-1}{2}!$.*

Demonstração
Pelas proposições anteriores, sabemos que $(p-1)! \equiv -1 \pmod{p}$.
Como $p \equiv 1 \pmod{4}$, existe um número natural n, tal que $p = 4n+1$. Então,

$$\begin{aligned}(p-1)! = (4n)! &\equiv 1 \times 2 \times \cdots \times (2n-1) \times (2n) \times (2n+1) \times \cdots \times (4n) \pmod{p} \\ &\equiv 1 \times 2 \times \cdots \times (2n-1) \times (2n) \times (-2n) \times (-2n+1) \times \cdots \times (-2) \times (-1) \pmod{p} \\ &\equiv 1^2 \times 2^2 \times \cdots \times (2n-1)^2 \times (2n)^2 \times (-1)^{2n} \pmod{p} \\ &\equiv (1 \times 2 \times \cdots \times (2n))^2 \pmod{p} \\ &\equiv ((2n)!)^2 \pmod{p}\end{aligned}$$

Então, $((2n)!)^2 \equiv -1 \pmod{p}$. Logo, a congruência quadrática $x^2 \equiv -1 \pmod{p}$ admite a solução $(2n)!$, ou seja, $\frac{p-1}{2}!$.
É claro que $-\left(\frac{p-1}{2}!\right)$ também é solução da mesma congruência quadrática.

Proposição 23 *Proposição (Teorema de Euler-Fermat)*
Sejam φ a função de Euler, m um número natural e $a \in \mathbb{Z}$, tais que $\operatorname{mdc}(a,m) = 1$. Então, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demonstração
Seja $R = \{x_1, x_2, \ldots, x_{\varphi(m)}\}$ um sistema residual reduzido, módulo m.
Seja $S = \{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$. Vejamos que S também é um sistema residual reduzido, módulo m:
Suponhamos que $ax_i \equiv ax_j \pmod{m}$. Então, m divide $ax_i - ax_j$, ou seja, m divide $a(x_i - x_j)$. Mas, como m é primo com a, m divide $x_i - x_j$, donde se conclui que $x_i \equiv x_j \pmod{m}$ e, portanto, que $x_i = x_j$.
Então os elementos de S são mutuamente incongruentes, módulo m, pelo que S é um sistema residual reduzido, módulo m.
Então, cada elemento de S é congruente, módulo m, com um elemento de R.
Logo, $x_1 x_2 \cdots x_{\varphi(m)} \equiv ax_1 ax_2 \cdots ax_{\varphi(m)} \pmod{m}$ e, uma vez que $x_1, x_2, \ldots, x_{\varphi(m)}$ são primos com m, temos que $1 \equiv a^{\varphi(m)} \pmod{m}$.

Corolário 24 *(Teorema de Fermat)*

Sejam $p \in \mathbb{N}$ um número primo e $a \in \mathbb{Z}$, tais que p não divide a. Então, $a^{p-1} \equiv 1 \pmod{p}$.
Demonstração
Consequência imediata do corolário anterior, pois $\operatorname{mdc}(a,p) = 1$ e $\varphi(p) = p-1$.

Corolário 25 *Seja $p \in \mathbb{N}$ um número primo e seja $a \in \mathbb{Z}$. Então, $a^p \equiv a \pmod{p}$.*

Demonstração
Se p divide a, então $a^p \equiv 0 \equiv a \pmod{p}$.
Se p não divide a, então $a^{p-1} \equiv 1 \pmod{p}$, donde se conclui que $a^p \equiv a \pmod{p}$.
Está, assim, terminada a demonstração.

Definição 26 *Sejam m um inteiro positivo e $a \in \mathbb{Z}$, tais que $\mathrm{mdc}(a, m) = 1$. Ao menor inteiro positivo t, tal que $a^t \equiv 1 \pmod{m}$, chama-se ordem de a relativamente ao módulo m e tal número t é representado por $\mathrm{ord}_a(m)$.*

Observação
O número $t = \mathrm{ord}_a(m)$, referido na definição anterior, existe necessariamente, uma vez que temos $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proposição 27 *Sejam m um inteiro positivo e $a \in \mathbb{Z}$, tais que $\mathrm{mdc}(a, m) = 1$. Seja φ a função de Euler. Então, $\mathrm{ord}_a(m)$ é um divisor de $\varphi(m)$.*

Demonstração
Seja $d = \mathrm{ord}_a(m)$. É claro que $d \leq \varphi(m)$ e $a^d \equiv 1 \pmod{m}$. Dividida-se $\varphi(m)$ por d. Então, existem números inteiros não negativos q e r, tais que $\varphi(m) = dq + r$, com $0 \leq r < d$.
Então, $1 \equiv a^{\varphi(m)} \equiv a^{dq+r} \equiv \left(a^d\right)^q \times a^r \equiv (1)^q \times a^r \equiv a^r \pmod{m}$. Então, $r = 0$, uma vez que $0 \leq r < d$.
Logo, $\mathrm{ord}_a(m)$ é um divisor de $\varphi(m)$.

Definição 28 *Sejam φ a função de Euler, m um número natural e $a \in \mathbb{Z}$, tais que $\mathrm{mdc}(a, m) = 1$. Se $\mathrm{ord}_a(m) = \varphi(m)$, diz-se que a é uma raiz primitiva módulo m, ou que a é uma raiz primitiva de m.*

Proposição 29 *Seja m um número natural e seja ψ a aplicação de $\mathbb{N}$ em $\mathbb{N}_0$, tal que $\psi(n)$ é o número de elementos de $\{1, 2, \ldots, m\}$ que têm ordem n, relativamente ao módulo m. Então, $\sum_{d|\varphi(m)} \psi(d) = \varphi(m)$.*

Demonstração
No conjunto $\{1, 2, \ldots, m\}$ há $\varphi(m)$ elementos primos com a. Cada um desses elementos tem uma ordem que é um divisor de $\varphi(m)$, sendo que cada elemento é "contado"por ψ, uma e uma só vez, quando d percorre os divisores de $\varphi(m)$.
Logo, $\sum_{d|\varphi(m)} \psi(d) = \varphi(m)$.
Note-se que só definimos ordem de um número, relativamente ao módulo m, se esse número for primo com m.

Exemplo 30 *Seja $m = 8$. Os números naturais menores ou iguais a 8 que são primos com 8 são 1, 3, 5 e 7, tendo-se $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$.*

Então $\varphi(8) = 4$, $\psi(1) = 1$, $\psi(2) = 3$ e $\psi(4) = 0$.
Logo, $\psi(1) + \psi(2) + \psi(4) = 1 + 3 + 0 = 4 = \varphi(8)$.
Se $m = 9$, temos que $\varphi(m) = \varphi(9) = 6$, sendo que os divisores de 6 são os números 1, 2, 3 e 6.
Note-se que $2^6 \equiv 4^3 \equiv 5^6 \equiv 7^3 \equiv 8^2 \equiv 1 \pmod{9}$, sendo os expoentes anteriores os expoentes positivos mínimos para se obter um número congruente com 1, módulo 9.
Então, $\psi(1) + \psi(2) + \psi(3) = 1 + 1 + 2 + 2 = 6 = \varphi(9)$.

Corolário 31 *Seja p um número primo. Então, com as notações anteriores, temos:*
$\sum_{d|p-1} \varphi(d) = p - 1$ *e* $\sum_{d|p-1} \psi(d) = p - 1$.

Demonstração

A primeira igualdade resulta imediatamente de $\sum_{d|\varphi(m)} \varphi(d) = m$, substituindo m por p, uma vez que $\varphi(p) = p - 1$.

A segunda igualdade resulta de $\sum_{d|\varphi(m)} \psi(d) = \varphi(m)$, fazendo $m = p$, já que $\varphi(p) = p - 1$.

Proposição 32 *Seja p um número primo. Então, com as notações anteriores, temos $\psi(d) = \varphi(d)$, para qualquer divisor d de $p - 1$.*

Demonstração

Seja d um divisor de $p - 1$, tal que $\psi(d) > 0$. Então, existe um elemento x, primo com p, de ordem d. Vejamos que $x, x^2, \ldots, x^d$ são mutuamente incongruentes, módulo p, e satisfazem a condição $y^d \equiv 1 \pmod{p}$:

Sejam r e s, dois números naturais tais que $1 \leq r \leq s$ e $x^r \equiv x^s \pmod{p}$.

Então, $x^{s-r} \equiv 1 \pmod{p}$, tendo-se $0 \leq s - r \leq d$, pelo que tem de ser $s - r = 0$, uma vez que d é a ordem de x.

Logo, $r = s$, o que prova que os números $x, x^2, \ldots, x^d$ são mutuamente incongruentes, módulo p.

É claro que $(x^r)^d \equiv x^{rd} \equiv \left(x^d\right)^r \equiv 1^r \equiv 1 \pmod{p}$, qualquer que seja o número natural n.

Como p é primo, a congruência $y^d \equiv 1 \pmod{p}$ não pode ter mais do que d soluções mutuamente incongruentes, módulo p. Então, um elemento de ordem d, tem de ser congruente com um dos números $x, x^2, \ldots, x^d$.

Vamos, agora, provar que a ordem de x^r é d, se e só se, r é um número primo com d:

Suponhamos que r é primo com d e que $(x^r)^t \equiv 1 \pmod{p}$. Então, $x^{rt} \equiv 1 \pmod{p}$, pelo que d é um divisor de rt. Mas, como d é primo com r, então d é um divisor de t. Logo, a ordem de x^r é d.

Suponhamos que r não é primo com d. Então, existe um número primo q, tal que q divide r e q divide d. Então, $(x^r)^{\frac{d}{q}} \equiv x^{\frac{rd}{q}} \equiv \left(x^{\frac{r}{q}}\right)^d \equiv 1 \pmod{p}$, pelo que a ordem de x^r não é d.

E agora, podemos afirmar que entre $x, x^2, \ldots, x^d$ há, exactamente, $\varphi(d)$ números que têm ordem d, o que prova que se $\psi(d) > 0$, então $\psi(d) = \varphi(d)$.

E, como $\sum_{d|p-1} \varphi(d) = p - 1$ e $\sum_{d|p-1} \psi(d) = p - 1$, então não pode ser $\psi(d) = 0$, para nenhum divisor d de $p - 1$.

Então, $\psi(d) = \varphi(d)$, para qualquer divisor d de $p - 1$.

Corolário 33 *Seja p um número primo. Então, existe um número inteiro x, tal que x tem ordem $p-1$. Mais precisamente, existem $\varphi(p-1)$ inteiros de ordem $p - 1$ e mutuamente incongruentes, módulo p.*

Demonstração

Da proposição anterior, resulta que $\psi(p-1) = \varphi(p-1) > 0$, o que termina a demonstração.

Lema 34 *Sejam m, n dois inteiros tais que $m > 2$, $n > 2$ e $\text{mdc}(m, n) = 1$. Então, mn não admite raiz primitiva.*

Demonstração

Suponhamos que $m > 2$, $n > 2$ e $\text{mdc}(m, n) = 1$. Então, $\varphi(m)$ e $\varphi(n)$ são pares, pelo que $\text{mmc}(\varphi(m), \varphi(n)) < \varphi(m) \times \varphi(n) = \varphi(mn)$.

Seja $b \in \mathbb{Z}$, tal que $\text{mdc}(mn, b) = 1$. Então:

$$\begin{aligned}
\text{mdc}(mn, b) = 1 &\implies \text{mdc}(m, b) = \text{mdc}(n, b) = 1 \\
&\implies b^{\varphi(m)} \equiv 1 \pmod{m} \wedge b^{\varphi(n)} \equiv 1 \pmod{n} \\
&\implies b^{\text{mmc}(\varphi(m),\varphi(n))} \equiv 1 \pmod{m} \wedge b^{\text{mmc}(\varphi(m),\varphi(n))} \equiv 1 \pmod{n} \\
&\implies b^{\text{mmc}(\varphi(m),\varphi(n))} \equiv 1 \pmod{mn}
\end{aligned}$$

Logo, b não é raiz primitiva de mn. Como b pode ser qualquer número primo com mn, então mn não admite raiz primitiva.

Lema 35 *Seja k um número natural maior que 2 e seja b um número inteiro ímpar. Então, $b^{2^{k-2}} \equiv 1 \pmod{2^k}$.*

Demonstração

A demonstração faz-se por indução em k. Observemos que, se b é ímpar, existe $r \in \mathbb{Z}$, tal que $b = 2r + 1$.

Fazendo $k = 3$, obtemos $b^2 \equiv 1 \pmod 8$ que é uma proposição verdadeira, pois $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod 8$.

Hipótese de indução: $b^{2^{k-2}} \equiv 1 \pmod{2^k}$

Tese: $b^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$. Ora,

$$\begin{aligned} b^{2^{k-2}} \equiv 1 \pmod{2^k} &\implies b^{2^{k-2}} = 1 + a \times 2^k, a \in \mathbb{Z} \\ &\implies \left(b^{2^{k-2}}\right)^2 = \left(1 + a \times 2^k\right)^2, a \in \mathbb{Z} \\ &\implies b^{2^{k-2} \times 2} = 1 + a \times 2^{k+1} + a^2 \times 2^{2k}, a \in \mathbb{Z} \\ &\implies b^{2^{k-1}} = 1 + a \times 2^{k+1} + a^2 \times 2^{k+1} \times 2^{k-1}, a \in \mathbb{Z} \\ &\implies b^{2^{k-1}} \equiv 1 \pmod{2^{k+1}} \end{aligned}$$

Está, assim, terminada a demonstração.

Lema 36 *Seja k um número natural maior que 2. Então, 2^k não admite raiz primitiva.*

Demonstração

Pelo lema anterior, se b é um número ímpar, então $b^{2^{k-2}} \equiv 1 \pmod{2^k}$, pelo que a ordem de b é menor ou igual a 2^{k-2}. Por outro lado, temos $\varphi\left(2^k\right) = 2^{k-1}$. Logo, a ordem de b, relativamente a 2^k, é menor que $\varphi\left(2^k\right)$. Logo, 2^k não admite raiz primitiva. Note-se que nenhum número par é primo com 2^k, com $k \geq 2$.

Lema 37 *Seja $p \in \mathbb{N}$ um número primo ímpar. Então, p admite uma raiz primitiva g, tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$.*

Demonstração

Já vimos que todo o primo p admite uma raiz primitiva h.

Se $h^{p-1} \not\equiv 1 \pmod{p^2}$, então $g = h$.

Se $h^{p-1} \equiv 1 \pmod{p^2}$„ consideramos $g = h + p$, que ainda é raiz primitiva de p. Agora, vamos provar que $(h+p)^{\pi-1} \not\equiv 1 \pmod{p^2}$. Ora,

$$g^{p-1} = (h+p)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} h^{p-1-k} p^k = h^{p-1} + (p-1)\, h^{p-2} p + \sum_{k=2}^{p-1} \binom{p-1}{k} h^{p-1-k} p^k$$

Logo,

$$\begin{aligned} g^{p-1} &\equiv h^{p-1} + (p-1)\, h^{p-2} p + \sum_{k=2}^{p-1} \binom{p-1}{k} h^{p-1-k} p^k \pmod{p^2} \\ &\equiv 1 + (p-1)\, h^{p-2} p \pmod{p^2} \\ &\equiv 1 + p^2 h^{p-2} - p h^{p-2} \pmod{p^2} \\ &\equiv 1 - h^{p-2} p \pmod{p^2} \end{aligned}$$

Então, $g^{p-1} \not\equiv 1 \pmod{p^2}$, pois se $g^{p-1} \equiv 1 \pmod{p^2}$, então p dividia h^{p-2}, donde p dividia h. Mas, então, h não era raiz primitiva de p.

Está, assim terminada a demonstração deste lema.

Lema 38 *Seja $p \in \mathbb{N}$ um número primo ímpar. Seja g uma raiz primitiva de p, tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$. Então, para cada número inteiro k, tal que $k \geq 2$, verifica-se que $g^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$.*

Demonstração

Se $k = 2$, então obtemos $g^{p-1} \not\equiv 1 \pmod{p^2}$ que é a hipótese deste lema (e que está de acordo com o lema anterior).

Hipótese de indução: $g^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$

Tese: $g^{(p-1)p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$

Como $\operatorname{mdc}(g, p) = 1$, uma vez que g é uma raiz primitiva de p, então $\operatorname{mdc}\left(g, p^{k-1}\right) = 1$, para $k \geq 2$.

Como $\varphi\left(p^{k-1}\right) = (p-1)\,p^{k-2}$, então $g^{\varphi\left(p^{k-1}\right)} = g^{(p-1)p^{k-2}} \equiv 1 \pmod{p^{k-1}}$

Logo, existe um inteiro a, tal que $g^{(p-1)p^{k-2}} = 1 + ap^{k-1}$.

Vejamos que $\operatorname{mdc}(a, p) = 1$:

Se fosse $\operatorname{mdc}(a, p) = p$, teríamos $a = a_0 p$, para certo inteiro a_0.

Então, $g^{(p-1)p^{k-2}} = 1 + a_0 p p^{k-1} = 1 + a_0 p^k \equiv 1 \pmod{p^k}$, o que contradiz a hipótese de indução. Logo, $\operatorname{mdc}(a, p) = 1$.

Então:

$$\begin{aligned}
\left(g^{(p-1)p^{k-2}}\right)^p &= \left(1 + ap^{k-1}\right)^p = 1 + ap^{k-1}p + \binom{p}{2} a^2 p^{2k-2} + \cdots \\
&= 1 + ap^k + \frac{p\,(p-1)}{2} a^2 p^{2k-2} + \cdots \\
&= 1 + ap^k + \frac{p-1}{2} a^2 p^{2k-1} + \cdots
\end{aligned}$$

Logo,

$$\left(g^{(p-1)p^{k-2}}\right)^p = g^{(p-1)p^{k-1}} = 1 + ap^k + \frac{p-1}{2} a^2 p^{2k-1} + \cdots$$

Logo, $g^{(p-1)p^{k-1}} \equiv 1 + ap^k \pmod{p^{k+1}} \not\equiv 1 \pmod{p^{k+1}}$, porque, como vimos, $\operatorname{mdc}(a, p) = 1$.

Lema 39 *Seja $p \in \mathbb{N}$ um primo ímpar. Então, para cada natural k, temos que p^k admite raiz primitiva.*

Demonstração

Seja g uma raiz primitiva de p, tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$. Vejamos que g é raiz primitiva de p^k, para qualquer numero natural k.

Para $k = 1$, temos que g é uma raiz primitiva de p.

Suponhamos que $k \geq 2$. Então, temos $\varphi\left(p^k\right) = (p-1)\,p^{k-1}$.

Seja t a ordem de g, relativamente ao módulo p^k. Então, $g^t \equiv 1 \pmod{p^k}$ e t é um divisor de $(p-1)\,p^{k-1}$. Logo, existe um inteiro z, tal que $tz = (p-1)\,p^{k-1}$.

Por outro lado, de $g^t \equiv 1 \pmod{p^k}$, vem $g^t \equiv 1 \pmod{p}$, pelo que t é um múltiplo da ordem de g, relativamente ao módulo p. Mas, como g é raiz primitiva de p, temos que t é um múltiplo de $p-1$. Logo, existe um inteiro r, tal que $t = r\,(p-1)$.

Então, $tz = (p-1)\,p^{k-1}$ e $t = r\,(p-1)$. Então, $zr\,(p-1) = (p-1)\,p^{k-1}$, pelo que $zr = p^{k-1}$.

Então, r é uma potência de p, isto é, $r = p^\alpha$, com $0 \leq \alpha \leq k-1$.

Então, $t = (p-1)\,p^\alpha$, com $0 \leq \alpha \leq k-1$.

Suponhamos que $0 \leq \alpha \leq k-2$. Então, $g^{(p-1)p^{k-2}} \equiv 1 \left(\mathrm{mod}\, p^k\right)$, porque $(p-1)\,p^{k-2}$ é um múltiplo de t.

Mas este resultado contradiz o lema anterior. Então, é absurdo supor que $t = (p-1)\,p^{\alpha}$, com $0 \leq \alpha \leq k-2$. Então, $t = (p-1)\,p^{k-1}$.

Logo, g é raiz primitiva de p^k, para qualquer número natural k.

Lema 40 *Seja p um primo ímpar. Então, para cada natural k, temos que $2p^k$ admite raiz primitiva.*

Demonstração

Seja g uma raiz primitiva de p. Se g é par, temos que $g+p$ é uma raiz primitiva ímpar de p. Logo, podemos supor, sem perda de generalidade, que g é uma raiz primitiva ímpar de p.

Mas se $g^s \equiv 1 \left(\mathrm{mod}\, 2p^k\right)$, então $g^s \equiv 1 \left(\mathrm{mod}\, p^k\right)$.

E, reciprocamente, se $g^s \equiv 1 \left(\mathrm{mod}\, p^k\right)$, com g ímpar, então $g^s \equiv 1 \left(\mathrm{mod}\, 2\right)$, pelo que $g^s \equiv 1 \left(\mathrm{mod}\, 2p^k\right)$.

Logo, se g é ímpar, então $g^s \equiv 1 \left(\mathrm{mod}\, p^k\right)$ se e só se $g^s \equiv 1 \left(\mathrm{mod}\, 2p^k\right)$.

Então, com g ímpar, a ordem de g é a mesma para os módulos p^k e $2p^k$.

Como $\varphi\left(p^k\right) = \varphi\left(p^k\right)$ e g é raiz primitiva (ímpar) de p^k, então g é raiz primitiva de $2p^k$.

Proposição 41 *Teorema das raízes primitivas*

Os números naturais que admitem raízes primitivas são 1, 2, 4, p^k e $2p^k$, com $k \in \mathbb{N}$ e p um primo ímpar.

Demonstração

É fácil verificar que, por exemplo, 3 é raiz primitiva de 1, 2 e 4.

Os números da forma p^k e $2p^k$ (com $k \in \mathbb{N}$ e p um primo ímpar) admitem raiz primitiva, como acabámos de provar.

Os restantes números, ou são uma potência de 2 maior que 4 e, como já provámos, não admitem raiz primitiva, ou podem decompor-se num produto de dois números primos entre si e maiores que 2 e, por isso, também, não admitem raiz primitiva.

1.2 Congruências Quadráticas

Definição 42 *Sejam $p \in \mathbb{N}$ e $a \in \mathbb{Z}$, tais que $\mathrm{mdc}\,(a,p) = 1$ e p é primo ímpar. Dizemos que a é resíduo quadrático, módulo p, se existir $x \in \mathbb{Z}$, tal que $x^2 \equiv a \left(\mathrm{mod}\, p\right)$. Dizemos que a é resíduo não quadrático, módulo p, se não existir $x \in \mathbb{Z}$, tal que $x^2 \equiv a \left(\mathrm{mod}\, p\right)$. Se $\mathrm{mdc}\,(a,p) = p$, então a não é resíduo quadrático, nem é resíduo não quadrático, módulo p. Daqui em diante, representaremos o conjunto dos números primos por $\mathbb{P}$.*

Definição 43 *Sejam $a \in \mathbb{Z}$ e p um primo ímpar. O símbolo de Legendre $\left(\frac{a}{p}\right)$ define-se do seguinte modo:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \Longleftarrow \quad p \text{ divide } a \\ 1 & \Longleftarrow \quad a \text{ é resíduo quadrático, módulo } p \\ -1 & \Longleftarrow \quad a \text{ é resíduo não quadrático, módulo } p \end{cases}$$

Definição 44 *Sejam $p_1, \ldots, p_k$ primos ímpares não necessariamente distintos e $a \in \mathbb{Z}$. O símbolo de Jacobi $\left(\frac{a}{p_1 \ldots p_k}\right)$ é definido por $\left(\frac{a}{p_1}\right) \times \cdots \times \left(\frac{a}{p_k}\right)$, isto é, o símbolo de Jacobi é um produto de símbolos de Legendre.*

Proposição 45 *Sejam $p \in \mathbb{P}$ e $a \in \mathbb{Z}$, tais que $\mathrm{mdc}\,(a,p) = 1$ e p é ímpar. Então, são válidas as seguintes propriedades:*

Se a é resíduo quadrático, módulo p, então $a^{\frac{p-1}{2}} \equiv 1 \left(\mathrm{mod}\, p\right)$.

Se a é resíduo não quadrático, módulo p, então $a^{\frac{p-1}{2}} \equiv -1 \left(\mathrm{mod}\, p\right)$.

Demonstração

Suponhamos que a é resíduo quadrático módulo p. Então existe $x \in \mathbb{Z}$, tal que $x^2 \equiv a \pmod{p}$.

Então $a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$, porque $\operatorname{mdc}(x,p) = 1$.

Suponhamos, agora, que a é resíduo não quadrático módulo p.

Então, pelo Teorema de Wilson, temos $(p-1)! \equiv -1 \pmod{p}$.

Logo, $1 \times 2 \times \cdots \times (p-1) \equiv -1 \pmod{p}$.

Como p é ímpar, o número de factores do produto anterior é par, pelo que podemos associá-los dois a dois, da seguinte maneira:

Seja $i \in \{1, 2, \ldots, p-1\}$. Como a congruência $iX \equiv a \pmod{p}$ tem solução não congruente com zero, então, existe $j \in \{1, 2, \ldots, p-1\}$, tal que $ij \equiv a \pmod{p}$. Se fosse $i = j$, teríamos $i^2 \equiv a \pmod{p}$, o que contradiz a hipótese de que a é resíduo não quadrático módulo p. Logo $i \neq j$.

Então, no produto $1 \times 2 \times \cdots \times (p-1)$, associamos i com j.

Se $p \geq 5$, ainda há outros factores para associar.

Seja $i_1 \in \{1, 2, \ldots, p-1\}$, com $i_1 \neq i$ e $i_1 \neq j$. Então existe $j_1 \{1, 2, \ldots, p-1\}$ tal que $j_1 \neq i_1$ e $i_1 j_1 \equiv a \pmod{p}$.

Além disso, $j_1 \neq i$ e $j_1 \neq j$, pois se, por exemplo, fosse $j_1 = i$, teríamos $ij \equiv a \pmod{p}$ e $i_1 j_1 = i i_1 \equiv a \pmod{p}$, donde se concluía que $i i_1 \equiv ij \pmod{p}$, pelo que $i_1 \equiv j \pmod{p}$. Então, seria $i_1 = j$, contra a hipótese $i_1 \neq j$.

Analogamente se mostrava que $j_1 \neq j$.

Então, no produto $1 \times 2 \times \cdots \times (p-1)$, associamos i_1 com j_1.

A repetição deste raciocínio mostra-nos que os factores de $1 \times 2 \times \cdots \times (p-1)$ podem ser associados aos pares, de modo que o produto de cada dois factores seja congruente com a, módulo p.

Logo, $a^{\frac{p-1}{2}} \equiv 1 \times 2 \times \cdots \times (p-1) \equiv -1 \pmod{p}$.

Desta proposição resultam imediatamente os seguintes corolários:

Corolário 46 *Sejam $p \in \mathbb{P}$ e $a \in \mathbb{Z}$, tais que $\operatorname{mdc}(a,p) = 1$ e p é ímpar. Então, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Corolário 47 *Sejam $p \in \mathbb{P}$ e $a \in \mathbb{Z}$, tais que $\operatorname{mdc}(a,p) = 1$ e p é ímpar. São válidas as seguintes propriedades:*

1. *Se $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, então a é um resíduo não quadrático, módulo p.*
2. *Se $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, então a é um resíduo quadrático, módulo p.*

Exemplo 48 *Consideremos $a = 7$, $b = 13$ e $p = 17$.*

Ora, $7^2 = 49 \equiv 15 \equiv -2 \pmod{17}$, pelo que $7^8 \equiv (-2)^4 \equiv 16 \equiv -1 \pmod{17}$. Então, 7 é um resíduo não quadrático, módulo p.

Por outro lado, $13^8 \equiv (-4)^8 \equiv 4^8 - 2 \pmod{17}$

Proposição 49 *Seja p um número primo ímpar. Então:*

1. *O produto de dois resíduos quadráticos, módulo p é um resíduo quadrático, módulo p.*
2. *O produto de dois resíduos não quadráticos, módulo p é um resíduo quadrático, módulo p.*
3. *O produto de um resíduo quadrático, módulo p, por um resíduo não quadrático, módulo p, é um resíduo não quadrático, módulo p.*

Demonstração

1. Sejam $a, b \in \mathbb{Z}$, dois resíduos quadráticos, módulo p. Então, $a^{\frac{p-1}{2}} \equiv 1 \equiv b^{\frac{p-1}{2}} \pmod{p}$.
   Logo:
   $$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \times b^{\frac{p-1}{2}} \equiv 1 \times 1 \equiv 1 \pmod{p}$$
   Logo, ab é um resíduo quadrático, módulo p.

2. Sejam $a, b \in \mathbb{Z}$, dois resíduos não quadráticos, módulo p. Então:
   $$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \times b^{\frac{p-1}{2}} \equiv (-1) \times (-1) \equiv 1 \pmod{p}$$
   Logo, ab é um resíduo quadrático, módulo p.

3. Sejam $a, b \in \mathbb{Z}$, tais que a é um resíduo quadrático, módulo p, e b é um resíduo não quadrático, módulo p.
   Então,$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \times b^{\frac{p-1}{2}} \equiv 1 \times (-1) \equiv -1 \pmod{p}$
   Logo, ab é um resíduo não quadrático, módulo p.

Corolário 50 *Seja p um primo ímpar e sejam $a, b \in \mathbb{Z}$. Então o símbolo de Legendre $\left(\frac{ab}{p}\right)$ é dado por $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)$.*

Demonstração
Se $a \equiv 0 \vee b \equiv 0 \pmod{p}$, então $ab \equiv 0 \pmod{p}$ e $\left(\frac{ab}{p}\right) = 0 = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)$.
Se $ab \not\equiv 0 \pmod{p}$, então $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)$ é uma consequência imediata da proposição anterior.

Corolário 51 *Seja p um número primo. O número inteiro -1 é resíduo quadrático, módulo p, se e só se, $p = 2$ ou $p \equiv 1 \pmod{4}$.*

Demonstração

1. Suponhamos que $p = 2$. Então, $1^2 \equiv -1 \pmod{2}$, donde -1 é um resíduo quadrático, módulo 2.

2. Se $p \equiv 1 \pmod{4}$, então $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \equiv 1 \pmod{p}$, uma vez que $\frac{p-1}{2}$ é um número par.
   Então, -1 é um resíduo quadrático, módulo p.

3. Se $p \equiv 3 \pmod{4}$, então $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \equiv -1 \pmod{p}$, uma vez que $\frac{p-1}{2}$ é um número ímpar.
   Então, -1 é um resíduo não quadrático, módulo p.

Proposição 52 *Sejam $p_1, \ldots, p_k$ primos ímpares não necessariamente distintos e seja $a \in \mathbb{Z}$. Se o símbolo de Jacobi de a, relativamente ao produto $p_1 \ldots p_k$ é -1, isto é, se tivermos $\left(\frac{a}{p_1 \ldots p_k}\right) = -1$, então não existe nenhum inteiro x, tal que $x^2 \equiv a \pmod{p_1 \ldots p_k}$.*

Se o símbolo de Jacobi de a, relativamente ao produto $p_1 \ldots p_k$ é 1, então nada se pode concluir sobre a existência dum inteiro x, tal que $x^2 \equiv a \pmod{p_1 \ldots p_k}$.
Demonstração
Se $\left(\frac{a}{p_1 \ldots p_k}\right) = -1$, então existe $j \in \{1, 2, \ldots, k\}$, tal que $\left(\frac{a}{p_j}\right) = -1$.

Logo não existe nenhum inteiro x, tal que $x^2 \equiv a \pmod{p_j}$, pelo que também não existe nenhum inteiro x, tal que $x^2 \equiv a \pmod{p_1 \dots p_k}$.

Quanto à segunda parte da proposição, basta-nos verificar que $\left(\frac{2}{3\times 5}\right) = \left(\frac{2}{3}\right) \times \left(\frac{2}{5}\right) = (-1)\times(-1) = 1$ e não existe nenhum inteiro x, tal que $x^2 \equiv 2 \pmod{15}$, enquanto que, por outro lado, $\left(\frac{4}{3\times 5}\right) = \left(\frac{4}{3}\right) \times \left(\frac{4}{5}\right) = 1 \times 1 = 1$ e existe um inteiro x, tal que $x^2 \equiv 4 \pmod{15}$, uma vez que $2^2 \equiv 4 \pmod{15}$.

Dito de outra forma, se um produto de dois ou mais números inteiros é 1, não podemos concluir que todos os inteiros sejam iguais a 1.

Proposição 53 *São válidas as seguintes propriedades do símbolo de Jacobi:*

1. *Sejam $a, b, c \in \mathbb{Z}$, com c ímpar e $c > 1$. Então $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right) \times \left(\frac{b}{c}\right)$.*
2. *Sejam $a, b, c \in \mathbb{Z}$, com b, c ímpares, $b > 1$ e $c > 1$. Então $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right) \times \left(\frac{a}{c}\right)$.*

Demonstração

1. Se c é primo, o resultado é imediato.

   Se c é ímpar e não é primo, então c é um produto de primos ímpares, digamos $c = p_1 \dots p_r$, com $r \geq 2$. Então:

$$\begin{aligned}
\left(\frac{ab}{c}\right) &= \left(\frac{ab}{p_1 \cdots p_r}\right) = \left(\frac{ab}{p_1}\right) \times \cdots \times \left(\frac{ab}{p_r}\right) \\
&= \left(\frac{a}{p_1}\right) \times \left(\frac{b}{p_1}\right) \times \cdots \times \left(\frac{a}{p_r}\right) \times \left(\frac{b}{p_r}\right) \\
&= \left(\frac{a}{p_1}\right) \times \cdots \times \left(\frac{a}{p_r}\right) \times \left(\frac{b}{p_1}\right) \times \cdots \times \left(\frac{b}{p_r}\right) \\
&= \left(\frac{a}{p_1 \cdots p_r}\right) \times \left(\frac{b}{p_1 \cdots p_r}\right) \\
&= \left(\frac{a}{c}\right) \times \left(\frac{b}{c}\right)
\end{aligned}$$

2. Suponhamos que $b = q_1 \dots q_t$ e $c = p_1 \dots p_r$, com $t \geq 1$, $r \geq 1$ e $q_1, \dots, q_t, p_1, \dots, p_r$ primos ímpares. Então:

$$\begin{aligned}
\left(\frac{a}{bc}\right) &= \left(\frac{a}{q_1 \cdots q_t \times p_1 \cdots p_r}\right) = \left(\frac{a}{q_1}\right) \times \cdots \times \left(\frac{a}{q_t}\right) \times \left(\frac{a}{p_1}\right) \times \cdots \times \left(\frac{a}{p_r}\right) \\
&= \left(\frac{a}{q_1 \cdots q_t}\right) \times \left(\frac{a}{p_1 \cdots p_r}\right) = \left(\frac{a}{b}\right) \times \left(\frac{a}{c}\right)
\end{aligned}$$

Está, assim, terminada a demonstração.

Proposição 54 *Lema de Gauss*

Sejam p um primo ímpar e $b \in \mathbb{Z}$, tal que $\operatorname{mdc}(b, p) = 1$. Consideremos os conjuntos $S = \left\{b, 2b, \dots, \frac{p-1}{2}b\right\}$ e $S' = \left\{R_1, \dots, R_n, r_1, \dots, r_{\frac{p-1}{2}-n}\right\}$ tais que $S' \subseteq \{1, 2, \dots, p-1\}$ e em que cada elemento de S' é congruente, módulo p, com um elemento de S, sendo $R_1, \dots, R_n > \frac{p}{2}$ e $r_1, \dots, r_{\frac{p-1}{2}-n} < \frac{p}{2}$. Então, $\left(\frac{b}{p}\right) = (-1)^n$.

Demonstração

Seja $S_1 = \left\{p - R_1, \ldots, p - R_n, r_1, \ldots, r_{\frac{p-1}{2}-n}\right\}$.

Todos os elementos de S_1 são inteiros positivos menores que $\frac{p}{2}$.

Como $\text{mdc}\,(b,p) = 1$, temos que os elementos de S são incongruentes, módulo p, o mesmo acontecendo com os elementos de S'.

Logo, os números $p - R_1, \ldots, p - R_n$ são incongruentes, módulo p, o mesmo acontecendo com os números $r_1, \ldots, r_{\frac{p-1}{2}-n}$.

Suponhamos que $p - R_i \equiv r_j$, para certos inteiros i, j tais que $1 \leq i \leq n$ e $1 \leq j \leq \frac{p-1}{2} - n$.

Então, $R_i + r_j \equiv 0\,(\text{mod}\,p)$, pelo que existiam inteiros k, l tais que $1 \leq k \leq \frac{p-1}{2}$, $1 \leq l \leq \frac{p-1}{2}$ e $kb + lb \equiv 0\,(\text{mod}\,p)$. Então, $(k+l)\,b \equiv 0\,(\text{mod}\,p)$, donde vem $k + l \equiv 0\,(\text{mod}\,p)$, o que é impossível, pois temos $2 \leq k + l \leq p - 1$.

Então, os elementos de S' são mutuamente incongruentes, módulo p. Então, em S_1, há $\frac{p-1}{2}$ elementos distintos pertencentes ao conjunto $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, pelo que $S_1 = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.

Logo,

$$\begin{aligned} R_1 \times \cdots \times R_n \times r_1, \cdots \times r_{\frac{p-1}{2}-n} &\equiv b \times 2b \times \cdots \times \frac{p-1}{2} b\,(\text{mod}\,p) \\ &\equiv b^{\frac{p-1}{2}} \times \left(\frac{p-1}{2}\right)!\,(\text{mod}\,p) \end{aligned}$$

Por outro lado, temos

$$\begin{aligned} R_1 \times \cdots \times R_n \times r_1, \cdots \times r_{\frac{p-1}{2}-n} &\equiv (-1)^n \prod_{i=1}^{n} (p - R_i) \times \prod_{j=1}^{\frac{p-1}{2}-n} r_j\,(\text{mod}\,p) \\ &\equiv (-1)^n \times \left(\frac{p-1}{2}\right)!\,(\text{mod}\,p) \end{aligned}$$

Das condições anteriores vem que $b^{\frac{p-1}{2}} \times \left(\frac{p-1}{2}\right)! \equiv (-1)^n \times \left(\frac{p-1}{2}\right)!\,(\text{mod}\,p)$.

Então, $b^{\frac{p-1}{2}} \equiv (-1)^n\,(\text{mod}\,p)$. Mas, $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right)\,(\text{mod}\,p)$.

Então, $\left(\frac{b}{p}\right) \equiv (-1)^n\,(\text{mod}\,p)$. Logo, $\left(\frac{b}{p}\right) = (-1)^n$, porque p é um primo ímpar.

Note-se que, para $p = 2$, a conclusão anterior não seria válida.

Proposição 55 *Sejam p um primo ímpar e $b \in \mathbb{Z}$ tais que* $\text{mdc}\,(b, 2p) = 1$. *Então $\left(\frac{b}{p}\right) = (-1)^t$, com $t = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kb}{p} \rfloor$, lembrando-se que $\lfloor x \rfloor$ representa o maior inteiro não superior a x.*

Demonstração

Seja $k \in \mathbb{N}$, tal que $1 \leq k \leq \frac{p-1}{2}$. Efectuando a divisão inteira de kb por p, obtemos $kb = pq_k + r'_k$, com $1 \leq r'_k \leq p - 1$ e $q_k = \lfloor \frac{kb}{p} \rfloor$. Seja $S' = \left\{r'_k : 1 \leq k \leq \frac{p-1}{2}\right\}$.

Suponhamos que $r'_i = r'_j$, para certos inteiros i, j com $i, j \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Então:

$$\begin{aligned} r'_i = r'_j &\implies ib - pq_i = jb - pq_j \implies ib \equiv jb\,(\text{mod}\,p) \\ &\implies i \equiv j\,(\text{mod}\,p) \implies i = j \end{aligned}$$

Então, os elementos de S' são todos distintos.

Ora, os elementos de S' dividem-se em dois grupos: uns são maiores que $\frac{p}{2}$, enquanto outros são menores que $\frac{p}{2}$.

De modo análogo à demonstração da proposição anterior, temos $S' = \left\{R_1, \ldots, R_n, r_1, \ldots, r_{\frac{p-1}{2}-n}\right\}$, com $R_1, \ldots, R_n > \frac{p}{2}$ e $r_1, \ldots, r_{\frac{p-1}{2}-n} < \frac{p}{2}$ e $S_1 = \left\{p - R_1, \ldots, p - R_n, r_1, \ldots, r_{\frac{p-1}{2}-n}\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Então:

$$\begin{aligned}
b\sum_{k=1}^{\frac{p-1}{2}} k &= \sum_{k=1}^{\frac{p-1}{2}} bk = \sum_{k=1}^{\frac{p-1}{2}} \left(pq_k + r'_k\right) = \sum_{k=1}^{\frac{p-1}{2}} pq_k + \sum_{k=1}^{\frac{p-1}{2}} r'_k \\
&= p\sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{i=1}^{n} R_i + \sum_{j=1}^{\frac{p-1}{2}-n} r_j = p\sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{i=1}^{n} (2R_i - p + p - R_i) + \sum_{j=1}^{\frac{p-1}{2}-n} r_j \\
&= p\sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{i=1}^{n} (2R_i - p) + \left(\sum_{i=1}^{n} (p - R_i) + \sum_{j=1}^{\frac{p-1}{2}-n} r_j\right) \\
&= p\sum_{k=1}^{\frac{p-1}{2}} q_k + 2\sum_{i=1}^{n} R_i - \sum_{i=1}^{n} p + \sum_{k=1}^{\frac{p-1}{2}} k
\end{aligned}$$

Então, $(b-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\sum_{k=1}^{\frac{p-1}{2}} q_k + 2\sum_{i=1}^{n} R_i - \sum_{i=1}^{n} p$, donde vem $(b-1)\,\frac{p^2-1}{8} = p\sum_{k=1}^{\frac{p-1}{2}} q_k + 2\sum_{i=1}^{n} R_i - np$.

Como $b-1$ é par, o primeiro membro é par.

Então, $\sum_{k=1}^{\frac{p-1}{2}} q_k - n \equiv 0 \pmod 2$, donde vem $n \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k \pmod 2$.

Mas, como demonstrado na proposição anterior, temos $\left(\frac{b}{p}\right) = (-1)^n$.

Então, $\left(\frac{b}{p}\right) = (-1)^n = (-1)^t$, com $t = \sum_{k=1}^{\frac{p-1}{2}} q_k = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kb}{p} \rfloor$.

Proposição 56 *Lei da reciprocidade quadrática de Gauss*

Sejam p e q dois primos ímpares distintos. Então $\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$.

Demonstração

Seja $T = \left\{(x, y) \in \mathbb{N}^2 \colon 1 \leq x \leq \frac{p-1}{2} \wedge 1 \leq y \leq \frac{q-1}{2}\right\}$.

Então, temos $T \subset \left[1, \frac{p-1}{2}\right] \times \left[1, \frac{q-1}{2}\right]$, havendo, em T, $\frac{p-1}{2} \times \frac{q-1}{2}$ elementos, isto é, $|T| = \frac{p-1}{2} \times \frac{q-1}{2}$.

Sejam $T_1 = \left\{(x, y) \in T \colon y \leq \frac{q}{p}x\right\}$ e $T_2 = \left\{(x, y) \in T \colon x \leq \frac{p}{q}y\right\}$.

Então $T = T_1 \cup T_2$ e, como p e q são primos distintos, T_1 e T_2 são disjuntos.

Consideremos o conjunto T_1. Se fixarmos x, com $1 \leq x \leq \frac{p-1}{2}$, temos que o número de valores de y, de modo que $(x, y) \in T$, é $\lfloor \frac{qx}{p} \rfloor$.

Então, $|T_1| = \sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$ e, analogamente, $|T_2| = \sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$.

Logo,

$$\begin{aligned} |T| = |T_1| + |T_2| \quad &\Longrightarrow \quad \frac{p-1}{2} \times \frac{q-1}{2} = \sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor + \sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor \\ &\Longrightarrow \quad (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} = (-1)^{|T_1|} \times (-1)^{|T_2|} \\ &\Longrightarrow \quad (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} = \left(\frac{q}{p}\right) \times \left(\frac{p}{q}\right) = \left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) \end{aligned}$$

Observe-se que, conforme verificámos na proposição anterior, temos $(-1)^{|T_1|} = \left(\frac{q}{p}\right)$ e $(-1)^{|T_2|} = \left(\frac{p}{q}\right)$.

Corolário 57 *Sejam p e q dois números primos ímpares distintos. Então, são válidas as seguintes propriedades:*

1. *Se $p \equiv q \equiv 3 \pmod 4$, então $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.*
2. *Se $p \equiv 1 \pmod 4$ ou $q \equiv 1 \pmod 4$, então $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.*

Demonstração

1. Se $p \equiv q \equiv 3 \pmod 4$, então existem números inteiros r e s tais que $p = 4r + 3$ e $q = 4s + 3$.
   Então, $\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} = (-1)^{\frac{4r+3-1}{2} \times \frac{4s+3-1}{2}} = (-1)^{(2r+1)(2s+1)} = -1$.
   Logo, $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.
2. Se $p \equiv 1 \pmod 4$ ou $q \equiv 1 \pmod 4$, então $\frac{p-1}{2} \times \frac{q-1}{2}$ é um número par, pelo que $\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = 1$.
   Logo, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

Proposição 58 *Seja p um número primo ímpar. Então, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

Demonstração

1. Se $p = 4t+1$, para certo inteiro t, de acordo com o lema de Gauss, temos $S = S' = \{2, 4, \ldots, p-1\}$, pelo que há, em S', t elementos maiores que $\frac{p}{2}$. Logo, $\left(\frac{2}{p}\right) = (-1)^t$.
   Mas, $\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(4t+2)(4t)}{8} = (2t+1)\,t$.
   Então, $(-1)^{\frac{p^2-1}{8}} = (-1)^{(2t+1)t} = (-1)^{2t^2} \times (-1)^t = (-1)^t = \left(\frac{2}{p}\right)$.
2. Se $p = 4t + 3$, com t inteiro, temos $S = S' = \{2, 4, \ldots, p-1\} = \{2, 4, \ldots, 4t+2\}$, pelo que há, em S', $t+1$ elementos maiores que $\frac{p}{2}$. Logo, pelo lema de Gauss, $\left(\frac{2}{p}\right) = (-1)^{t+1}$.
   Mas, $\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(4t+4)(4t+2)}{8} = (2t+1)\,(t+1)$.
   Então, $(-1)^{\frac{p^2-1}{8}} = (-1)^{(2t+1)(t+1)} = (-1)^{2t^2} \times (-1)^{t+1} = (-1)^{t+1} = \left(\frac{2}{p}\right)$.

Proposição 59 *Seja b um número natural ímpar maior que 1. Então $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.*

Demonstração
Comecemos por provar que, se m e n são inteiros ímpares, então $\frac{m^2-1}{8}+\frac{n^2-1}{8}\equiv\frac{m^2n^2-1}{8}\,(\mathrm{mod}\,2)$.
Se m e n são números inteiros ímpares, então $m=2x+1$ e $n=2y+1$, para certos inteiros x e y.
Então, $\frac{m^2-1}{8}=\frac{(2x+1)^2-1}{8}=\frac{4x^2+4x}{8}=\frac{x^2+x}{2}\in\mathbb{Z}$. Analogamente, $\frac{n^2-1}{8}\in\mathbb{Z}$.
Se m e n são ímpares, então, $m^2\equiv 1\,(\mathrm{mod}\,8)$ e $n^2\equiv 1\,(\mathrm{mod}\,8)$.
Ora,

$$\begin{aligned}
m^2\equiv 1\,(\mathrm{mod}\,8)\wedge n^2\equiv 1\,(\mathrm{mod}\,8) &\implies m^2-1\equiv 0\,(\mathrm{mod}\,8)\wedge n^2-1\equiv 0\,(\mathrm{mod}\,8)\\
&\implies \left(m^2-1\right)\left(n^2-1\right)\equiv 0\,(\mathrm{mod}\,64)\\
&\implies m^2n^2-m^2-n^2+1\equiv 0\,(\mathrm{mod}\,64)\\
&\implies m^2n^2-1\equiv m^2+n^2-2\,(\mathrm{mod}\,64)\\
&\implies \frac{m^2n^2-1}{8}\equiv\frac{m^2-1}{8}+\frac{n^2-1}{8}\,(\mathrm{mod}\,8)\\
&\implies \frac{m^2n^2-1}{8}\equiv\frac{m^2-1}{8}+\frac{n^2-1}{8}\,(\mathrm{mod}\,2)
\end{aligned}$$

Passemos, agora, à demonstração propriamente dita:
1^o caso: Suponhamos que b é primo, digamos $b=p$.
Então, pela proposição anterior, $\left(\frac{2}{b}\right)=(-1)^{\frac{b^2-1}{8}}$.
2^o caso: Suponhamos que b é um produto de dois primos, digamos $b=pq$. Então,

$$\begin{aligned}
\left(\frac{2}{b}\right) &= \left(\frac{2}{pq}\right)=\left(\frac{2}{p}\right)\times\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}\times(-1)^{\frac{q^2-1}{8}}\\
&= (-1)^{\frac{p^2-1}{8}+\frac{q^2-1}{8}}=(-1)^{\frac{p^2q^2-1}{8}}=(-1)^{\frac{b^2-1}{8}}
\end{aligned}$$

E agora, por indução no número de primos em que se decompõe b, é fácil provar o resultado pretendido.

Exemplo 60 *Cálculo do símbolo de Legendre:*

$$\begin{aligned}
\left(\frac{-1890}{101}\right) &= \left(\frac{29}{101}\right)=\left(\frac{101}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2\times 7}{29}\right)=\left(\frac{2}{29}\right)\times\left(\frac{7}{29}\right)\\
&= (-1)^{\frac{29^2-1}{8}}\times\left(\frac{29}{7}\right)=(-1)^{\frac{30\times 28}{8}}\times\left(\frac{1}{7}\right)\\
&= (-1)^{15\times 7}\times 1=-1
\end{aligned}$$

Observações:

1. $-1890\equiv 29\,(\mathrm{mod}\,101)$, pelo que $\left(\frac{-1890}{101}\right)=\left(\frac{29}{101}\right)$
2. $29\equiv 1\,(\mathrm{mod}\,4)$, pelo que $\left(\frac{29}{101}\right)=\left(\frac{101}{29}\right)$
3. $101\equiv 14\,(\mathrm{mod}\,29)$
4. $29\equiv 1\,(\mathrm{mod}\,4)$, pelo que $\left(\frac{7}{29}\right)=\left(\frac{29}{7}\right)$

Outra maneira

$$\begin{aligned}
\left(\frac{-1890}{101}\right) &= \left(\frac{-1\times 2\times 3^3\times 5\times 7}{101}\right) = \left(\frac{-1}{101}\right)\times\left(\frac{2}{101}\right)\times\left(\frac{3^3}{101}\right)\times\left(\frac{5}{101}\right)\times\left(\frac{7}{101}\right)\\
&= (-1)^{50}\times(-1)^{101^1-1}\times\left(\frac{3}{101}\right)\times\left(\frac{5}{101}\right)\times\left(\frac{7}{101}\right)\\
&= (-1)^{\frac{102\times 100}{8}}\times\left(\frac{101}{3}\right)\times\left(\frac{101}{5}\right)\times\left(\frac{101}{7}\right)\\
&= (-1)^{51\times 25}\times\left(\frac{2}{3}\right)\times\left(\frac{1}{5}\right)\times\left(\frac{3}{7}\right)\\
&= -1\times(-1)^{\frac{3^2-1}{8}}\times 1\times(-1)\times\left(\frac{7}{3}\right)\\
&= -1\times\left(\frac{1}{3}\right) = -1
\end{aligned}$$

Proposição 61 *Sejam n um número natural e q um primo tal que $q\equiv 3\,(\mathrm{mod}\,4)$. Se q divide n, então não existem inteiros x e y, tais que $\mathrm{mdc}\,(x,y)=1$ e $n=x^2+y^2$. Em particular, se n é um número natural tal que $n\equiv 3\,(\mathrm{mod}\,4)$, então n não pode ser escrito como soma de dois quadrados.*

Demonstração

Suponhamos que $\mathrm{mdc}\,(x,y)=1$. Suponhamos, com vista a um absurdo, que $n=x^2+y^2$, para certos inteiros x e y.

Como q divide n, teríamos $x^2+y^2\equiv 0\,(\mathrm{mod}\,q)$.

Se q dividisse x, então q dividia y e reciprocamente, pelo que q dividia $\mathrm{mdc}\,(x,y)$, o que é absurdo, pois $\mathrm{mdc}\,(x,y)=1$.

Então q não divide x nem q divide y.

Então, pelo Teorema de Fermat, temos $x^{q-1}\equiv 1\,(\mathrm{mod}\,q)$.

Mas:

$$\begin{aligned}
x^{q-1}\equiv 1\,(\mathrm{mod}\,q) &\implies yx^{q-1}\equiv y\,(\mathrm{mod}\,q)\\
&\implies xyx^{q-2}\equiv y\,(\mathrm{mod}\,q)\\
&\implies x^2y^2x^{2q-4}\equiv y^2\,(\mathrm{mod}\,q)\\
&\implies x^2+x^2y^2x^{2q-4}\equiv x^2+y^2\,(\mathrm{mod}\,q)\\
&\implies x^2\left(1+y^2x^{2q-4}\right)\equiv 0\,(\mathrm{mod}\,q)\\
&\implies 1+y^2x^{2q-4}\equiv 0\,(\mathrm{mod}\,q)\\
&\implies 1+\left(yx^{q-2}\right)^2\equiv 0\,(\mathrm{mod}\,q)
\end{aligned}$$

Ora, $1+\left(yx^{q-2}\right)^2\equiv 0\,(\mathrm{mod}\,q)$ é falso, porque a congruência $1+z^2\equiv 0\,(\mathrm{mod}\,q)$ é impossível, quando $q\equiv 3\,(\mathrm{mod}\,4)$.

Então é absurdo supor que existem inteiros x e y tais que $\mathrm{mdc}\,(x,y)=1$ e $n=x^2+y^2$.

Se $n\equiv 3\,(\mathrm{mod}\,4)$ e $n=x^2+y^2$, então $n=(2a)^2+(2b+1)^2$, com $a,b\in\mathbb{Z}$.

Logo, $n=4a^2+4b^2+4b+1\equiv 1\,(\mathrm{mod}\,q)$. Então, não podemos ter $n\equiv 3\,(\mathrm{mod}\,4)$ e $n=x^2+y^2$.

Logo, se $n\equiv 3\,(\mathrm{mod}\,4)$, então n não é soma de dois quadrados.

Está, portanto, terminada a demonstração.

Proposição 62 *Sejam $q\in\mathbb{N}$ um primo tal que $q\equiv 3\,(\mathrm{mod}\,4)$ e n um número natural. Então, q^{2n-1} não é soma de dois quadrados.*

Demonstração
Ora, $q^{2n-1} \equiv 3^{2n-1} \equiv (-1)^{2n-1} \equiv -1 \equiv 3 \pmod 4$.
Logo, pela proposição anterior, n não é soma de dois quadrados.

Proposição 63 *Seja q um número primo tal que $q \equiv 3 \pmod 4$. Então, q^2pode ser escrito como soma de dois quadrados, apenas da maneira $q^2 = q^2 + 0^2 = 0^2 + q^2$.*

Demonstração
Suponhamos que tínhamos $q^2 = a^2 + b^2$, para certos inteiros a e b. Então, $a^2 + b^2 \equiv 0 \pmod q$, pelo que seria $a^2 \equiv -b^2 \pmod q$.
Suponhamos que divide a. Então, é trivial mostrar que q divide b.
Então, temos $a = qr$ e $b = qs$, para certos números inteiros r e s.
Logo, temos $q^2 = a^2 + b^2 = q^2r^2 + q^2s^2$.
Então $1 = r^2 + s^2$, pelo que $r = 0$ ou $s = 0$. Então, $a = 0$ ou $b = 0$.
Suponhamos que q não divide a. Então, $\text{mdc}\,(a, b) = 1$, pelo que q^2 não é soma de dois quadrados, conforme vimos numa das proposições anteriores.
Está, portanto, terminada a demonstração.

Proposição 64 *Seja p um primo ímpar, tal que $p \equiv 1 \pmod 4$. Então existem inteiros x e m, tais que $1 + x^2 = mp$, com $0 < m < p$.*

Demonstração
Como $\left(\frac{-1}{p}\right) = 1$, existe um inteiro x, tal que $1 \leq x \leq p-1$ e $1 + x^2 \equiv 0 \pmod p$. Então, $1 + x^2 = mp$, para certo $m \in \mathbb{N}$. Mas $x^2 \leq (p-1)^2$, pelo que $1 + x^2 \leq p^2 - 2p + 2 < p^2$.
Logo, $0 < 1 + x^2 = mp < p^2$, donde se conclui que $0 < m < p$.
Está, assim, terminada a demonstração.

Proposição 65 *Seja p um primo ímpar. Então, existem inteiros x, y, m, tais que $1 + x^2 + y^2 = mp$, com $0 < m < p$.*

Demonstração
Se $p \equiv 1 \pmod 4$, então a proposição é verdadeira (basta utilizar a proposição anterior, fazendo $y = 0$). Mas a demonstração seguinte também se aplica nesse caso e não apenas, se $p \equiv 3 \pmod 4$.
Seja p um primo ímpar. Consideremos os p números $0^2, 1^2, \ldots, (p-1)^2$. O primeiro destes números é incongruente, módulo p, com os restantes, os quais são congruentes, módulo p, dois a dois; mais exactamente, se $0 \leq x, y \leq p-1$ e $x^2 \equiv y^2 \pmod p$, então $x = y$ ou $x = p - y$.
Consideremos os conjuntos $A = \left\{0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$ e $B = \left\{-1 - 0^2, -1 - 1^2, \ldots, -1 - \left(\frac{p-1}{2}\right)^2\right\}$.
Os elementos de A, são incongruentes, módulo p, dois a dois.
Os elementos de B, também são incongruentes, módulo p, dois a dois.
Como existem $\frac{p+1}{2}$ números, quer em A, quer em B, o conjunto $A \cup B$ é constituído por $p + 1$ números (todos distintos). Desses números, tem de haver dois que são congruentes, módulo p. Logo um dos números tem de pertencer a A e o outro a B, pois já vimos que não podem estar ambos em A, nem ambos em B.
Logo, $x^2 \equiv -1 - y^2 \pmod p$, para certos inteiros x e y, tais que $0 \leq x \leq \frac{p-1}{2}$ e $0 \leq y \leq \frac{p-1}{2}$.
Então, $x^2 + y^2 + 1 = mp$. Mas, temos $0 \leq x^2 \leq \left(\frac{p-1}{2}\right)^2$ e $0 \leq y^2 \leq \left(\frac{p-1}{2}\right)^2$.
Então, $0 < x^2 + y^2 + 1 \leq \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1$.
Logo, $0 < x^2 + y^2 + 1 < p^2$, donde vem $0 < mp < p^2$.
Então, $0 < m < p$, o que termina a demonstração.

Proposição 66 *Sejam p um primo tal que $p \equiv 1 \pmod 4$, $k = \lfloor \sqrt{p} \rfloor$ e $a \in \mathbb{N}$, tais que $a^2 \equiv -1 \pmod p$. Então, existem inteiros i e j, tais que $1 \leq i \leq k \wedge -k \leq j \leq k \wedge j \neq 0 \wedge ia \equiv j \pmod p$.*

Demonstração

Comecemos por recordar que sistema residual completo, módulo m, é um conjunto maximal de inteiros mutuamente incongruentes, módulo m, conjunto esse que tem, precisamente, m elementos.

Então, num conjunto que tenha mais do que m elementos, tem de haver dois elementos congruentes, módulo m.

Consideremos, agora, os $(k+1)^2$ números colocados no quadro seguinte:

0	1	2	...	k
a	$1+a$	$2+a$	...	$k+a$
$2a$	$1+2a$	$2+2a$	...	$k+2a$
...	...	...	...	...
ka	$1+ka$	$2+ka$	...	$k+ka$

Como $k < \sqrt{p} < k+1$, então $p < (k+1)^2$. Logo, dos $(k+1)^2$ números colocados na tabela anterior, há dois que são congruentes módulo p.

É imediato que em nenhuma linha há dois elementos congruentes, módulo p. Quanto às colunas, observe-se que os elementos da primeira coluna são incongruentes, módulo p, porque $\operatorname{mdc}(a,p) = 1$. Então, os elementos de qualquer coluna também são incongruentes, módulo p.

Logo os dois números congruentes, módulo p, estão em linhas e colunas distintas, pelo que existem inteiros r, s, t, u, tais que:

$$r, s, t, u \in [0, k] \wedge r \neq t \wedge s \neq u \wedge r + sa \equiv t + ua \pmod p$$

Sem perda de generalidade, podemos supor que $r < t$. Ora:

$$\begin{aligned} r + sa \equiv t + ua \pmod p \quad &\Longrightarrow \quad sa \equiv t - r + ua \pmod p \\ &\Longrightarrow \quad sa^2 \equiv (t-r)\,a + ua^2 \pmod p \\ &\Longrightarrow \quad -s \equiv (t-r)\,a - u \pmod p \\ &\Longrightarrow \quad (t-r)\,a \equiv u - s \pmod p \end{aligned}$$

Mas, $0 < t - r \leq t \leq k$ e $-k \leq u - s \leq k$. Então, fazendo $i = t - r$ e $j = u - s \neq 0$, temos que $1 \leq i \leq k \wedge -k \leq j \leq k \wedge j \neq 0 \wedge ia \equiv j \pmod p$, como se pretendia provar.

Note-se que é mais rápido considerar que há um elemento da primeira coluna que é congruente com um elemento de outa linha e outra coluna.

Proposição 67 *Seja p um primo tal que $p \equiv 1 \pmod 4$. Então, existem números naturais a e b, tais que $p = a^2 + b^2$. Mais, à parte a ordem das parcelas, a decomposição de p, numa soma de dois quadrados, é única.*

Demonstração

Recordemos que, dado $x \in \mathbb{R}$, $\lfloor x \rfloor$ é o maior inteiro que não é superior a x.

Sejam $k = \lfloor \sqrt{p} \rfloor$ e $a \in \mathbb{N}$, tais que $a^2 \equiv -1 \pmod p$.

Então, pela proposição anterior, existem inteiros i e j, tais que $1 \leq i \leq k \wedge -k \leq j \leq k \wedge j \neq 0 \wedge ia \equiv j \pmod p$.

Então, $0 < i^2 \leq k^2 < p$ e $0 < j^2 \leq k^2 < p$.

Logo, $0 < i^2 + j^2 < 2p$. Por outro lado, temos $ia \equiv j \pmod p$.

Então, $i^2a^2 \equiv j^2 \pmod p$. Logo, $-i^2 \equiv j^2 \pmod p$. Então, p é um divisor de i^2+j^2.
Logo, $i^2+j^2 = p$, porque $0 < i^2+j^2 < 2p$.
Suponhamos, agora, que $p = m^2+n^2 = i^2+j^2$, com $i,j,m,n \in \mathbb{N}$, $m \leq i < j \leq n$.
Ora,

$$\begin{aligned} p = m^2+n^2 = i^2+j^2 &\implies m^2+n^2 \equiv 0 \pmod p \wedge i^2+j^2 \equiv 0 \pmod p \\ &\implies m^2 \equiv -n^2 \pmod p \wedge i^2 \equiv -j^2 \pmod p \\ &\implies m^2i^2 \equiv n^2j^2 \pmod p \\ &\implies p \mid m^2i^2 - n^2j^2 \\ &\implies p \mid (mi-nj)(mi+nj) \\ &\implies p \mid mi-nj \vee p \mid mi+nj \end{aligned}$$

1. Suponhamos que $p \mid mi-nj$. Ora,

$$\begin{aligned} 0 < m \leq i < j \leq n &\implies m^2 \leq im \leq i^2 \wedge j^2 \leq nj \leq n^2 \\ &\implies m^2 \leq im \leq i^2 \wedge -n^2 \leq -nj \leq -j^2 \\ &\implies m^2-n^2 \leq im-nj \leq i^2-j^2 \\ &\implies -m^2-n^2 < im-nj < i^2+j^2 \\ &\implies -p < im-nj < p \end{aligned}$$

   Então, $im-nj = 0$, ou seja, $im = nj$.

   Mas, de $p = m^2+n^2 = i^2+j^2$ vem $\operatorname{mdc}(m,n) = 1 = \operatorname{mdc}(i,j)$.

   E de $im = nj$ vem $\frac{m}{n} = \frac{j}{i}$, pelo que $m = j \wedge n = i$, uma vez que i,j,m,n são números naturais e as fracções $\frac{m}{n}$ e $\frac{j}{i}$ são irredutíveis.

2. Suponhamos que p divide $mi+nj$. Ora,

$$\begin{aligned} 0 < m \leq i < j \leq n &\implies m^2 \leq im \leq i^2 \wedge j^2 \leq nj \leq n^2 \\ &\implies 0 < m^2+j^2 \leq im+nj \leq i^2+n^2 < i^2+j^2+m^2+n^2 \\ &\implies 0 < im+nj < 2p \end{aligned}$$

   Então, $im+nj = 2p$. Por outro lado, temos

$$\begin{aligned} p^2+(im-nj)^2 &= (im+nj)^2+(in-mj)^2 \\ &= i^2m^2+2imnj+n^2j^2+i^2n^2-2imnj+m^2j^2 \\ &= i^2m^2+n^2j^2+i^2n^2+m^2j^2 \\ &= i^2\left(m^2+n^2\right)+j^2\left(m^2+n^2\right) \\ &= \left(i^2+j^2\right)\left(m^2+n^2\right) = p \times p = p^2 \end{aligned}$$

   Logo, $p^2+(im-nj)^2 = p^2$, pelo que $im-nj = 0$.

   Analogamente ao caso anterior, temos $\frac{m}{n} = \frac{j}{i}$, com as duas fracções irredutíveis. Então, $m = j \wedge n = i$.

Ficou, asim, demonstrada a proposição.

Exemplo 68 *Consideremos $p = 41$. Vejamos a tabela anteriormente referida.*

Ora, $\lfloor\sqrt{41}\rfloor = 6$, tendo-se que $(20!)^2 \equiv -1 \pmod{41}$. Ora, $5! \equiv -3 \pmod{41}$.
Então, $7! \equiv -3 \pmod{41}$, porque $7 \times 6 \equiv 1 \pmod{41}$. E $9 \times 8 \equiv -10 \pmod{41}$.
Logo, $9! \equiv 30 \pmod{41}$ e $10! \equiv 300 \equiv 13 \pmod{41}$.
Mas, $12 \times 11 \equiv 132 \equiv 9 \pmod{41}$. Então, $12! \equiv 13 \times 9 \equiv -6 \pmod{41}$.
De $14 \times 13 \equiv 182 \equiv 18 \pmod{41}$, vem $14! \equiv -108 \equiv 15 \pmod{41}$.
De $16 \times 15 \equiv 240 \equiv -6 \pmod{41}$, vem $16! \equiv -90 \equiv -8 \pmod{41}$.
De $18 \times 17 \equiv 306 \equiv 19 \pmod{41}$, vem $18! \equiv -152 \equiv 12 \pmod{41}$.
De $20 \times 19 \equiv 380 \equiv 11 \pmod{41}$, vem $20! \equiv 132 \equiv 9 \pmod{41}$.
Ora, de facto, $9^2 \equiv -1 \pmod{41}$.
E, agora, temos $9 \times 4 \equiv -5 \pmod{41}$, tendo-se $0 < 4 < \sqrt{41}$ e $|-5| < \sqrt{41}$.
Então, $41 = 5^2 + 4^2$.
Passemos à tabela:
Como $a = 9$ e $\lfloor\sqrt{41}\rfloor = 6$, temos

0	1	2	3	4	5	6
9	10	11	12	13	14	15
18	19	20	21	22	23	24
27	28	29	30	31	32	33
36	37	38	39	40	41	42
45	46	47	48	49	50	51
54	55	56	57	58	59	60

0	1	2	3	4	5	6
9	10	11	12	13	14	15
18	19	20	21	22	23	24
27	28	29	30	31	32	33
36	37	38	39	40	0	1
4	5	6	7	8	9	10
13	14	15	16	17	18	19

Assim, por exemplo, $45 \equiv 4 \pmod{41}$. Logo, $5 \times 9 \equiv 4 \pmod{41}$.
Também podia ser $54 \equiv 13 \pmod{41}$. Logo, $6 \times 9 \equiv 4 + 9 \pmod{41}$.
Então, $6 \times 9^2 \equiv 4 \times 9 + 9^2 \pmod{41}$. Logo, $-6 \equiv 4 \times 9 - 1 \pmod{41}$.
Então, $-5 \equiv 4 \times 9 \pmod{41}$, com $0 < 4 < \sqrt{41}$ e $|-5| < \sqrt{41}$. Logo, $41 = 5^2 + 4^2$.

Proposição 69 *Seja p um primo tal que $p \equiv 1 \pmod{4}$. Então, existem números naturais a e b, tais que $p = a^2 + b^2$.*

(Outra) Demonstração

Esta demonstração é mais complicada do que a anteriormente apresentada, mas é a demonstração tradicional.

A congruência $x^2 \equiv -1 \pmod{p}$ tem solução, porque $p \equiv 1 \pmod{4}$.

Então, existe um número natural u tal que $u^2 \equiv -1 \pmod{p}$ e podemos escolher u, de modo que $u < \frac{p}{2}$.

De $u^2 \equiv -1 \pmod{p}$, vem que p divide u^2+1, pelo que existe um número natural l tal que $u^2+1 = lp$.

Então, para tal l, a equação $x^2 + y^2 = lp$ tem solução (no conjunto dos números naturais).

Se $l = 1$, nada mais há a fazer, pois $p = x^2 + 1^2$. Suponhamos que $l > 1$. Vamos mostrar que existe um inteiro positivo k, tal que $k < l$ e $x^2 + y^2 = kp$ tem solução, isto é, existem inteiros x, y, tais que $x^2 + y^2 = kp$. Ora:

$$u^2 + 1 = lp \wedge 0 < u < \frac{p}{2} \implies lp < \frac{p^2}{4} + 1 = \frac{p^2 + 4}{4} < \frac{p^2}{2} \implies l < \frac{p}{2}$$

Logo, $1 < l < \frac{p}{2}$.

Suponhamos, com vista a um absurdo, que l divide x e l divide y.

Então, l^2 divide x^2 e l^2 divide y^2, pelo que l^2 divide $x^2 + y^2$. Então, l^2 divide lp. Logo, l divide p.

E obtivemos uma contradição, pois $1 < l < \frac{p}{2}$.

Então, x e y não são ambos divisíveis por l.

Sejam $x_1, y_1 \in \mathbb{Z}$, tais que $x_1 \equiv x \pmod{l}, y_1 \equiv y \pmod{l}, |x_1| \leq \frac{l}{2}, |y_1| \leq \frac{l}{2}$.
Daqui vem que existem inteiros c, d tais que $x_1 = x + cl, y_1 = y + dl$.
Como x_1 e y_1 não podem ser ambos nulos, temos:

$$0 < x_1^2 + y_1^2 < \frac{l^2}{4} + \frac{l^2}{4} = \frac{l^2}{2}$$

Então, $x_1^2 + y_1^2 \equiv x^2 + y^2 \equiv lp \equiv 0 \pmod{l}$. Logo, $x_1^2 + y_1^2 = lr$, para certo $l \in \mathbb{N}$.
Então, $0 < x_1^2 + y_1^2 = lr < \frac{l^2}{2}$. Então, $0 < r < \frac{l}{2}$.
Por outro lado, temos que:

$$\begin{aligned}
\begin{cases} x^2 + y^2 = lp \\ x_1^2 + y_1^2 = lr \end{cases} \quad &\Longrightarrow \quad \left(x^2 + y^2\right)\left(x_1^2 + y_1^2\right) = l^2 pr \\
&\Longrightarrow \quad x^2x_1^2 + x^2y_1^2 + y^2x_1^2 + y^2y_1^2 + 2xyx_1y_1 - 2xyx_1y_1 = l^2pr \\
&\Longrightarrow \quad (xx_1 + yy_1)^2 + (xy_1 - yx_1)^2 = l^2pr \\
&\Longrightarrow \quad (x(x + cl) + y(y + dl))^2 + (x(y + dl) - y(x + cl))^2 = l^2pr \\
&\Longrightarrow \quad \left(x^2 + clx + y^2 + dly\right)^2 + (xy + dlx - yx - cly)^2 = l^2pr \\
&\Longrightarrow \quad \left(x^2 + y^2 + l(cx + dy)\right)^2 + (l(dx - cy))^2 = l^2pr \\
&\Longrightarrow \quad (lp + l(cx + dy))^2 + (l(dx - cy))^2 = l^2pr \\
&\Longrightarrow \quad (p + cx + dy)^2 + (dx - cy)^2 = pr
\end{aligned}$$

Logo,existem inteiros X e Y, tais que $X^2 + Y^2 = pr$, com $0 < r < \frac{l}{2}$.
Se $r = 1$, nada mais há a fazer. Se $r > 1$, então o processo continua, obtendo-se uma sequência estritamente decrescente de números inteiros positivos, que tem forçosamente de chegar a 1.
Logo, existem inteiros x e y, tais que $x^2 + y^2 = p$.

Proposição 70 *Seja p um primo tal que $p \equiv 3 \pmod{8}$. Então, existem números naturais a, b, c, tais que $p = a^2 + b^2 + c^2$.*

Demonstração
$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{8n+3-1}{2}}(-1)^{\frac{(8n+3)^2-1}{8}} = (-1)^{4n+1}(-1)^{\frac{(8n+4)(8n+2)}{8}} = -1 \times (-1)^{(2n+1)(4n+1)} = 1$
Então, existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -2 \pmod{p}$. Seja $k = \lfloor \sqrt{p} \rfloor$.
Consideremos a tabela seguinte:

0	1	2	...	k
a	$1 + a$	$2 + a$	...	$k + a$
$2a$	$1 + 2a$	$2 + 2a$	...	$k + 2a$
...	...	...	...	...
ka	$1 + ka$	$2 + ka$	...	$k + ka$

Nesta tabela, estão colocados $(k + 1)^2$ números inteiros (não necessariamente distintos).
Como $k < \sqrt{p} < k + 1$, então, $p < (k + 1)^2$. Então, na tabela anterior tem de haver dois números congruentes módulo p.
Tais números não podem estar na mesma coluna nem na mesma linha.
Então, tem de existir um elemento da primeira coluna que é congruente com algum elemento doutra coluna e outra linha: digamos que $ba \equiv ca + d \pmod{p}$, com $0 \leq a, b, c \leq k, b \neq c, d \neq 0$. Nota: Se não fosse da primeira coluna, bastava deslocarmo-nos para a esquerda um número conveniente de casas, em ambas as linhas.

Então, $(b-c)\,a \equiv d \pmod p$, com $-k \leq b-c \leq k$.
Logo, existe um inteiro $j \in [-k,k]$ tal que $aj \equiv d \pmod p$.
Então, $a^2j^2 \equiv d^2 \pmod p$, pelo que $\left|-2j^2-d^2\right| = 2j^2+d^2 = mp$, para certo inteiro m.
Ora, $0 \leq 2j^2 \leq 2k^2 < 2p \wedge 0 \leq d^2 \leq k^2 < p$.
Então, $0 \leq 2j^2+d^2 < 3p$, pelo que $2j^2+d^2 = p \vee 2j^2+d^2 = 2p$.
Se $2j^2+d^2 = p$, então $p = j^2+j^2+d^2$.
Se $2j^2+d^2 = 2p$, então d é par.
Então, $2j^2+4s^2 = 2p$, pelo que $j^2+2s^2 = p$.
Está, assim, terminada a demonstração.

Acabámos de verificar que todo o número primo p da forma $p = 8m+3$ admite uma decomposição numa soma de três quadrados, sendo duas das parcelas iguais.

Assim,

$$\begin{aligned} 3 &= 1^2+1^2+1^2 \\ 11 &= 3^2+1^2+1^2 \\ 19 &= 3^2+3^2+1^2 \\ 43 &= 5^2+3^2+3^2 \\ 59 &= 5^2+5^2+3^2 = 7^2+3^2+1^2 \end{aligned}$$

A última decomposição mostra que nem a decomposição é única, nem tem de haver duas parcelas iguais.

Exemplo 71 *Construção da tabela referente ao caso* $p = 19 = 2\times 8+3$.

0	1	2	3	4
6	7	8	9	10
12	13	14	15	16
18	0	1	2	3
5	6	7	8	9

$0a \equiv 3a+1 \implies 0 \equiv 3a^2+a \pmod{19} \implies 0 \equiv -6+a \pmod{19}$
$38 = 6^2+2\times 1^2 = 4\times 3^2+2\times 1^2 \implies 19 = 2\times 3^2+1^2$
Então, $19 = 3^2+3^2+1^2$.

Proposição 72 *Seja p um primo tal que $p \equiv 3 \pmod 8$. Então, para qualquer número natural n, p^n pode decompor-se numa soma de três quadrados.*

Demonstração
Se p é um primo tal que $p \equiv 3 \pmod 8$, então $p = 2x^2+y^2$, para certos naturais x, y.
Então, $p^{2m+1} = (p^m)^2\left(x^2+x^2+y^2\right) = (xp^m)^2+(xp^m)^2+(yp^m)^2$.
E, trivialmente, $p^{2m} = (p^m)^2+0^2+0^2$.
Registe-se que, em qualquer dos casos, a decomposição de p^n numa soma de três quadrados pode ser feita com duas parcelas iguais.

Proposição 73 *Seja p um primo tal que $p \equiv 3 \pmod 8$. Então, para quaisquer números naturais m, n, 2^mp^n pode decompor-se numa soma de três quadrados.*

Demonstração
Já vimos que $p^n = 2x_n^2 + y_n^2$, para certos naturais x_n, y_n.
Então, $2p^n = 4x_n^2 + 2y_n^2$, para certos naturais x_n, y_n.
Logo, $2p^n = (2x_n)^2 + y_n^2 + y_n^2$, para certos naturais x_n, y_n.
Mas, $2^{2a}p^n = 2^{2a}\left(2x_n^2 + y_n^2\right) = (2^a)^2\left(x_n^2 + x_n^2 + y_n^2\right) = (2^a x_n)^2 + (2^a x_n)^2 + (2^a y_n)^2$.
E, por fim, $2^{2a+1}p^n = 2 \times 2^{2a}\left(2x_n^2 + y_n^2\right) = (2^a)^2\left(4x_n^2 + y_n^2 + y_n^2\right) = \left(2^{a+1}x_n\right)^2 + (2^a y_n)^2 + (2^a y_n)^2$.

Lema 74 *Sejam $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$, números reais. Então,*

$$\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

$$com \begin{cases} z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \end{cases}$$

Demonstração
A demonstração consiste em efectuar os cálculos indicados em cada membro da igualdade. Esses cálculos são aborrecidos e ocupam muito espaço, pelo que não são apresentados.
Para a demonstração, ver o Capítulo intitulado O Anel dos Quaterniões.

Proposição 75 *Todo o primo p é soma de quatro quadrados.*

Demonstração
Se $p = 2$, então p é soma de quatro quadrados (dois dos quais nulos).
Se $p \equiv 1 \pmod 4$, então p é soma de dois quadrados, pelo que pode ser escrito como soma de quatro quadrados (dois dos quais nulos).
Suponhamos que $p \equiv 3 \pmod 4$.
Então, como já vimos, existem inteiros x, y, m, tais que $1 + x^2 + y^2 = mp$, com $0 < m < p$. Logo, existe um múltiplo de p, entre 0 e p^2, que é soma de três quadrados ($1^2 + x^2 + y^2 = mp$, com $0 < m < p$).
Logo existe um certo inteiro m, com $0 < m < p$, tal que a equação $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$ tem solução, com $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.
Se $m = 1$, então p é soma de quatro quadrados ($p = x^2 + y^2 + 1^2 + 0^2$).
Se $m > 1$, vamos mostrar que existe um inteiro positivo n, tal que $n < m$ e a equação tem solução. Isto prova que o menor inteiro positivo k, tal que a equação $x_1^2 + x_2^2 + x_3^2 + x_4^2 = kp$ tem solução, é 1.
Suponhamos que $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$, com $m > 1$, tem solução.
Suponhamos, ainda, que p divide x_1, x_2, x_3 e x_4. Então p^2 divide mp, pelo que p divide m, o que contradiz $0 < m < p$. Então é absurdo supor que p divide, simultaneamente, x_1, x_2, x_3 e x_4.
Vamos considerar dois casos, consoante m seja par ou ímpar.
1^o caso: m é par
Como $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod 2$, então $x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 2$.
Então, temos três hipóteses a considerar:
(a) x_1, x_2, x_3 e x_4 são todos pares
(b) x_1, x_2, x_3 e x_4 são todos ímpares
(c) x_1 e x_2 são pares, x_3 e x_4 são ímpares (sem perda de generalidade).
Sejam $y_1 = \frac{x_1+x_2}{2}$, $y_2 = \frac{x_1-x_2}{2}$, $y_3 = \frac{x_3+x_4}{2}$ e $y_4 = \frac{x_3-x_4}{2}$.

Em quaquer das três hipóteses anteriores, temos que y_1, y_2, y_3 e y_4 são inteiros, verificando-se que:

$$\begin{aligned} y_1^2+y_2^2+y_3^2+y_4^2 &= \left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2 \\ &= \frac{1}{4}\left(2x_1^2+2x_2^2+2x_3^2+2x_4^2\right)=\frac{1}{2}\left(x_1^2+x_2^2+x_3^2+x_4^2\right)=\frac{mp}{2} \end{aligned}$$

Como $0<\frac{m}{2}<m$ e m é par, temos o resultado pretendido.

2^o caso: m é ímpar

Então $3\leq m<p$.

Sejam $y_1,y_2,y_3,y_4\in\mathbb{Z}$, tais que $y_j\equiv x_j\,(\mathrm{mod}\,m)\wedge|y_j|<\frac{m}{2}$, para $j=1,2,3,4$.

Suponhamos que m divide qualquer x_j $(j=1,2,3,4)$. Então, m^2 divide qualquer x_j^2. Logo, m^2 divide $x_1^2+x_2^2+x_3^2+x_4^2$, pelo que m^2 divide mp. Então, m divide p, o que contradiz $3\leq m<p$.

Logo, é absurdo supor que m divide, simultaneamente, os quatro números x_1, x_2, x_3 e x_4, pelo que m não divide, simultaneamente, os números y_1,y_2,y_3,y_4.

Mas, $0<y_1^2+y_2^2+y_3^2+y_4^2<4\times\frac{m^2}{4}=m^2$, tendo-se, ainda, que $y_1^2+y_2^2+y_3^2+y_4^2\equiv 0\,(\mathrm{mod}\,m)$.

Então, $x_1^2+x_2^2+x_3^2+x_4^2=mp$ e $y_1^2+y_2^2+y_3^2+y_4^2=nm$, com $0<n<m$.

Logo, $\left(x_1^2+x_2^2+x_3^2+x_4^2\right)\left(y_1^2+y_2^2+y_3^2+y_4^2\right)=m^2np$.

Mas, já vimos que

$$\left(x_1^2+x_2^2+x_3^2+x_4^2\right)\left(y_1^2+y_2^2+y_3^2+y_4^2\right)=z_1^2+z_2^2+z_3^2+z_4^2$$

$$\text{com}\begin{cases} z_1=x_1y_1+x_2y_2+x_3y_3+x_4y_4\\ z_2=x_1y_2-x_2y_1+x_3y_4-x_4y_3\\ z_3=x_1y_3-x_3y_1+x_4y_2-x_2y_4\\ z_4=x_1y_4-x_4y_1+x_2y_3-x_3y_2 \end{cases}.$$

$$\text{Então,}\begin{cases} z_1\equiv x_1^2+x_2^2+x_3^2+x_4^2\equiv 0\,(\mathrm{mod}\,m)\\ z_2\equiv x_1x_2-x_2x_1+x_3x_4-x_4x_3\equiv 0\,(\mathrm{mod}\,m)\\ z_3\equiv x_1x_3-x_3x_1+x_4x_2-x_2x_4\equiv 0\,(\mathrm{mod}\,m)\\ z_4\equiv x_1x_4-x_4x_1+x_2x_3-x_3x_2\equiv 0\,(\mathrm{mod}\,m) \end{cases}.$$

$$\text{Então,}\begin{cases} z_1=mw_1\\ z_2=mw_2\\ z_3=mw_3\\ z_4=mw_4 \end{cases}\text{, com } w_i\in\mathbb{N}\ (\text{para } i=1,2,3,4).$$

Então, $z_1^2+z_2^2+z_3^2+z_4^2=m^2w_1^2+m^2w_2^2+m^2w_3^2+m^2w_4^2=m^2\left(w_1^2+w_2^2+w_3^2+w_4^2\right)$.

Logo, $m^2\left(w_1^2+w_2^2+w_3^2+w_4^2\right)=m^2np$, pelo que $w_1^2+w_2^2+w_3^2+w_4^2=np$, com $0<n<m$.

Está, assim, terminada a demonstração de que todo o número primo é soma de quatro quadrados.

Corolário 76 *Todo o número natural é soma de quatro quadrados*

Demonstração

Seja n um número natural.

Se $n=1$, então n é soma de quatro quadrados: $1=1^2+0^2+0^2+0^2$.

Se n é um número primo, então, pela proposição anterior, n é soma de quatro quadrados.

Se n é um produto de dois primos, então n é soma de quatro quadrados, conforme se afirmou anteriormente.

Finalmente, se n é um produto de um número finito de primos, então demonstra-se, por indução no número de primos, que n é soma de quatro quadrados.

Proposição 77 *Nenhum número natural da forma $8m-1$, com $m\in\mathbb{N}$, é soma de três quadrados.*

Demonstração

Suponhamos que existiam $a, b, c \in \mathbb{Z}$, tais que $8m - 1 = a^2 + b^2 + c^2$. Então teríamos $a^2 + b^2 + c^2 \equiv 7 \pmod 8$ o que é impossível, pois, como pode ser facilmente verificado, $a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5$ ou $6 \pmod 8$, uma vez que $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, $0^2 \equiv 4^2 \equiv 0 \pmod 8$ e $2^2 \equiv 6^2 \equiv 4 \pmod 8$.

Proposição 78 *Seja $p \in \mathbb{N}$, um primo ímpar. Seja $\mu(p)$ o número de pares de inteiros consecutivos, pertencentes ao intervalo $[1, p-1]$, que são resíduos quadráticos, módulo p.*

Então, $\mu(p) = \frac{1}{4}\left(p - 4 - (-1)^{\frac{p-1}{2}}\right)$.

Demonstração

Comecemos por observar que, para cada $n \in \mathbb{N}$, com $1 \leq n \leq p-1$, existe $\overline{n} \in \mathbb{N}$, tal que $1 \leq \overline{n} \leq p-1$ e $n\overline{n} \equiv 1 \pmod p$. Além disso, quando n percorre $\{1, 2, \ldots, p-1\}$, $\overline{n}$ percorre o mesmo conjunto (e reciprocamente). Note-se, ainda, que $\left(\frac{p}{p}\right) = 0$.

Agora, vamos mostrar que $\sum_{n=1}^{p-2} \left(\frac{n(n+1)}{p}\right) = -1$:

$$\begin{aligned}
\sum_{n=1}^{p-2}\left(\frac{n(n+1)}{p}\right) &= \sum_{n=1}^{p-1}\left(\frac{n(n+1)}{p}\right) = \sum_{n=1}^{p-1}\left(\left(\frac{n(n+1)}{p}\right)\left(\frac{\overline{n}}{p}\right)^2\right) \\
&= \sum_{n=1}^{p-1}\left(\frac{n\overline{n}\overline{n}(n+1)}{p}\right) = \sum_{n=1}^{p-1}\left(\frac{\overline{n}(n+1)}{p}\right) \\
&= \sum_{n=1}^{p-1}\left(\frac{\overline{n}n + \overline{n}}{p}\right) = \sum_{n=1}^{p-1}\left(\frac{1+\overline{n}}{p}\right) \\
&= \sum_{\overline{n}=1}^{p-1}\left(\frac{1+\overline{n}}{p}\right) = \sum_{\overline{n}=1}^{p-2}\left(\frac{1+\overline{n}}{p}\right) \\
&= \sum_{\overline{n}=2}^{p-1}\left(\frac{\overline{n}}{p}\right) \\
&= -1
\end{aligned}$$

Note-se que num sistema residual reduzido, módulo p, com p primo ímpar, o número de resíduos quadráticos é igual ao número de resíduos não quadráticos, módulo p, pelo que $\sum_{n=1}^{p-1}\left(\frac{n}{p}\right) = 0$.

Então, $\sum_{n=2}^{p-1}\left(\frac{n}{p}\right) = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right) - \left(\frac{1}{p}\right) = 0 - 1 = -1$.

Seja $n \in \mathbb{N}$. Seja $f_p(n) = \begin{cases} 1 & \Longleftarrow \quad \left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) = 1 \\ 0 & \Longleftarrow \quad \left(\frac{n}{p}\right) \neq 1 \vee \left(\frac{n+1}{p}\right) \neq 1 \end{cases}$

Então, $f_p(n) = \frac{1}{4}\left(1 + \left(\frac{n}{p}\right)\right) \times \left(1 + \left(\frac{n+1}{p}\right)\right)$, pois cada parênteses é 2 ou 0, sendo 2, apenas no caso de n e $n+1$ serem resíduos quadráticos, módulo p.

Então, temos que:

$$\begin{aligned}
\mu(p) &= \sum_{n=1}^{p-2} f_p(n) \\
&= \frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)\right)\times\left(1+\left(\frac{n+1}{p}\right)\right) \\
&= \frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)+\left(\frac{n+1}{p}\right)+\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\right) \\
&= \frac{1}{4}\sum_{n=1}^{p-2}1+\frac{1}{4}\sum_{n=1}^{p-2}\left(\frac{n}{p}\right)+\frac{1}{4}\sum_{n=1}^{p-2}\left(\frac{n+1}{p}\right)+\frac{1}{4}\sum_{n=1}^{p-2}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) \\
&= \frac{p-2}{4}+\frac{1}{4}\left(0-\left(\frac{-1}{p}\right)\right)+\frac{1}{4}(-1)+\frac{1}{4}\sum_{n=1}^{p-2}\left(\frac{n(n+1)}{p}\right) \\
&= \frac{p-2}{4}-\frac{1}{4}(-1)^{\frac{p-1}{2}}-\frac{1}{4}+\frac{1}{4}(-1) \\
&= \frac{p-4}{4}-\frac{1}{4}(-1)^{\frac{p-1}{2}} \\
&= \frac{1}{4}\left(p-4-(-1)^{\frac{p-1}{2}}\right)
\end{aligned}$$

Proposição 79 *Seja p um primo ímpar. Sejam $a, b \in \mathbb{Z}$.*

Então, $\sum_{n=0}^{p-1}\left(\frac{(n-a)(n-b)}{p}\right) = \begin{cases} p-1 & \Longleftarrow \quad a \equiv b \pmod p \\ -1 & \Longleftarrow \quad a \not\equiv b \pmod p \end{cases}$

Demonstração

Suponhamos, em primeiro lugar, que $a \equiv b \pmod p$. Então:

$$\begin{aligned}
\sum_{n=0}^{p-1}\left(\frac{(n-a)(n-b)}{p}\right) &= \sum_{n=-a}^{p-a-1}\left(\frac{n(n+a-b)}{p}\right) \\
&= \sum_{n=0}^{p-1}\left(\frac{n(n+a-b)}{p}\right) \\
&= \sum_{n=0}^{p-1}\left(\frac{n(n+0)}{p}\right) \\
&= \sum_{n=0}^{p-1}\left(\frac{n^2}{p}\right) = p-1
\end{aligned}$$

Suponhamos, agora, que $a \not\equiv b \pmod p$. Para cada natural n, tal que p não divide n, existe $\overline{n} \in \mathbb{N}$, tal que $1 \leq \overline{n} \leq p-1$ e $n\overline{n} \equiv 1 \pmod p$. Além disso, quando n percorre $\{1, 2, \ldots, p-1\}$, $\overline{n}$ percorre o mesmo conjunto (e reciprocamente).

Então:

$$\begin{aligned}
\sum_{n=0}^{p-1}\left(\frac{(n-a)(n-b)}{p}\right) &= \sum_{n=-a}^{p-a-1}\left(\frac{n(n+a-b)}{p}\right)=\sum_{n=0}^{p-1}\left(\frac{n(n+a-b)}{p}\right)\\
&= \sum_{n=1}^{p-1}\left(\frac{n(n+a-b)}{p}\right)=\sum_{n=1}^{p-1}\left(\frac{n\overline{nn}(n+a-b)}{p}\right)\\
&= \sum_{n=1}^{p-1}\left(\frac{1\overline{n}(n+a-b)}{p}\right)=\sum_{n=1}^{p-1}\left(\frac{\overline{n}n+\overline{n}(a-b)}{p}\right)\\
&= \sum_{\overline{n}=1}^{p-1}\left(\frac{1+\overline{n}(a-b)}{p}\right)=\sum_{m=1}^{p-1}\left(\frac{1+m}{p}\right)=\sum_{m=2}^{p}\left(\frac{m}{p}\right)\\
&= \sum_{m=2}^{p-1}\left(\frac{m}{p}\right)=\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)-\left(\frac{1}{p}\right)\\
&= 0-1=-1
\end{aligned}$$

Note-se que $a\not\equiv b\,(\mathrm{mod}\,p)$ e, por isso, quando $\overline{n}$ percorre um sistema residual reduzido, módulo p, o mesmo acontece com $\overline{n}\,(a-b)$.

Então, $\sum\limits_{\overline{n}=1}^{p-1}\left(\frac{1+\overline{n}(a-b)}{p}\right)=\sum\limits_{m=1}^{p-1}\left(\frac{1+m}{p}\right)$, como utilizado acima.

Lema 80 *Seja p um primo ímpar. Seja $\nu(p)$ o número de pares de inteiros consecutivos, pertencentes ao intervalo $[1,p-1]$, que são resíduos quadráticos, módulo p.*

Então, $\nu(p)=\frac{p}{8}+\frac{1}{8}\left(\sum\limits_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right)-8-\left(\frac{-2}{p}\right)-3\left(\frac{2}{p}\right)-3\left(\frac{-1}{p}\right)\right)$.

Demonstração

Como já vimos $\sum\limits_{n=1}^{p-1}\left(\frac{n}{p}\right)=0$, porque o número de resíduos quadráticos, módulo p, é igual ao número de resíduos não quadráticos, módulo p. Consideremos a aplicação de $\mathbb{N}$ em $\mathbb{Z}$, definida por:

$$g_p(n)=\begin{cases}1 & \Longleftarrow \quad \left(\frac{n}{p}\right)=\left(\frac{n+1}{p}\right)=\left(\frac{n+2}{p}\right)=1\\ 0 & \Longleftarrow \quad \left(\frac{n}{p}\right)\neq 1\vee\left(\frac{n+1}{p}\right)\neq 1\vee\left(\frac{n+2}{p}\right)\neq 1\end{cases}$$

Então, temos que

$$\begin{aligned}
8\nu(p) &= 8\sum_{n=1}^{p-3}g_p(n)\\
&= \sum_{n=1}^{p-3}\left[1+\left(\frac{n}{p}\right)\right]\times\left[1+\left(\frac{n+1}{p}\right)\right]\times\left[1+\left(\frac{n+2}{p}\right)\right]\\
&= \sum_{n=1}^{p-3}1+\sum_{n=1}^{p-3}\left(\frac{n}{p}\right)+\sum_{n=1}^{p-3}\left(\frac{n+1}{p}\right)+\sum_{n=1}^{p-3}\left(\frac{n+2}{p}\right)+\sum_{n=1}^{p-3}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\\
&\quad+\sum_{n=1}^{p-3}\left(\frac{n}{p}\right)\left(\frac{n+2}{p}\right)+\sum_{n=1}^{p-3}\left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right)+\sum_{n=1}^{p-3}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right)
\end{aligned}$$

Ora,

$$\begin{cases} \sum_{n=1}^{p-3} 1 = p-3 \\ \sum_{n=1}^{p-3} \left(\frac{n}{p}\right) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) - \left(\frac{p-2}{p}\right) - \left(\frac{p-1}{p}\right) = 0 - \left(\frac{-2}{p}\right) - \left(\frac{-1}{p}\right) = -\left(\frac{-2}{p}\right) - \left(\frac{-1}{p}\right) \\ \sum_{n=1}^{p-3} \left(\frac{n+1}{p}\right) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = -\left(\frac{1}{p}\right) - \left(\frac{p-1}{p}\right) = 0 - \left(\frac{1}{p}\right) - \left(\frac{-1}{p}\right) = -1 - \left(\frac{-1}{p}\right) \\ \sum_{n=1}^{p-3} \left(\frac{n+2}{p}\right) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) - \left(\frac{1}{p}\right) - \left(\frac{2}{p}\right) = 0 - 1 - \left(\frac{2}{p}\right) = -1 - \left(\frac{2}{p}\right) \end{cases}$$

Por outro lado,

$$\begin{cases} \sum_{n=1}^{p-3} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = \sum_{n=1}^{p-3} \left(\frac{n(n+1)}{p}\right) = \sum_{n=1}^{p-2} \left(\frac{n(n+1)}{p}\right) - \left(\frac{(p-2)(p+1)}{p}\right) = -1 - \left(\frac{2}{p}\right) \\ \sum_{n=1}^{p-3} \left(\frac{n}{p}\right)\left(\frac{n+2}{p}\right) = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)\left(\frac{n+2}{p}\right) - 0 - 0 - \left(\frac{p-1}{p}\right)\left(\frac{p+1}{p}\right) = -1 - \left(\frac{-1}{p}\right) \\ \sum_{n=1}^{p-3} \left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right) = \sum_{n=0}^{p-1} \left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right) - \left(\frac{2}{p}\right) - 0 - 0 = -1 - \left(\frac{2}{p}\right) \end{cases}$$

Então,

$$\begin{aligned} 8\nu(p) &= p - 3 - \left(\frac{-2}{p}\right) - \left(\frac{-1}{p}\right) - 1 - \left(\frac{-1}{p}\right) - 1 - \left(\frac{2}{p}\right) - 1 - \left(\frac{2}{p}\right) - 1 - \left(\frac{-1}{p}\right) - 1 - \left(\frac{2}{p}\right) \\ &\quad + \sum_{n=1}^{p-3} \left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right)\left(\frac{n}{p}\right) \\ &= p - 8 - \left(\frac{-2}{p}\right) - 3\left(\frac{2}{p}\right) - 3\left(\frac{-1}{p}\right) + \sum_{n=1}^{p-3} \left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right)\left(\frac{n}{p}\right) \end{aligned}$$

E, finalmente

$$\nu(p) = \frac{p}{8} + \frac{1}{8}\left(\sum_{n=1}^{p-3} \left(\frac{n(n+1)(n+2)}{p}\right) - 8 - \left(\frac{-2}{p}\right) - 3\left(\frac{2}{p}\right) - 3\left(\frac{-1}{p}\right)\right)$$

Lema 81 *Seja p um primo ímpar.*

Seja θ a função de $\mathbb{Z}$ em $\mathbb{Z}$, definida por $\theta(m) = \sum_{n=1}^{p} \left(\frac{n(n^2-m)}{p}\right)$.

Então, $\theta(1) = \sum_{n=1}^{p-3} \left(\frac{n(n+1)(n+2)}{p}\right)$.

Demonstração

$$\begin{aligned}
\theta(1) &= \sum_{n=1}^{p}\left(\frac{n\left(n^2-1\right)}{p}\right)=\sum_{n=1}^{p}\left(\frac{(n-1)\,n\,(n+1)}{p}\right)\\
&= \sum_{n=0}^{p-1}\left(\frac{n\,(n+1)\,(n+2)}{p}\right)=\left(\frac{0}{p}\right)+\sum_{n=1}^{p-1}\left(\frac{n\,(n+1)\,(n+2)}{p}\right)\\
&= \sum_{n=1}^{p-3}\left(\frac{n\,(n+1)\,(n+2)}{p}\right)+\sum_{n=p-2}^{p-1}\left(\frac{n\,(n+1)\,(n+2)}{p}\right)\\
&= \sum_{n=1}^{p-3}\left(\frac{n\,(n+1)\,(n+2)}{p}\right)+0+0\\
&= \sum_{n=1}^{p-3}\left(\frac{n\,(n+1)\,(n+2)}{p}\right)
\end{aligned}$$

Lema 82 *Seja p um primo ímpar, tal que $p\equiv 3\,(\mathrm{mod}\,4)$. Seja θ a função de $\mathbb{Z}$ em $\mathbb{Z}$, definida por $\theta(m)=\sum\limits_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right)$. Então, $\theta(m)=0,\forall m\in\mathbb{Z}$.*

Demonstração
Como $p\equiv 3\,(\mathrm{mod}\,4)$, temos que $p=4t+3$, para certo inteiro t.
Então:

$$\begin{aligned}
\theta(m) &= \sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right)=\sum_{n=1}^{p-1}\left(\frac{n\left(n^2-m\right)}{p}\right)=\sum_{n=1}^{4t+2}\left(\frac{n\left(n^2-m\right)}{p}\right)\\
&= \sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)+\sum_{n=2t+2}^{4t+2}\left(\frac{n\left(n^2-m\right)}{p}\right)\\
&= \sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)+\sum_{n=1}^{2t+1}\left(\frac{(p-n)\left((p-n)^2-m\right)}{p}\right)\\
&= \sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)+\sum_{n=1}^{2t+1}\left(\frac{(p-n)\left(p^2-2np+n^2-m\right)}{p}\right)\\
&= \sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)+\sum_{n=1}^{2t+1}\left(\frac{-n\left(n^2-m\right)}{p}\right)\\
&= \sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)+\sum_{n=1}^{2t+1}\left(\frac{-1}{p}\right)\left(\frac{n\left(n^2-m\right)}{p}\right)\\
&= \sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)+\sum_{n=1}^{2t+1}(-1)^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)\\
&= \sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)-\sum_{n=1}^{2t+1}\left(\frac{n\left(n^2-m\right)}{p}\right)\\
&= 0
\end{aligned}$$

Lema 83 *Seja p um primo ímpar, tal que $p \equiv 1 \pmod 4$.*
Seja θ a função de $\mathbb{Z}$ em $\mathbb{Z}$, definida por $\theta(m) = \sum_{n=1}^{p} \left(\frac{n(n^2-m)}{p}\right)$.
Então, $\theta(m) = 2\sum_{n=1}^{\frac{p-1}{2}} \left(\frac{n(n^2-m)}{p}\right), \forall m \in \mathbb{Z}$.

Demonstração
Como $p \equiv 1 \pmod 4$, temos que $t = 4t + 1$, para certo inteiro t. Então:

$$\begin{aligned}
\theta(m) &= \sum_{n=1}^{p} \left(\frac{n\left(n^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{p-1} \left(\frac{n\left(n^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{4t} \left(\frac{n\left(n^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) + \sum_{n=2t+1}^{4t} \left(\frac{n\left(n^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) + \sum_{n=1}^{2t} \left(\frac{(p-n)\left((p-n)^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) + \sum_{n=1}^{2t} \left(\frac{(p-n)\left(p^2-2np+n^2-m\right)}{p}\right)
\end{aligned}$$

Logo,

$$\begin{aligned}
\theta(m) &= \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) + \sum_{n=1}^{2t} \left(\frac{-n\left(n^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) + \sum_{n=1}^{2t} \left(\frac{-1}{p}\right)\left(\frac{n\left(n^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) + \sum_{n=1}^{2t} (-1)^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) \\
&= \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) + \sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right) \\
&= 2\sum_{n=1}^{2t} \left(\frac{n\left(n^2-m\right)}{p}\right)
\end{aligned}$$

Lema 84 *Seja p um primo ímpar.Seja $k \in \mathbb{Z}$, tal que $\operatorname{mdc}(p,k) = 1$. Seja θ a função de $\mathbb{Z}$ em $\mathbb{Z}$, definida por $\theta(m) = \sum_{n=1}^{p} \left(\frac{n(n^2-m)}{p}\right)$. Então, $\theta(m) = \left(\frac{k}{p}\right)\theta\left(mk^2\right), \forall m \in \mathbb{Z}$.*

Demonstração
Como $\text{mdc}\,(p,k)=1$, então $\left(\frac{k^4}{p}\right)=1$. Então:

$$\begin{aligned}\theta(m) &= \sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right)=\sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right)\left(\frac{k^4}{p}\right)\\ &= \sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)k^4}{p}\right)=\sum_{n=1}^{p}\left(\frac{knk\left(n^2k^2-mk^2\right)}{p}\right)\\ &= \left(\frac{k}{p}\right)\sum_{n=1}^{p}\left(\frac{nk\left((nk)^2-mk^2\right)}{p}\right)\\ &= \left(\frac{k}{p}\right)\sum_{N=1}^{p}\left(\frac{N\left(N^2-mk^2\right)}{p}\right)=\left(\frac{k}{p}\right)\theta\left(mk^2\right)\end{aligned}$$

Corolário 85 *Sejam p um primo ímpar, u e v dois resíduos quadráticos, módulo p. Seja θ a função de $\mathbb{Z}$ em $\mathbb{Z}$, definida por $\theta(m)=\sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right)$. Então, $|\theta(u)|=|\theta(v)|$.*

Demonstração
Suponhamos que $\text{mdc}\,(p,k)=1$.
Então, pelo lema anterior, temos que $\theta(m)=\sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right), \forall m\in\mathbb{Z}$.
Logo, $|\theta(1)|=\left|\left(\frac{k}{p}\right)\theta\left(k^2\right)\right|=\left|\theta\left(k^2\right)\right|$.
Então, como u e v são dois resíduos quadráticos, módulo p, temos $u\equiv x^2\,(\text{mod}\,p)$ e $v\equiv y^2\,(\text{mod}\,p)$, para certos inteiros x e y.

$$\begin{cases}|\theta(u)|=\left|\theta\left(x^2\right)\right|=|\theta(1)|\\ |\theta(v)|=\left|\theta\left(y^2\right)\right|=|\theta(1)|\end{cases}$$

Logo, $|\theta(u)|=|\theta(v)|$.

Corolário 86 *Sejam p um primo ímpar, u e v dois resíduos não quadráticos, módulo p e a função θ definida por $\theta(m)=\sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right)$.*

Então, $|\theta(u)|=|\theta(v)|$.
Demonstração
Como u e v são dois resíduos não quadráticos, módulo p, então $\text{mdc}\,(p,u)=1=\text{mdc}\,(p,v)$.
Seja g uma raiz primitiva de p.
Então existem $a,b\in\mathbb{N}_0$, tais que $u\equiv g^{2a+1}\,(\text{mod}\,p)\,, v\equiv g^{2b+1}\,(\text{mod}\,p)$.
Note-se que os expoentes têm de ser ímpares, pois, u e v são resíduos não quadráticos, módulo p.
Se tivermos $b\geq a$, fazemos $y=g^{b-a}$.
Então, $v\equiv g^{2b+1}\equiv g^{2b+1+2a-2a}\equiv g^{2a+1}\times g^{2b-2a}\equiv u\times g^{2(b-a)}\equiv uy^2\,(\text{mod}\,p)$.
Mas, por um lema anterior, $\theta(u)=\left(\frac{y}{p}\right)\theta\left(uy^2\right)$.
Então, $|\theta(u)|=\left|\theta\left(uy^2\right)\right|=|\theta(v)|$.
Se tivermos $b<a$, a demonstração é análoga.
Observemos que, no caso de m ser múltiplo de p, temos:

$$\sum_{n=1}^{p}\left(\frac{n\left(n^2-m\right)}{p}\right)=\sum_{n=1}^{p}\left(\frac{n\times n^2}{p}\right)=\sum_{n=1}^{p}\left(\frac{n}{p}\right)=0$$

Observemos, também, que $\theta(m) = \theta(m+p) = \theta(m+np), \forall n \in \mathbb{Z}$.

Observação

Demonstração alternativa:

Como $\text{mdc}(p,u) = 1 = \text{mdc}(p,v)$, a congruência $ux \equiv v \pmod{p}$ tem solução z.

Então, existe um inteiro z, tal que $uz \equiv v \pmod{p}$ e $\text{mdc}(p,z) = 1$.

O inteiro z tem de ser um resíduo quadrático, módulo p.

Então, $z \equiv y^2 \pmod{p}$, para certo inteiro y.

Logo, $v \equiv uy^2 \pmod{p}$. E o resto da demonstração é igual.

Corolário 87 *Sejam p um primo ímpar, e v um resíduo não quadrático, módulo p.*

Seja θ a função definida por $\theta(m) = \sum_{n=1}^{p} \left(\frac{n(n^2-m)}{p}\right)$.

Então, $\sum_{m=1}^{p} (\theta(m))^2 = 2p(p-1)$.

Demonstração

$$\begin{aligned}
\sum_{m=1}^{p-1} (\theta(m))^2 &= \sum_{m=1}^{p-1} \left[\left(\sum_{i=1}^{p-1} \left(\frac{i(i^2-m)}{p} \right) \right) \times \left(\sum_{j=1}^{p-1} \left(\frac{j(j^2-m)}{p} \right) \right) \right] \\
&= \sum_{m=1}^{p-1} \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \left(\frac{ij}{p}\right) \left(\frac{i^2-m}{p}\right) \left(\frac{j^2-m}{p}\right) \\
&= \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{ij}{p}\right) \left(\frac{i^2-m}{p}\right) \left(\frac{j^2-m}{p}\right) \\
&= \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{ij}{p}\right) \left(\frac{m-i^2}{p}\right) \left(\frac{m-j^2}{p}\right) \\
&= \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \left(\frac{ij}{p}\right) \sum_{m=1}^{p-1} \left(\frac{m-i^2}{p}\right) \left(\frac{m-j^2}{p}\right) \\
&= \sum_{i=1}^{p-1} \sum_{\substack{j=1 \\ j^2 \equiv i^2}}^{p-1} \left(\frac{ij}{p}\right) \sum_{m=1}^{p-1} \left(\frac{m-i^2}{p}\right) \left(\frac{m-j^2}{p}\right) \\
&\quad + \sum_{i=1}^{p-1} \sum_{\substack{j=1 \\ ,j^2 \not\equiv i^2 (\text{mod}\, p)}}^{p-1} \left(\frac{ij}{p}\right) \sum_{m=1}^{p-1} \left(\frac{m-i^2}{p}\right) \left(\frac{m-j^2}{p}\right) \\
&= \sum_{i=1}^{p-1} \sum_{\substack{j=1 \\ ,j^2 \equiv i^2 (\text{mod}\, p)}}^{p-1} \left(\frac{ij}{p}\right)(p-1) + \sum_{i=1}^{p-1} \sum_{\substack{j(\text{mod}\, p) \\ j^2 \not\equiv i^2 (\text{mod}\, p)}}^{p-1} \left(\frac{ij}{p}\right) \sum_{m=1}^{p-1} (-1) \\
&= (p-1) \sum_{i=1}^{p-1} 2 - \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \sum_{\substack{j=1 \\ j^2 \not\equiv i^2 (\text{mod}\, p)}}^{p-1} \left(\frac{j}{p}\right)
\end{aligned}$$

Logo,

$$\begin{aligned}\sum_{m=1}^{p-1}(\theta(m))^2 &= (p-1)\sum_{i=1}^{p-1}2-\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\left(0-\left(\frac{i}{p}\right)-\left(\frac{-i}{p}\right)\right)\\ &= 2(p-1)^2+2\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\left(\frac{i}{p}\right)\\ &= 2(p-1)^2+2(p-1)\\ &= 2p(p-1)\end{aligned}$$

Corolário 88 *Seja p um primo ímpar tal que $p\equiv 1\pmod 4$ e v um resíduo não quadrático, módulo p. Seja θ a função definida por $\theta(m)=\sum_{n=1}^{p}\left(\frac{n(n^2-m)}{p}\right)$. Então, $\sum_{m=1}^{p}(\theta(m))^2=\frac{p-1}{2}(\theta(1))^2+\frac{p-1}{2}(\theta(v))^2$.*

Demonstração

Já sabemos que $|\theta(x)|=|\theta(y)|$, se x e y são ambos resíduos quadráticos, módulo p, ou ambos resíduos não quadráticos, módulo p.

Logo, $|\theta(m)|$ só pode tomar dois valores, consoante m é ou não resíduo quadrático, módulo p.

É claro que o mesmo acontece com $(\theta(m))^2$. Ora, $\theta(p)=\sum_{n=1}^{p}\left(\frac{n(n^2)}{p}\right)=\sum_{n=1}^{p}\left(\frac{n}{p}\right)=0$, pelo que $\theta(m)=\sum_{n=1}^{p-1}\left(\frac{n(n^2-m)}{p}\right)$-

Então, $\sum_{m=1}^{p}(\theta(m))^2=\sum_{m=1}^{p-1}(\theta(m))^2=\frac{p-1}{2}(\theta(1))^2+\frac{p-1}{2}(\theta(v))^2$, porque há $\frac{p-1}{2}$ resíduos quadráticos, módulo p, e $\frac{p-1}{2}$ resíduos não quadráticos, módulo p.

Corolário 89 *Seja p um número primo tal que $p\equiv 1\pmod 4$. Então, p é soma de dois quadrados.*

Demonstração

Na demonstração dos corolários anteriores verificámos que, se tivermos $p\equiv 1\pmod 4$, então temos $\sum_{m=1}^{p-1}(\theta(m))^2=\frac{p-1}{2}(\theta(1))^2+\frac{p-1}{2}(\theta(v))^2=2p(p-1)$, onde v é um resíduo não quadrático, módulo p. Então:

$$(\theta(1))^2+(\theta(v))^2=4p$$

Logo, $\theta(1)$ e $\theta(v)$ são ambos pares ou ambos ímpares. Mas não podem ser ambos ímpares, porque $(2a+1)^2+(2b+1)^2=4a^2+4a+4b^2+4b+2$ que não é múltiplo de 4. Então, $\theta(1)$ e $\theta(v)$ são ambos pares.

Então, $p=\left(\frac{\theta(1)}{2}\right)^2+\left(\frac{\theta(v)}{2}\right)^2$, ou seja, p é soma dos quadrados de dois números inteiros.

Exemplo 90 *Consideremos o número primo 29, número este que é congruente com 1, módulo 4. Os resíduos quadráticos, módulo 29, são 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28; os resíduos não quadráticos, módulo 29, são 2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27.*

Ora, $\theta(1)=\sum_{n=1}^{26}\left(\frac{n(n+1)(n+2)}{p}\right)$. Mas,

$$\begin{cases} \sum_{n=1}^{4}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{2\times3}{29}\right)+\left(\frac{2\times3\times4}{29}\right)+\left(\frac{3\times4\times5}{29}\right)+\left(\frac{4\times5\times6}{29}\right)=1+1-1+1=2 \\ \sum_{n=5}^{8}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{5\times6\times7}{29}\right)+\left(\frac{6\times7\times8}{29}\right)+\left(\frac{7\times8\times9}{29}\right)+\left(\frac{8\times9\times10}{29}\right)=1-1-1+1=0 \\ \sum_{n=9}^{11}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{9\times10\times11}{29}\right)+\left(\frac{10\times11\times12}{29}\right)+\left(\frac{11\times12\times13}{29}\right)=1-1+1=1 \\ \sum_{n=12}^{14}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{12\times13\times14}{29}\right)+\left(\frac{13\times14\times15}{29}\right)+\left(\frac{14\times15\times16}{29}\right)=1+1+1=3 \\ \sum_{n=15}^{17}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{15\times16\times17}{29}\right)+\left(\frac{16\times17\times18}{29}\right)+\left(\frac{17\times18\times19}{29}\right)=1+1-1=1 \\ \sum_{n=18}^{20}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{18\times19\times20}{29}\right)+\left(\frac{19\times20\times21}{29}\right)+\left(\frac{20\times21\times22}{29}\right)=1+1-1=1 \\ \sum_{n=21}^{23}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{21\times22\times23}{29}\right)+\left(\frac{22\times23\times24}{29}\right)+\left(\frac{23\times24\times25}{29}\right)=-1+1+1=1 \\ \sum_{n=24}^{26}\left(\frac{n(n+1)(n+2)}{p}\right)=\left(\frac{24\times25\times26}{29}\right)+\left(\frac{25\times26\times27}{29}\right)+\left(\frac{26\times27\times28}{29}\right)=-1+1+1=1 \end{cases}$$

Então,

$$\theta(1)=2+0+1+3+1+1+1+1+0=10$$

De modo análogo calculávamos $\theta(2)$.

$$\theta(2)=\sum_{n=1}^{26}\left(\frac{n\left(n^2-2\right)}{p}\right)=\sum_{n=1}^{26}\left(\frac{n(n+1)(n+2)}{p}\right)=\cdots=4$$

Então, $\frac{1}{2}\theta(1)=5$ e $\frac{1}{2}\theta(2)=2$, pelo que $29=5^2+2^2$.

É claro que este deve ser o pior processo de descobrir que $29=5^2+2^2$. No entanto, provou-se que que qualquer primo da forma $4n+1$ (com $n\in\mathbb{N}$) é uma soma de dois quadrados.

Proposição 91 *Seja p um primo ímpar. Seja $\nu(p)$ o número de pares de inteiros consecutivos, pertencentes ao intervalo $[1,p-1]$, que são resíduos quadráticos, módulo p. Então $\nu(p)=\frac{p}{8}+E_p$, com $|E_p|<2+\frac{1}{4}\sqrt{p}$.*

Demonstração

Num doslemas anteriores, vimos que $\nu(p)=\frac{p}{8}+\frac{1}{8}\left(\sum_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right)-8-\left(\frac{-2}{p}\right)-3\left(\frac{2}{p}\right)-3\left(\frac{-1}{p}\right)\right)$, com:

Seja $E_p=\frac{1}{8}\left(\sum_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right)-8-\left(\frac{-2}{p}\right)-3\left(\frac{2}{p}\right)-3\left(\frac{-1}{p}\right)\right)$.

Então, $E_p=\frac{1}{8}\sum_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right)-1-\frac{1}{8}\left(\frac{-2}{p}\right)-\frac{3}{8}\left(\frac{2}{p}\right)-\frac{3}{8}\left(\frac{-1}{p}\right)$.

Logo, $|E_p|\leq\frac{1}{8}\left|\sum_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right)\right|+1+\frac{1}{8}+\frac{3}{8}+\frac{3}{8}$.

Logo, $|E_p| < 2 + \frac{1}{8}\left|\sum_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right)\right|$.
Seja u um resíduo não quadrático.
Então, $(\theta(1))^2 + (\theta(u))^2 = 4p$, conforme já verificámos.
Então, $0 < (\theta(1))^2 < 4p$, donde se conclui que $|\theta(1)| < 2\sqrt{p}$.
Então,

$$\left|\sum_{n=1}^{p-1}\left(\frac{n\left(n^2-1\right)}{p}\right)\right| = \left|\sum_{n=2}^{p-2}\left(\frac{(n-1)\,n\,(n+1)}{p}\right)\right| = \left|\sum_{n=1}^{p-3}\left(\frac{n\,(n+1)\,(n+2)}{p}\right)\right| < 2\sqrt{p}$$

Logo,

$$|E_p| < 2 + \frac{1}{4}\sqrt{p}$$

Capítulo 2

Grupos Cíclicos Finitos

Definição 92 *Recordamos, de forma abreviada, que grupo é um conjunto não vazio G, no qual se define uma operação binária associativa para a qual existe um elemento neutro 1 e, para todo o elemento $g \in G$, existe um elemento g' tal que $gg' = g'g = 1$. Esse elemento g', habitualmente, é representado por g^{-1}, recebendo o nome de inverso de g.*

Definição 93 *Um grupo G diz-se comutativo, se $gh = hg, \forall g, h \in G$.*

Definição 94 *Sejam G um grupo finito e $g \in G$. Ordem de g, que se denota por $\operatorname{ord}(g)$, é o menor inteiro positivo t, tal que $g^t = 1$. Ordem de G, que se denota por $|G|$, é o número de elementos de G.*

Definição 95 *Seja G um grupo e seja S um subconjunto não vazio de G. Diz-se que S é subgrupo de G, se $\forall x, y \in S, xy^{-1} \in S$.*

Definição 96 *Sejam G um grupo, g um elemento de G e n um número natural.*

Definição 97 *Define-se potência de do seguinte modo:* $\begin{cases} g^0 = 1 \\ g^{n+1} = g^n g \\ g^{-n} = (g^n)^{-1} \end{cases}$

Proposição 98 *Seja G um grupo comutativo. São válidas as seguintes propriedades:*

1. $g^m g^n = g^{m+n}, \forall g \in G, \forall m, n \in \mathbb{Z}$
2. $(g^m)^n = g^{mn}, \forall g \in G, \forall m, n \in \mathbb{Z}$
3. $g^m h^m = (gh)^m, \forall g, h \in G, \forall m \in \mathbb{Z}$

Definição 99 *O subgrupo S, gerado por um elemento de um grupo G, é o conjunto S definido por $S = \{g^m : m \in \mathbb{Z}\}$. Se S é gerado por g, escrevemos $S = \langle g \rangle$.*

Definição 100 *Seja G um grupo. Diz-se que G é um grupo cíclico, se existir $g \in G$ tal que G é o subgrupo gerado por g.*

Proposição 101 *Todo o grupo cíclico é comutativo.*

Definição 102 *Todo o subgrupo de um grupo cíclico é cíclico.*

Proposição 103 *Sejam G um grupo e $g \in G$. Seja S o subgrupo de G, gerado por g. Se S é finito, então $\operatorname{ord}(g) = |S|$.*

Proposição 104 *Sejam G um grupo e $g \in G$. Sejam m a ordem de g e S o subgrupo de G, gerado por g. Se $m > 1$, então $S = \{g, g^2, \ldots, g^m\}$ e os m elementos de S são todos distintos.*

Proposição 105 *(Teorema de Lagrange)*
Sejam G um grupo finito e S um subgrupo de G. Então, $|S|$ divide $|G|$.

Definição 106 *Seja G um grupo finito. Expoente de G, $e(G)$, é o mínimo múltiplo comum entre as ordens dos elementos de G.*

Proposição 107 *Seja G um grupo abeliano (grupo comutativo) finito. Então existe em G um elemento g tal que* $\operatorname{ord}(g) = e(G)$

Demonstração
Se $e(G) = p^n$, a demonstração é trivial, porque o mínimo múltiplo comum entre as ordens é a maior delas.

Suponhamos que $e(G) = m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ com $k \geq 2, \alpha_i \geq 1, p_1, \ldots, p_k$ números primos tais que, se $i \neq j$, então $p_i \neq p_j$, com $1 \leq i, j \leq k$ e $G = \{g_1, \ldots, g_n\}$.

Então existe $h_1' \in G$, tal que $\operatorname{ord}(h_1') = p_1^{\alpha_1} \times q_1$, com $q_1 \in \mathbb{N}$ e $\operatorname{mdc}(p_1, q_1)$.

Logo existe $h_1 \in G$, tal que $\operatorname{ord}(h_1) = p_1^{\alpha_1}$ (por exemplo $(h_1')^{q_1}$).

Analogamente, existe $h_i \in G$, tal que $\operatorname{ord}(h_i) = p_i^{\alpha_i}$, para $2 \leq i \leq k$.

Seja S_i, o subgrupo de G, gerado por h_i (com $1 \leq i \leq k$). Seja $g = h_1 \cdots h_k$.

Vejamos que $\operatorname{ord}(g) = m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Seja $r \in \mathbb{N}$.

Como G é comutativo, $g^r = (h_1 \cdots h_k)^r = h_1^r \cdots h_k^r$.

Suponhamos, agora, que $g^r = 1$. Então, $h_1^{-r} = h_2^r \cdots h_k^r$.

Logo, $h_1^{-r} \in S_1 \cap S_2 \cdots S_k = \{1\}$. Logo, $h_1^r = 1$, pelo que r é múltiplo da ordem de h_1.

Analogamente se mostra que r é múltiplo da ordem de h_i (para $2 \leq i \leq k$).

Então, r é múltiplo de $p_i^{\alpha_i}$, para $1 \leq i \leq k$, pelo que r é múltiplo de $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Logo, a ordem de g é um múltiplo de $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Ora, $(h_1)^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} = \left((h_1)^{p_1^{\alpha_1}}\right)^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = (1)^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = 1$.

E, analogamente se mostra que $(h_i)^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} = 1$, para $2 \leq i \leq k$.

Então, $g^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} = (h_1 \cdots h_k)^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} = (h_1)^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \cdots (h_k)^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} = 1$.

Logo, a ordem de g é um divisor de $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Logo a ordem de é $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, como se pretendia demonstrar.

Proposição 108 *Seja $\mathbb{K}$ um corpo e seja G um subgrupo finito do grupo multiplicativo $\mathbb{K}^*$. Então, G é cíclico.*

Demonstração
Seja $e = e(G)$, o expoente de G. Pela proposição anterior, existe $g \in G$ tal que $\operatorname{ord}(g) = e$.

Consideremos S, o subgrupo de G gerado por g. É claro que S é cíclico.

Seja $x \in G$. Então $x^e = 1$, porque e é o expoente de G. Logo, x é raiz do polinómio $t^e - 1 \in \mathbb{K}[t]$.

Como o polinómio $t^e - 1$ tem, no máximo, e raízes, então o número de elementos de G é menor ou igual a e, isto é, $|G| \leq e$.

Por outro lado, $e = |S| \leq |G|$, porque S é um subgrupo de G.

Logo $|G| = e = |S|$, pelo que $G = S$, uma vez que G é finito. Logo, G é cíclico.

Proposição 109 *Seja $p \in \mathbb{N}$ um número primo. Então, $\mathbb{Z}_p^*$ é um grupo cíclico de ordem $p - 1$.*

Demonstração
Consequência imediata do facto de $\mathbb{Z}_p$ ser um corpo finito, de $\mathbb{Z}_p^*$ ter $p-1$ elementos e da proposição anterior.

Proposição 110 *Seja G um grupo comutativo finito. Então,* $\operatorname{ord}\left(\prod_{g\in G} g\right) \leq 2$.

Demonstração
Seja $x = \prod_{g\in G} g$. Então,

$$x^2 = \left(\prod_{g\in G} g\right)\left(\prod_{g\in G} g\right) = \left(\prod_{g\in G} g\right)\left(\prod_{g\in G} g^{-1}\right) = \prod_{g\in G}\left(gg^{-1}\right) = \prod_{g\in G} 1 = 1$$

Logo, $\operatorname{ord}\left(\prod_{g\in G} g\right) \leq 2$.

Proposição 111 *Seja G um grupo cíclico finito e seja $x = \prod_{g\in G} g$. Então, temos que:*

1. *Se $|G|$ é ímpar, então* $\operatorname{ord}(x) = 1$.
2. *Se $|G|$ é par, então* $\operatorname{ord}(x) = 2$.

Demonstração
Pela proposição anterior, $\operatorname{ord}(x) \leq 2$.

1. Se $|G|$ é ímpar, então $\operatorname{ord}(x) = 1$, porque 2 não divide $|G|$ (que é ímpar).
2. Se $|G|$ é par, então x é o único elemento de G que é diferente de 1 e coincide com o seu oposto, porque em $\prod_{g\in G} g$, produto dos elementos de G, todos cortam com o seu oposto, com excepção dos dois que coincidem com o oposto. Logo, $\operatorname{ord}(x) = 2$.

Definição 112 *Função φ de Euler é a aplicação de em definida por:*

$\varphi(n)$ é o número de elementos de $\{1, 2, \ldots, n\}$ que são primos com n.

Proposição 113 *Sejam G um grupo cíclico de ordem finita m, g um gerador de G e $r \in \mathbb{Z}$. Então, $\langle g^r\rangle = G$, se e só se* $\operatorname{mdc}(m, r) = 1$.

Demonstração
Suponhamos que $\operatorname{mdc}(m, r) = 1$ e que $(g^r)^d = 1$. Então $g^{rd} = 1$. Então, $rd = mk$, para certo inteiro k.

Se r divide mk e r é primo com m, então r divide k. Logo, $k = qr$, com $q \in \mathbb{Z}$. Então, $rd = mqr$, donde se conclui que $d = mq$.

É claro que $(g^r)^m = (g^m)^r = 1$. Então, $\operatorname{ord}(g^r) = m$, pelo que $\langle g^r\rangle = G$.

Suponhamos, agora, que $\operatorname{mdc}(m, r) \neq 1$. Então, existe um número primo p, tal que p divide m e p divide r.

Então, $(g^r)^{\frac{m}{p}} = g^{\frac{rm}{p}} = (g^m)^{\frac{r}{p}} = 1$.

Logo, a ordem de g^r é menor ou igual a $\frac{m}{p}$, pelo que g^r não é um gerador de G.

Proposição 114 *Num grupo cíclico finito de ordem m, há, exactamente, $\varphi(m)$ geradores.*

Demonstração

Seja $g \in G$, um gerador de G. Então, $\operatorname{ord}(g) = m$ e $G = \{g, g^2, \ldots, g^m\}$.

Então, pela proposição anterior, é imediato concluir que há $\varphi(m)$ geradores de G, uma vez que $g, g^2, \ldots, g^m$ são elementos distintos.

Proposição 115 *Seja G um grupo cíclico finito. Sejam $a, b \in G$ tais que $\operatorname{ord}(a) = \operatorname{ord}(b)$. Então, $\langle a \rangle = \langle b \rangle$.*

Demonstração

Sejam m a ordem de G e d um divisor de m, tal que $\operatorname{ord}(a) = \operatorname{ord}(b) = d$. Seja g um gerador de G. Então, $g^{\frac{m}{d}}$ também tem ordem d. Vejamos que a pertence ao subgrupo de G gerado por $g^{\frac{m}{d}}$. Se $a \in G$, então $a = g^n$, para certo $n \in \mathbb{N}$. Então, $1 = a^d = (g^n)^d = g^{nd}$.

Então, nd é um múltiplo de m, ou seja, $nd = km$, para certo inteiro k. Então, $n = k\frac{m}{d}$, pelo que $a \in \langle g^{\frac{m}{d}} \rangle$. Logo, $\langle a \rangle \subseteq \langle g^{\frac{m}{d}} \rangle$, pelo que se verifica $\langle a \rangle = \langle g^{\frac{m}{d}} \rangle$, uma vez que os dois subgrupos têm a mesma ordem (finita).

Analogamente, $\langle b \rangle = \langle g^{\frac{m}{d}} \rangle$. Então, $\langle a \rangle = \langle b \rangle$, conforme se pretendia mostrar.

Proposição 116 *Seja m um número natural. Então, $\sum_{d|m} \varphi(d) = m$.*

Demonstração

Seja m um número natural e consideremos um grupo cíclico de ordem m. Tal é possível, porque há grupos cíclicos de qualquer ordem (finita).

Para cada divisor d de m, existe, pelo menos, um elemento de ordem d.

Mais precisamente, para cada divisor d de m, há exactamente, $\varphi(d)$ elementos de ordem d.

E, quando percorremos os divisores de m, contamos todos os elementos de G, uma e uma só vez. Logo, $\sum_{d|m} \varphi(d) = m$.

Proposição 117 *Seja m um número natural. Seja G um grupo de ordem m tal que, para cada divisor d de m, não há mais do que d elementos de que satisfazem $x^d = 1$. Então, G é cíclico.*

Demonstração

Sejam d um divisor de m e $\psi(d)$ o número de elementos de G que têm ordem d. Se $\psi(d) > 0$, então há, pelo menos, um elemento de G que tem ordem d. Esse elemento gera um subgrupo S de G, subgrupo esse que é um grupo cíclico de ordem d. Todos os elementos desse subgrupo de G (e só esses) satisfazem a condição $x^d = 1$, pelo que em S (e em G) há, exactamente, $\varphi(d)$ elementos de ordem d. Logo, se $\psi(d) > 0$, então $\psi(d) = \varphi(d)$. Como $\sum_{d|m} \varphi(d) = m = \sum_{d|m} \psi(d)$ e $\psi(d) \leq \varphi(d)$, para todo o divisor d de m, então $\psi(d) = \varphi(d)$, para qualquer d que divida m. Em particular, $\psi(m) = \varphi(m) > 0$, donde se conclui que G é cíclico.

Proposição 118 *Seja $\mathbb{K}$ um corpo. Então, todo o subgrupo finito de $(\mathbb{K}^*, \times)$, é cíclico.*

Demonstração

Seja d um número natural. Num corpo, não há mais do que d elementos que satisfazem a condição $x^d = 1$, pelo que o resultado pretendido é uma consequência imediata da proposição anterior. Note-se que $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Proposição 119 *Seja $\mathbb{K}$ um corpo finito. Então todo o subgrupo de $(\mathbb{K}^*, \times)$, é cíclico.*

Demonstração

Se $\mathbb{K}$ é corpo finito, então todo o subgrupo de $(\mathbb{K}^*, \times)$, é finito. Então, pela proposição anterior, todo o subgrupo de $(\mathbb{K}^*, \times)$, é cíclico.

Proposição 120 *Seja p um número primo. Então, $\left(\mathbb{Z}_p^*, \times\right)$ é cíclico.*

Demonstração

Esta proposição é uma consequência imediata da proposição anterior, uma vez que $\mathbb{Z}_p$ é um corpo finito.

Proposição 121 *Seja m um número natural. Então $\mathbb{U}_m$, o conjunto das unidades de $\mathbb{Z}_m$, é um grupo multiplicativo de ordem $\varphi(m)$.*

Demonstração

Começamos por recordar que unidade dum Anel com identidade é um elemento invertível (para a multiplicação).

Sejam $A = \{1, 2, \ldots, m\}$ e $x \in A$. Se, $\operatorname{mdc}(x, m) = 1$, então existem números inteiros a e b, tais que $ax + bm = 1$. Então $ax \equiv 1 \pmod{m}$, pelo que x é invertível em $\mathbb{Z}_m$. Se $\operatorname{mdc}(x, m) > 1$, então não existem números inteiros a e b, tais que $ax + bm = 1$. Logo, x não é invertível em $\mathbb{Z}_m$. Logo, em $\mathbb{Z}_m$, há precisamente $\varphi(m)$ elementos invertíveis. Então, a ordem de $\mathbb{U}_m$ é $\varphi(m)$. É claro que $(\mathbb{U}_m, \times)$ é grupo, pelo que está terminada a demonstração.

Capítulo 3

O Anel dos Inteiros Gaussianos

Nota histórica

O aparecimento dos números complexos deve-se à procura da fórmula resolvente das equações de 3^o grau de coeficientes reais, as quais têm, no mínimo, uma solução real. Como veremos mais adiante, toda a equação de 3^o grau pode ser transformada numa equação da forma $x^3 + ax + b = 0$, pelo que basta obter a fórmula resolvente para este caso. Fazendo $x = u + v$, vem:

$$\begin{aligned}(u+v)^3 + a(u+v) + b = 0 &\iff u^3 + 3u^2v + 3uv^2 + v^3 + a(u+v) + b = 0\\ &\iff u^3 + v^3 + 3uv(u+v) + a(u+v) + b = 0\\ &\iff u^3 + v^3 + (3uv + a)(u+v) = -b\end{aligned}$$

Podemos escolher u e v de modo que $3uv = -a \wedge u^3 + v^3 = -b$. Então, $uv = -\frac{a}{3}$.

Logo, $u^3v^3 = -\frac{a^3}{27} \wedge u^3 + v^3 = -b$, donde se conclui que u^3 e v^3 são as raízes da equação de 2^o grau $\lambda^2 + b\lambda - \frac{a^3}{27} = 0$.

Como $\lambda^2 + b\lambda - \frac{a^3}{27} = 0 \iff \lambda = \frac{-b \pm \sqrt{b^2 + \frac{4a^3}{27}}}{2}$, temos $\begin{cases} u^3 = \frac{-b + \sqrt{b^2 + \frac{4a^3}{27}}}{2} \\ v^3 = \frac{-b - \sqrt{b^2 + \frac{4a^3}{27}}}{2} \end{cases}$.

Então, $\begin{cases} u = \sqrt[3]{\frac{-b + \sqrt{b^2 + \frac{4a^3}{27}}}{2}} \\ v = \sqrt[3]{\frac{-b - \sqrt{b^2 + \frac{4a^3}{27}}}{2}} \end{cases}$, pelo que $x = \sqrt[3]{\frac{-b + \sqrt{b^2 + \frac{4a^3}{27}}}{2}} + \sqrt[3]{\frac{-b - \sqrt{b^2 + \frac{4a^3}{27}}}{2}}$

Vejamos um exemplo de resolução de uma equação de terceiro grau, usando o método anterior:
Consideremos a equação $x^3 + 3x^2 - 3x - 1 = 0$.
Começamos por fazer a substituição $x = y + h$, com vista a eliminar o termo de 2^o grau, obtendo-se:

$$(y+h)^3 + 3(y+h)^2 - 3(y+h) - 1 = 0$$

A equação anterior é equivalente a

$$y^3 + 3y^2h + 3yh^2 + h^3 + 3y^2 + 6yh + 3h^2 - 3y - 3h - 1 = 0$$

Logo,

$$y^3 + (3h+3)y^2 + \left(3h^2 + 6h - 3\right)y + h^3 + 3h^2 - 3h - 1 = 0$$

Fazendo $h = -1$, vem $y^3 - 6y + 4 = 0$
Segue-se a nova substituição $y = u + v$, a qual nos conduz a $u^3 + v^3 = -4 \wedge u^3v^3 = 8$.
Então, u^3 e são as raízes da equação de $2\ ^o$ grau $\lambda^2 + 4\lambda + 8 = 0$, que *são* $-2 \pm \sqrt{-4}$.

Obtivemos, deste modo, uma raiz quadrada de um número negativo, a qual não representa nenhum número real.

Para quem já conhece os números imaginários, é *fácil* verificar que $u = \sqrt[3]{-2+2i} = 1+i$ e que $v = \sqrt[3]{-2-2i} = 1-i$.

Observe-se, no entanto, que $\sqrt[3]{-2+2i}$ é uma expressão pouco pacífica, uma vez que um número imaginário admite três raízes cúbicas e não apenas uma.

Se usarmos as raízes cúbicas $1+i$ e $1-i$, obtemos

$$y = u + v = 1 + i + 1 - i = 2 \wedge x = y + h = 2 - 1 = 1$$

Logo, uma das raízes da equação inicial é 1, o que permite encontrar as outras raízes (aplicando a regra de Ruffini).

	1	3	−3	−1
1		1	4	1
	1	4	1	0

Então, $x^3 + 3x^2 - 3x - 1 = 0 \iff (x-1)\left(x^2+4x+1\right) = 0 \iff x = -2 \pm \sqrt{3}$.

Repare-se que, embora as três raízes da equação sejam reais, para resolver a equação, tivemos de "sair"do conjunto $\mathbb{R}$.

E se tivéssemos usado outra raiz cúbica de $-2+2i$?

Vimos que uma das raízes cúbicas de é $1+i$.

Como $1+i = \sqrt{2}\,\mathrm{cis}\,\frac{\pi}{4}$, então as outras raízes cúbicas de $-2+2i$ são $\sqrt{2}\,\mathrm{cis}\left(\frac{\pi}{4}+\frac{2\pi}{3}\right)$ e $\sqrt{2}\,\mathrm{cis}\left(\frac{\pi}{4}-\frac{2\pi}{3}\right)$.

Seja $u = \sqrt{2}\,\mathrm{cis}\left(\frac{\pi}{4}+\frac{2\pi}{3}\right) = \sqrt{2}\,\mathrm{cis}\,\frac{11\pi}{12}$.

Ora, de $uv = 2$, vem $v = \frac{2}{u} = \frac{2}{\sqrt{2}\,\mathrm{cis}\,\frac{11\pi}{12}} = \sqrt{2}\,\mathrm{cis}\left(-\frac{11\pi}{12}\right)$

Então,

$$\begin{aligned} y &= u + v = \sqrt{2}\,\mathrm{cis}\,\frac{11\pi}{12} + \sqrt{2}\,\mathrm{cis}\left(-\frac{11\pi}{12}\right) = 2\sqrt{2}\cos\frac{11\pi}{12} = 2\sqrt{2}\cos\left(\frac{\pi}{4}+\frac{2\pi}{3}\right) \\ &= 2\sqrt{2}\left(\cos\frac{\pi}{4}\cos\frac{2\pi}{3} - \sin\frac{\pi}{4}\sin\frac{2\pi}{3}\right) = 2\sqrt{2}\left(\frac{\sqrt{2}}{2}\times\left(-\frac{1}{2}\right) - \frac{\sqrt{2}}{2}\times\frac{\sqrt{3}}{2}\right) \\ &= 2\sqrt{2}\left(-\frac{\sqrt{2}}{4} - \frac{\sqrt{6}}{4}\right) = -1 - \sqrt{3} \end{aligned}$$

Logo, $x = -1 - \sqrt{3} - 1 = -2 - \sqrt{3}$, obtendo-se, assim uma das raízes da equação inicial.

Definição 122 *Corpo dos números complexos é o conjunto* $\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}$*, algebrizado com as operações "adição" e "multiplicação" assim definidas:*

Adição: $(a+bi)+(c+di) = (a+c)+(b+d)\,i$

Multiplicação: $(a+bi)\times(c+di) = (ac-bd)+(ad+bc)\,i$

A definição da multiplicação apresentada resulta da multiplicação "usual" de polinómios com a condição suplementar $i^2 = -1$.

Definição 123 *Seja* $z = a+bi$*, com* $a, b \in \mathbb{R}$*. O complexo* $a-bi$*, é chamado conjugado de* z *(e é representado por* $\overline{z}$*), enquanto que ao número real* $\sqrt{a^2+b^2}$ *chamamos módulo de* z *(que é representado por* $|z|$*). Ao número* a *chamamos parte real de* z *e escrevemos* $\mathrm{Re}\,(z) = a$*, enquanto que ao número* b *chamamos parte imaginária de* z *e escrevemos* $\mathrm{Im}\,(z) = b$*.*

Definição 124 *Ao conjunto* $\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}\}$*, o qual algebrizado com a adição e multiplicação de complexos é um anel, chamamos anel dos inteiros gaussianos.*

Definição 125 *Inteiro algébrico é um elemento do conjunto* $\mathbb{C}$ *que anula um polinómio mónico de* $\mathbb{Z}[t]$*, isto é, anula um polinómio em* t *cujos coeficientes pertencem a* $\mathbb{Z}$ *e em que o termo de maior grau tem coeficiente* 1*.*

É fácil verificar que todos os elementos de $\mathbb{Z}(i)$ são inteiros algébricos; para isso, basta-nos considerar $a + bi$ e a equação de 2^o grau $x^2 - 2ax + a^2 + b^2 = 0$, com $a, b \in \mathbb{Z}$.

Observemos, ainda, que a definição de inteiro apresentada não cria, em $\mathbb{Q}$, mais inteiros, para além dos elementos de $\mathbb{Z}$, os quais, por esse motivo, são chamados inteiros racionais.

Definição 126 *Num anel com identidade, chama-se unidade a qualquer elemento do anel que seja invertível.*

Definição 127 *Dois elementos dum anel com identidade dizem-se associados, se exitir uma unidade do anel que multiplicada por um dos elementos dê o outro.*

Definição 128 *Em* $\mathbb{Z}(i)$*, define-se norma, como sendo a aplicação* N*, de* $\mathbb{Z}(i)$ *em* $\mathbb{Z}$*, tal que* $\mathrm{N}(a + bi) = a^2 + b^2$*.*

Proposição 129 *A aplicação anterior satisfaz as propriedades seguintes:*

1. $\mathrm{N}(a + bi) \geq 0, \forall a, b \in \mathbb{Z}$
2. Se $a, b \in \mathbb{Z}$, então $\mathrm{N}(a + bi) = 0 \iff a = b = 0$
3. $\mathrm{N}(z) = \mathrm{N}(\overline{z}), \forall z \in \mathbb{Z}(i)$
4. $\mathrm{N}(zw) = \mathrm{N}(z) \times \mathrm{N}(w), \forall z, w \in \mathbb{Z}(i)$

Uma vantagem da aplicação norma, em relação à aplicação módulo, reside no facto da norma de qualquer inteiro gaussiano ser um número inteiro racional, enquanto que o módulo dum inteiro gaussiano pode ser um número irracional.

Proposição 130 *O conjunto* $\mathbb{U}$*, dos elementos invertíveis de um anel com identidade, forma um grupo multiplicativo.*

Demonstração

$\mathbb{U}$ é um conjunto não vazio, porque $1 \in \mathbb{U}$.

Sejam $u, v \in \mathbb{U}$. Então existem, em $\mathbb{U}$, elementos s e t, tais que $su = us = 1 = tv = vt$.

De $(uv)(ts) = u(vt)s = u(1s) = us = 1$ e de $(ts)(uv) = t(su)v = t(1v) = tv = 1$, concluímos que uv é um elemento invertível, donde vem que $\mathbb{U}$ é um grupo para a multiplicação, uma vez que esta operação é associativa, existe, em $\mathbb{U}$, elemento neutro e todo o elemento de $\mathbb{U}$ é invertível.

Definição 131 *Sejam* A *um anel e* $a, b \in A$*. Diz-se que* a *divide* b *(e escrevemos* $a \,|\, b$*), se existir, em* A*, um elemento* c*, tal que* $ac = b$*. Se não existir um tal* c*, diz-se que* a *não divide* b*.*

Definição 132 *Seja* $\alpha \in \mathbb{Z}(i)$*. Diz-se que é irredutível, se, sempre que tivermos* $\alpha = \beta\sigma$*, com* β, σ *pertencentes a* $\mathbb{Z}(i)$*, então, pelo menos, um dos elementos* β, σ *é unidade.*

Definição 133 *Seja $\alpha \in \mathbb{Z}(i)$. Diz-se que α é primo, se α não é unidade e sempre que α divide um produto de dois elementos de $\mathbb{Z}(i)$, então α divide um dos factores. Diz-se que α não é primo, se α é unidade ou se α divide um produto de dois elementos de $\mathbb{Z}(i)$ e não divide nenhum dos factores.*

Proposição 134 *Seja $\alpha \in \mathbb{Z}(i)$. Então, α é uma unidade de $\mathbb{Z}(i)$, sse $\mathrm{N}(\alpha) = 1$.*

Demonstração

Seja $\alpha = a + bi$, com $a, b \in \mathbb{Z}$. Se α é uma unidade de $\mathbb{Z}(i)$, então existe $\beta \in \mathbb{Z}(i)$, tal que $\alpha\beta = 1$. Então, $1 = \mathrm{N}(1) = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$.

Como $\mathrm{N}(\alpha)$ e $\mathrm{N}(\beta)$ são números inteiros não negativos, temos que $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 1$. Logo, $\mathrm{N}(\alpha) = 1$.

Reciprocamente, se $\mathrm{N}(\alpha) = 1$, então existem inteiros a, b tais que $1 = \mathrm{N}(\alpha) = a^2 + b^2$. Logo, $(a + bi)(a - bi) = a^2 + b^2 = 1$, pelo que $a + bi$ é invertível e, por isso, uma unidade de $\mathbb{Z}(i)$.

Observe-se que se tivermos $a^2 + b^2 = 1$, então teremos forçosamente $a = 0, b = \pm 1$ ou $b = 0, a = \pm 1$.

Logo, as unidades de $\mathbb{Z}(i)$ são $\pm 1, \pm i$, todas elas da forma i^m, com $m \in \mathbb{Z}$.

Observação

Sejam $z, w \in \mathbb{Z}(i)$. Vimos que w divide z, se existir v pertencente a $\mathbb{Z}(i)$, tal que $wv = z$.

Observemos que se w divide z, então $\mathrm{N}(w)$ divide $\mathrm{N}(z)$, mas o recíproco não é válido, pois, por exemplo, $\mathrm{N}(2 + i)$ divide $\mathrm{N}(2 - i)$ e, no entanto, $2 + i$ não divide $2 - i$.

Definição 135 *Para cada número real x, define-se o número inteiro $\widetilde{x}$ como sendo $\widetilde{x} = \mathrm{arr}(x) = \left\lfloor x + \frac{1}{2} \right\rfloor$, onde $\lfloor y \rfloor$ é o maior número inteiro não superior a y.*

Esta função arredonda um dado número real para o inteiro mais próximo, a menos que o número a arredondar esteja equidistante de dois inteiros consecutivos, caso em que o arredondamento é feito por excesso.

Definição 136 *Sejam $z, w \in \mathbb{Z}(i)$, com $w \neq 0$ e $v \in \mathbb{C}$, tal que $v = \frac{z}{w} = x + yi$, com $x, y \in \mathbb{R}$. Sejam $q, r \in \mathbb{Z}(i)$, tais que $q = \widetilde{x} + \widetilde{y}i$ e $r = w\left((x - \widetilde{x}) + (y - \widetilde{y})\,i\right)$. Divisão inteira de z por w é a operação que, pelo processo agora descrito, determina os inteiros gaussianos q e r (chamados quociente e resto), e que satisfazem a condição $z = qw + r$.*

Exemplo 137 *Calculemos o quociente e o resto da divisão inteira de $20 + 3i$ por $4 + 5i$.*

Para isso, começamos por dividir, em $\mathbb{C}$, $20 + 3i$ por $4 + 5i$:

$$\frac{20 + 3i}{4 + 5i} = \frac{(20 + 3i)(4 - 5i)}{(4 + 5i)(4 - 5i)} = \frac{80 - 100i + 12i - 15i^2}{16 + 25} = \frac{95}{41} - \frac{88}{41}i$$

Então, na divisão inteira de $20 + 3i$ por $4 + 5i$, o quociente é dado por $2 - 2i$ (que se obtém, arredondando $\frac{95}{41}$ e $-\frac{88}{41}$), enquanto que o resto é dado por $r = z - qw = 20 + 3i - (2 - 2i)(4 + 5i) = 20 + 3i - 8 - 10i + 8i + 10i^2$. Então, $r = 2 + i$.

Observe-se que r pode ser dado por:

$$\begin{aligned} r &= \left(\left(\frac{95}{41} - 2\right) + \left(-\frac{88}{41} + 2\right)i\right)(4 + 5i) = \left(\frac{13}{41} - \frac{6}{41}i\right)(4 + 5i) \\ &= \frac{52}{41} + \frac{65}{41}i - \frac{24}{41}i - \frac{30}{41}i^2 = \frac{82}{41} + \frac{41}{41}i = 2 + i \end{aligned}$$

Proposição 138 *Sejam $z, w \in \mathbb{Z}(i)$, com $w \neq 0$. Então, com a notação introduzida, verificam-se as condições $(x - \widetilde{x})^2 + (y - \widetilde{y})^2 \leq \frac{1}{2}$ e $\mathrm{N}(r) \leq \frac{1}{2}\,\mathrm{N}(w)$.*

Demonstração
Como $\frac{z}{w} = x + yi = \widetilde{x} + (x - \widetilde{x}) + (\widetilde{y} + (y - \widetilde{y}))\, i$, temos:

$$z = w\,(x + yi) = w\,(\widetilde{x} + (x - \widetilde{x}) + (\widetilde{y} + (y - \widetilde{y}))\, i) = w\,(\widetilde{x} + \widetilde{y}i) + w\,((x - \widetilde{x}) + (y - \widetilde{y})\, i)$$

Então, $z - w\,(\widetilde{x} + \widetilde{y}i) = w\,((x - \widetilde{x}) + (y - \widetilde{y})\, i) = r \in \mathbb{Z}\,(i)$.
Como $|x - \widetilde{x}| \leq \frac{1}{2}$ e $|y - \widetilde{y}| \leq \frac{1}{2}$, então $(x - \widetilde{x})^2 + (y - \widetilde{y})^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, donde se conclui que $\mathrm{N}\,(r) \leq \frac{1}{2}\,\mathrm{N}\,(w)$.
Finalmente, observe-se que w divide z, se e só se, $\mathrm{N}\,(r) = 0$.

Proposição 139 *Seja $z = x + yi$, com $x, y \in \mathbb{Z}$, tais que p é primo, $p \equiv 1 \pmod 4$ e p divide $\mathrm{N}\,(z)$. Sejam $a, b \in \mathbb{N}$, tais que $p = a^2 + b^2$. Então, em $\mathbb{Z}\,(i)$, $a + bi$ divide $x + yi$ ou $a + bi$ divide $x - yi$.*

Demonstração

$$\frac{x + yi}{a + bi} = \frac{(x + yi)\,(a - bi)}{(a + bi)\,(a - bi)} = \frac{ax - bxi + ayi - byi^2}{a^2 + b^2} = \frac{ax + by}{p} + \frac{ay - bx}{p}i$$

$$\frac{x - yi}{a + bi} = \frac{(x - yi)\,(a - bi)}{(a + bi)\,(a - bi)} = \frac{ax - bxi - ayi + byi^2}{a^2 + b^2} = \frac{ax - by}{p} - \frac{ay + bx}{p}i$$

Vamos provar que, nas condições do enunciado, p divide $ax + by$ se e só se p divide $ay - bx$.

$$\begin{aligned}
\left\{ \begin{array}{l} p \,|ax + by \\ p = a^2 + b^2 \end{array} \right. \quad &\Longrightarrow \quad \left\{ \begin{array}{l} p \,\Big|(ax + by)^2 \\ p \,\Big|\left(a^2 + b^2\right)\left(x^2 + y^2\right) \end{array} \right. \\
&\Longrightarrow \quad \left\{ \begin{array}{l} p \,\Big|a^2x^2 + 2abxy + b^2y^2 \\ p \,\Big|a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2 \end{array} \right. \\
&\Longrightarrow \quad p \,\Big|a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2 - a^2x^2 - 2abxy - b^2y^2 \\
&\Longrightarrow \quad p \,\Big|a^2y^2 + b^2x^2 - 2abxy \\
&\Longrightarrow \quad p \,\Big|(ay - bx)^2 \implies p \,|ay - bx
\end{aligned}$$

Reciprocamente:

$$\begin{aligned}
\left\{ \begin{array}{l} p \,|ay - bx \\ p = a^2 + b^2 \end{array} \right. \quad &\Longrightarrow \quad \left\{ \begin{array}{l} p \,\Big|(ay - bx)^2 \\ p \,\Big|\left(a^2 + b^2\right)\left(x^2 + y^2\right) \end{array} \right. \\
&\Longrightarrow \quad \left\{ \begin{array}{l} p \,\Big|a^2y^2 - 2abxy + b^2x^2 \\ p \,\Big|a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2 \end{array} \right. \\
&\Longrightarrow \quad p \,\Big|a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2 - a^2y^2 + 2abxy - b^2x^2 \\
&\Longrightarrow \quad p \,\Big|a^2x^2 + b^2y^2 + 2abxy \\
&\Longrightarrow \quad p \,\Big|(ax + by)^2 \\
&\Longrightarrow \quad p \,|ax + by
\end{aligned}$$

Logo, nas condições do enunciado, p a parte real de $\frac{x+yi}{a+bi}$ é um número inteiro, se e só se, a parte imaginária de $\frac{x+yi}{a+bi}$ também é. Analogamente se mostrava que a parte real de $\frac{x-yi}{a+bi}$ é um número inteiro, se e só se, a parte imaginária de $\frac{x-yi}{a+bi}$ também é.

Mas, por hipótese, $p = a^2+b^2$ e p divide $\mathrm{N}(z) = x^2+y^2$. Então, p divide $\left(a^2+b^2\right)x^2 - b^2\left(x^2+y^2\right)$.

$$\begin{aligned} p \left| \left(a^2+b^2\right)x^2 - b^2\left(x^2+y^2\right) \right. &\implies p \left| a^2x^2 + b^2x^2 - b^2x^2 - b^2y^2 \right. \\ &\implies p \left| a^2x^2 - b^2y^2 \right. \\ &\implies p \left| (ax+by)(ax-by) \right. \\ &\implies p \left| ax+by \vee p \right| ax-by \end{aligned}$$

Se $p \left| ax+by \right.$, então $p \left| ay-bx \right.$, donde se conclui que $\frac{x+yi}{a+bi} \in \mathbb{Z}(i)$.
Se $p \left| ax-by \right.$, então $p \left| ay+bx \right.$, donde se conclui que $\frac{x-yi}{a+bi} \in \mathbb{Z}(i)$.
Então, $a+bi$ é primo em $\mathbb{Z}(i)$.

Proposição 140 *Seja $p \in \mathbb{N}$, um número primo, tal que $p \equiv 1 \pmod 4$. Sejam $a, b \in \mathbb{Z}$, tais que $p = a^2+b^2$. Então, $a+bi$ e $a-bi$ são primos em $\mathbb{Z}(i)$.*

Demonstração
Suponhamos que $a+bi$ divide z_1z_2, com $z_1, z_2 \in \mathbb{Z}(i)$. Dividindo z_1 e z_2 por $a+bi$, temos

$$\begin{cases} z_1 = (a+bi)w_1 + r_1, \text{ com } w_1, r_1 \in \mathbb{Z}(i) \text{ e } 0 \leq \mathrm{N}(r_1) \leq \frac{p}{2} \\ z_2 = (a+bi)w_2 + r_2, \text{ com } w_2, r_2 \in \mathbb{Z}(i) \text{ e } 0 \leq \mathrm{N}(r_2) \leq \frac{p}{2} \end{cases}$$

Então,

$$\begin{aligned} z_1z_2 &= ((a+bi)w_1 + r_1) \times ((a+bi)w_2 + r_2) \\ &= (a+bi)^2 w_1w_2 + (a+bi)w_1r_2 + (a+bi)w_2r_1 + r_1r_2 \end{aligned}$$

Então, $r_1r_2 = z_1z_2 - (a+bi)^2 w_1w_2 - (a+bi)w_1r_2 - (a+bi)w_2r_1$.
Então, $a+bi$ divide r_1r_2, porque $a+bi$ divide todas as parcelas do segundo membro da igualdade anterior.
Então, $\mathrm{N}(a+bi)$ divide $\mathrm{N}(r_1r_2) = \mathrm{N}(r_1)\mathrm{N}(r_2)$, ou seja, p divide $\mathrm{N}(r_1)$ ou p divide $\mathrm{N}(r_2)$.
Então, $\mathrm{N}(r_1) = 0$ ou $\mathrm{N}(r_2) = 0$, donde se conclui que $r_1 = 0$ ou $r_2 = 0$. Logo, $a+bi$ divide z_1 ou $a+bi$ divide z_2.
Observemos que p divide o produto $(a+bi)(a-bi)$ e p não divide nenhum dos dois factores. Então p, como elemento de $\mathbb{Z}(i)$, não é primo.

Proposição 141 *Seja $q \in \mathbb{N}$, um número primo, com $q \equiv 3 \pmod 4$. Então, q é irredutível em $\mathbb{Z}(i)$.*

Demonstração
Suponhamos que $q = z_1z_2$, com z_1 e z_2 não invertíveis. Ora, $\mathrm{N}(q) = q^2 = \mathrm{N}(z_1)\mathrm{N}(z_2)$. Então, teria de ser $\mathrm{N}(z_1) = \mathrm{N}(z_2) = q$, pelo que q seria uma soma de dois quadrados, o que sabemos ser falso. Logo, $\mathrm{N}(z_1) = 1$ ou $\mathrm{N}(z_2) = 1$
Logo, se q se decompuser num produto de dois elementos de $\mathbb{Z}(i)$, um desses elementos é uma unidade (por ter norma 1).
Então, q é irredutível em $\mathbb{Z}(i)$.

Proposição 142 *Seja $q \in \mathbb{N}$, um número primo, tal que $q \equiv 3 \pmod 4$. Então, q é primo em $\mathbb{Z}(i)$.*

Demonstração
Sejam $z_1 = x_1 + y_1 i$ e $z_2 = x_2 + y_2 i$, com $x_1, y_1, x_2, y_2 \in \mathbb{Z}$.
Suponhamos que q divide o produto $z_1 z_2$.

$$\begin{aligned}
q \,|z_1 z_2 &\implies q \,|(x_1 + y_1 i)\,(x_2 + y_2 i) \\
&\implies q \,|x_1 x_2 + x_1 y_2 i + x_2 y_1 i - y_1 y_2 \\
&\implies q \,|x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1)\, i \\
&\implies \begin{cases} q \,|x_1 x_2 - y_1 y_2 \\ q \,|x_1 y_2 + x_2 y_1 \end{cases} \\
&\implies \begin{cases} q \,|x_1^2 x_2 - x_1 y_1 y_2 \\ q \,|x_1 y_1 y_2 + x_2 y_1^2 \end{cases} \\
&\implies q \,|x_1^2 x_2 - x_1 y_1 y_2 + x_1 y_1 y_2 + x_2 y_1^2 \\
&\implies q \,|x_1^2 x_2 + x_2 y_1^2 \\
&\implies q \,|x_2 \left(x_1^2 + y_1^2\right) \\
&\implies q \,|x_2 \vee q \,|x_1^2 + y_1^2
\end{aligned}$$

1^o Caso: Suponhamos que q divide x_2 (em $\mathbb{Z}$). Então, temos

$$\begin{aligned}
\begin{cases} q \,|x_1 x_2 - y_1 y_2 \\ q \,|x_1 y_2 + x_2 y_1 \\ q \,|x_2 \end{cases} &\implies \begin{cases} q \,|y_1 y_2 \\ q \,|x_1 y_2 \\ q \,|x_2 \end{cases} \implies \begin{cases} q \,|y_1 \vee q \,|y_2 \\ q \,|x_1 \vee q \,|y_2 \\ q \,|x_2 \end{cases} \\
&\implies \begin{cases} q \,|y_1 \\ q \,|x_1 \end{cases} \vee \begin{cases} q \,|y_1 \\ q \,|y_2 \end{cases} \vee \begin{cases} q \,|y_2 \\ q \,|x_1 \end{cases} \vee \begin{cases} q \,|y_1 \\ q \,|y_2 \\ q \,|x_2 \end{cases} \\
&\implies q \,|z_1 \vee q \,|z_2
\end{aligned}$$

2^o Caso: Suponhamos que q divide $x_1^2 + y_1^2$ e que q não divide x_2. Seja d o máximo divisor comum entre x_1 e y_1.

Se q divide d, então q divide x_1 e divide x_2, pelo que q divide z_1.

Se q não divide d, então q divide $u^2 + v^2$, com $u = \frac{x_1}{d}$ e $v = \frac{y_1}{d}$. Mas esta hipótese não pode ocorrer, porque $q \equiv 3 \,(\mathrm{mod}\, 4)$ e o máximo divisor comum entre u e v é 1.

Está, assim, terminada a demonstração.

Proposição 143 *O elemento $1 + i$ é primo e irredutível em $\mathbb{Z}\,(i)$.*

Demonstração
Suponhamos que $1 + i = z_1 z_2$, com $z_1, z_2 \in \mathbb{Z}\,(i)$. Então, $2 = \mathrm{N}\,(1 + i) = \mathrm{N}\,(z_1 z_2) = \mathrm{N}\,(z_1)\,\mathrm{N}\,(z_2)$. Então, $\mathrm{N}\,(z_1) = 1 \vee \mathrm{N}\,(z_2) = 1$. Logo, um dos números z_1 e z_2 é uma unidade, pelo que $1+i$ é irredutível em $\mathbb{Z}\,(i)$.

Suponhamos, agora, que $1+i$ divide $z_1 z_2$, com $z_1, z_2 \in \mathbb{Z}\,(i)$. Então, $2 = \mathrm{N}\,(1 + i)$ divide $\mathrm{N}\,(z_1)\,\mathrm{N}\,(z_2)$, pelo que 2 divide uma das normas. Sem perda de generalidade, suponhamos que 2 divide $\mathrm{N}\,(z_1)$. Seja $z_1 = a + bi$, com $a, b \in \mathbb{Z}$. Então, 2 é um divisor de $a^2 + b^2$, pelo que a e b são ambos pares ou ambos ímpares. Se forem ambos pares, 2 divide z_1, pelo que $1 + i$ divide z_1, uma vez que $1 + i$ divide 2.

Suponhamos que a e b são ambos ímpares. Mas,

$$\frac{a + bi}{1 + i} = \frac{(a + bi)\,(1 - i)}{(1 + i)\,(1 - i)} = \frac{a - ai + bi + b}{(1 + i)\,(1 - i)} = \frac{a + b}{2} + \frac{b - a}{2} i$$

Então, $\frac{a+bi}{1+i} \in \mathbb{Z}(i)$, porque $a+b$ e $b-a$ são pares.

Logo, $1+i$ é primo em $\mathbb{Z}(i)$.

Em face das proposições anteriores, podemos concluir que um elemento de $\mathbb{Z}(i)$ é irredutível se e só se é primo.

Podemos concluir, ainda, que os primos de $\mathbb{Z}(i)$ são $1+i$, os primos de $\mathbb{N}$ que são congruentes com 3, módulo 4, e os elementos $a+bi$ e $a-bi$, tais que $a, b \in \mathbb{Z}$ e $a^2+b^2 = p$, com p primo em $\mathbb{N}$ e p congruente com 1, módulo 4 e, ainda, os respectivos associados.

Finalmente observe-se que, num Anel com identidade, todo o primo é irredutível, mas há Anéis com identidade em que nem todo o irredutível é primo.

Proposição 144 *Seja $p \in \mathbb{N}$ um número primo tal que $p \equiv 1 \pmod 4$. Então, existem $a, b \in \mathbb{N}$, tais que $a^2+b^2 = p$.*

Demonstração

Se $p \equiv 1 \pmod 4$, então 4 divide $p-1$. Como $\mathbb{Z}_p \setminus \{0\}$ é um grupo cíclico para a multiplicação (ver Teorema das raízes Primitivas), então existe em $\mathbb{Z}_p \setminus \{0\}$ um elemento m de ordem 4. Então, m^2 tem ordem 2, pelo que $m^2 \equiv -1 \pmod p$, donde vem que p divide m^2+1 (em $\mathbb{N}$). Logo, p divide m^2+1, em $\mathbb{Z}(i)$, ou seja, p divide $(m+i)(m-i)$.

Se p fosse irredutível em $\mathbb{Z}(i)$, então p dividia $m+i$ ou p dividia $m-i$, o que não acontece. Então, p não é irredutível em $\mathbb{Z}(i)$, pelo que existem $a, b, c, d \in \mathbb{Z}$, tais que $p = (a+bi)(c+di) = (ac-bd)+(ad+bc)i$, tendo-se que $a+bi$ e $c+di$ não são unidades. Como a norma de p é p^2, então as normas de $a+bi$ e $c+di$ são iguais a p. Então, $p = a^2+b^2 = c^2+d^2$.

Capítulo 4

Ternos Pitagóricos

Nota histórica

A existência de triângulos rectângulos, em que as medidas dos comprimentos dos lados são números inteiros, era do conhecimento dos Babilónios há cerca de 4000 anos.

Pensa-se, mesmo, que se os Babilónios não conheciam uma fórmula para todos os triângulos rectângulos de lados inteiros, pelo menos, deveriam conhecer fórmulas parciais para tal questão.

Alguns desses triângulos rectângulos de lados inteiros, também eram do conhecimento dos antigos Egípcios e Chineses.

Julga-se que Pitágoras conhecia os ternos Pitagóricos da forma $\left(2n+1, 2n^2+2n, 2n^2+2n+1\right)$, mas é a Diophantus de Alexandria que é atribuída a descoberta da fórmula geral dos ternos Pitagóricos.

Curiosamente, embora parte da obra de Diophantus seja bem conhecida, através de traduções para Árabe, não se sabe em que época o mesmo viveu, acreditando alguns historiadores que terá sido entre os séculos II antes de Cristo e III depois de Cristo, mas sem precisar a época exacta.

Tal como os babilónios, Diophantus considerava, não só triângulos rectângulos de lados inteiros, mas também triângulos rectângulos de lados racionais.

É bem conhecido o facto de Pierre de Fermat ser um estudioso da obra de Diophantus e de ter sido na margem duma página dum dos livros de Diophantus, que Fermat escreveu o enunciado do famoso último Teorema de Fermat, que só muito recentemente foi demonstrado.

O último Teorema de Fermat deve ter sido o teorema da Matemática que mais tempo demorou a demonstrar.

4.1 Fórmula geral dos Ternos Pitagóricos.

Definição 145 *Sejam $x, y, z \in \mathbb{N}$. Se $x^2 + y^2 = z^2$, dizemos que (x, y, z) é um terno Pitagórico (TP); terno Pitagórico primitivo (TPP) é um terno Pitagórico (x, y, z) tal que* $\operatorname{mdc}(x, y, z) = 1$.

Exemplo 146 $(3, 4, 5)$ *é um terno Pitagórico primitivo, porque* $3^2 + 4^2 = 5^2$ *e* $\operatorname{mdc}(3, 4, 5) = 1$. *Já* $(6, 8, 10)$ *é um terno Pitagórico não primitivo, porque* $6^2 + 8^2 = 10^2$, *mas* $\operatorname{mdc}(6, 8, 10) = 2$.

Interpretação geométrica

A cada terno Pitagórico (x, y, z) corresponde "um"triângulo rectângulo em que x e y são os catetos e z é a hipotenusa. Se (x, y, z) é um terno Pitagórico, então, para cada $k \in \mathbb{N}$, temos que (kx, ky, kz) é um terno Pitagórico. Observe-se que os triângulos rectângulos correspondentes aos ternos Pitagóricos (x, y, z) e (kx, ky, kz) são semelhantes.

Vejamos como determinar todos os ternos Pitagóricos, começando por alguns casos de ternos Pitagóricos primitivos:

Exemplo 147 *Ternos Pitagóricos primitivos da forma* $(y, x, x+1)$

Se $(y, x, x+1)$ é um terno Pitagórico, então

$$(x+1)^2 = y^2 + x^2 \iff x^2 + 2x + 1 = y^2 + x^2 \iff 2x + 1 = y^2$$

Logo y é ímpar, pelo que existe um número natural n, tal que $y = 2n + 1$. Então,

$$2x + 1 = (2n+1)^2 \iff 2x + 1 = 4n^2 + 4n + 1 \iff x = 2n^2 + 2n \iff x = 2n(n+1)$$

Então, $y = 2n + 1, x = 2n^2 + 2n, x + 1 = 2n^2 + 2n + 1$
Como $\text{mdc}(x, x+1) = 1$, então $\text{mdc}\left(2n+1, 2n^2+2n, 2n^2+2n+1\right) = 1$.
Logo, $\left(2n+1, 2n^2+2n, 2n^2+2n+1\right)$ é um terno Pitagórico primitivo, para qualquer valor de n.
Logo há infinitos ternos Pitagóricos da forma $(y, x, x+1)$. Alguns desses ternos Pitagóricos estão na tabela seguinte:

n	$2n+1$	$2n^2+2n$	$2n^2+2n+1$	TPP
1	3	4	5	$(3, 4, 5)$
2	5	12	13	$(5, 12, 13)$
3	7	24	25	$(7, 24, 25)$
4	9	40	41	$(9, 40, 41)$
5	11	60	61	$(11, 60, 61)$
6	13	84	85	$(13, 84, 85)$

Exemplo 148 *Ternos Pitagóricos primitivos da forma* $(y, x, x+2)$

Se $(y, x, x+2)$ é um terno Pitagórico, então

$$(x+2)^2 = y^2 + x^2 \iff x^2 + 4x + 4 = y^2 + x^2 \iff 4(x+1) = y^2$$

Logo y é par, pelo que existe um número natural m, tal que $y = 2m$. Então, $4(x+1) = 4m^2$, donde vem $x + 1 = m^2$. Se x fosse par, então y, x e $x + 2$ eram pares, pelo que $(y, x, x+2)$ não era um terno Pitagórico primitivo. Então, x deve ser ímpar, pelo que m é par. Então, $m = 2n$, para certo natural n. Então, $x + 1 = 4n^2$, donde se conclui que $x = 4n^2 - 1$ e $x + 2 = 4n^2 + 1$
Como x é ímpar, $\text{mdc}(x, x+2) = 1$, pelo que $\text{mdc}\left(4n, 4n^2-1, 4n^2+1\right) = 1$.
Então, $\left(4n, 4n^2-1, 4n^2+1\right)$ é um terno Pitagórico primitivo, para qualquer valor de n.
Logo há infinitos ternos Pitagóricos da forma $(y, x, x+1)$. Alguns desses ternos Pitagóricos estão na tabela seguinte:

n	$4n$	$4n^2-1$	$4n^2+1$	TPP
1	4	3	5	$(4, 3, 5)$
2	8	15	17	$(8, 15, 17)$
3	12	35	37	$(12, 35, 37)$
4	16	63	65	$(16, 63, 65)$
5	20	99	101	$(20, 99, 101)$
6	24	143	145	$(24, 143, 145)$
7	28	195	197	$(28, 195, 197)$

Exemplo 149 *Ternos Pitagóricos primitivos da forma* $(y, x, x+3)$

Se $(y, x, x+3)$ é um terno Pitagórico, então

$$(x+3)^2 = y^2 + x^2 \iff x^2 + 6x + 9 = y^2 + x^2 \iff 3(2x+3) = y^2$$

Logo y é múltiplo de 3, pelo que existe um número natural m, tal que $y = 3m$. Então, $3(2x+3) = 9m^2$, donde vem $2x + 3 = 3m^2$.

Então, $2x$ tem de ser múltiplo de 3, o mesmo acontecendo com x. Então y, x e $x+3$ são todos múltiplos de 3, pelo que não há ternos Pitagóricos primitivos da forma $(y, x, x+3)$.

Torna-se pertinente a questão de saber para que valores de a existem ternos Pitagóricos da forma $(y, x, x+a)$.

A essa questão daremos resposta nas proposições seguintes.

Proposição 150 *Seja p um primo ímpar. Então não há nenhum terno Pitagórico da forma $(y, x, x+p)$.*

Demonstração

Se $(y, x, x+p)$ é um terno Pitagórico, então $(x+p)^2 = y^2 + x^2$.

Logo, $x^2 + 2px + p^2 = y^2 + x^2$, donde vem $p(2x+p) = y^2$.

Então, y é múltiplo de p, pelo que existe um número natural m, tal que $y = pm$.

Então, $p(2x+p) = p^2m^2$, donde vem $2x + p = pm^2$.

Então, $2x$ tem de ser múltiplo de p, o mesmo acontecendo com x. Então y, x e $x+p$ são todos múltiplos de p, pelo que não há ternos Pitagóricos primitivos da forma $(y, x, x+p)$.

Proposição 151 *Seja $a \in \mathbb{N}$, tal que $a > 1$, a é ímpar e a não é quadrado (perfeito). Então não há nenhum TPP da forma $(y, x, x+a)$.*

Demonstração

Seja $a = bp^{2\alpha-1}$, com p primo ímpar, $\alpha, b \in \mathbb{N}$ e b ímpar tal que p não divide b.

De $x^2 + y^2 = x^2 + 2ax + a^2$, vem:

$$y^2 = 2ax + a^2 = a(2x+a) = bp^{2\alpha-1}\left(2x + bp^{2\alpha-1}\right)$$

Daqui vem que p^α divide y, pelo que $y = mp^\alpha$, para certo natural m.

Então, $y^2 = m^2p^{2\alpha} = bp^{2\alpha-1}\left(2x + bp^{2\alpha-1}\right)$.

Logo $m^2p = b\left(2x + bp^{2\alpha-1}\right)$, donde vem que p divide $2x + bp^{2\alpha-1}$. Então, p divide $2x$, pelo que p divide x. Então, $(y, x, x+a)$ não é um terno Pitagórico primitivo.

Proposição 152 *Se $(y, x, x+a)$ é um terno Pitagórico primitivo e a é ímpar, então a é um quadrado perfeito.*

Esta proposição é, apenas, outra maneira de afimar o mesmo que na proposição anterior. Observemos que esta proposição não garante a existência dum terno Pitagórico primitivo da forma $(y, x, x+a)$, se a for ímpar e quadrado perfeito, embora isso aconteça, como veremos na proposição seguinte.

Proposição 153 *Se a é ímpar e quadrado perfeito, então há infinitos ternos Pitagóricos primitivos da forma $(y, x, x+a)$.*

Demonstração

Suponhamos que $a = (2s-1)^2$, para um certo natural s e que existe um terno Pitagórico da forma considerada. Então:

$$y^2 + x^2 = x^2 + 2ax + a^2 \implies y^2 = a(2x+a) \implies y^2 = (2s-1)^2\left(2x + (2s-1)^2\right)$$

Então, $2x + (2s-1)^2$ é um quadrado perfeito ímpar, pelo que existe um número natural n, tal que $2x + (2s-1)^2 = (2n + 2s - 1)^2$.

Então, $2x + (2s-1)^2 = 4n^2 + 4n(2s-1) + (2s-1)^2$, pelo que $2x = 4n^2 + 4n(2s-1)$. Logo, $x = 2n^2 + 2n(2s-1)$.

Substituindo x nas expressões que nos dão y^2 e $x + (2s-1)^2$, obtemos

$$y^2 = (2s-1)^2 \left(2x + (2s-1)^2\right) = (2s-1)^2 (2n + 2s - 1)^2$$

Então, $y = (2s-1)(2n+2s-1) = (n+2s-1-n)(n+2s-1+n) = (n+2s-1)^2 - n^2$.

Logo, $(y, x, x+a) = \left((n+2s-1)^2 - n^2, 2n^2 + 2n(2s-1), 2n^2 + 2n(2s-1) + (2s-1)^2\right)$

Encontrámos, assim, uma expressão geral para os ternos Pitagóricos da forma $\left(y, x, x + (2s-1)^2\right)$. Falta, ainda, mostrar que há infinitos ternos Pitagóricos primitivos desta forma.

Consideremos o terno $\left((n+2s-1)^2 - n^2, 2n^2 + 2n(2s-1), 2n^2 + 2n(2s-1) + (2s-1)^2\right)$.

Vejamos que o terno Pitagórico anterior é um primitivo, se e só se, $\text{mdc}(n, 2s-1) = 1$.

Se o máximo divisor comum entre n e $2s-1$ for diferente de 1, existe um número primo p que divide n e $2s-1$. Então, p divide $(n+2s-1)^2 - n^2$, $n^2 + 2n(2s-1)$ e $2n^2 + 2n(2s-1) + (2s-1)^2$, pelo que $\left((n+2s-1)^2 - n^2, 2n^2 + 2n(2s-1), 2n^2 + 2n(2s-1) + (2s-1)^2\right)$ não é um terno Pitagórico primitivo.

Suponhamos, agora, que $\text{mdc}(n, 2s-1) = 1$.

Seja $d = \text{mdc}\left((n+2s-1)^2 - n^2, 2n^2 + 2n(2s-1), 2n^2 + 2n(2s-1) + (2s-1)^2\right)$.

Como $(n+2s-1)^2 - n^2 = (2s-1)(2n+2s-1)$ é ímpar, então d é ímpar. Suponhamos que $d > 1$. Então, existe um primo ímpar q, tal que q divide os números d, x, y, z. Então, q divide os dois números $z - x = (2s-1)^2$ e $z - y = 2n^2$, isto é, q divide n e q divide $2s-1$. Então, q divide $\text{mdc}(n, 2s-1) = 1$, o que não pode acontecer. Então, é absurdo supor que $d > 1$, pelo que $d = 1$.

Logo, $\left((n+2s-1)^2 - n^2, 2n^2 + 2n(2s-1), 2n^2 + 2n(2s-1) + (2s-1)^2\right)$ é um terno Pitagórico primitivo, para todo o valor de n primo com $2s-1$.

Uma vez que há infinitos números naturais que são primos com $2s-1$, concluimos, como pretendíamos demonstrar, que há infinitos ternos Pitagóricos primitivos da forma $\left(y, x, x + (2s-1)^2\right)$.

Exemplo 154 *Determinar os ternos Pitagóricos primitivos da forma* $(y, x, x+9)$.

Ora,

$$y^2 + x^2 = (x+9)^2 \iff y^2 + x^2 = x^2 + 18x + 91 \iff y^2 = 18x + 81 \iff y^2 = 9(2x+9)$$

E, agora, temos:

$$2x + 9 = (2n+3)^2 \iff 2x + 9 = 4n^2 + 12n + 9 \iff 2x = 4n^2 + 12n \iff x = 2n^2 + 6n$$

Logo, $x = 2n^2 + 6n$, $y = 3(2n+3) = 6n + 9$ e $z = 2n^2 + 6n + 9$.

É claro que, para obtermos os valores anteriores, podíamos ter aproveitado a proposição anterior e respectiva demonstração, bastando substituir por s por 2.

Na tabela seguinte estão indicados alguns dos ternos Pitagóricos primitivos da forma anterior:

n	$6n+9$	$2n^2+6n$	$2n^2+6n+9$	TPP
1	15	8	17	$(15,8,17)$
2	21	20	29	$(21,20,29)$
4	33	56	65	$(33,56,65)$
5	39	80	89	$(39,80,89)$
7	51	140	149	$(51,140,149)$
8	57	176	185	$(57,176,185)$
10	69	260	269	$(69,260,269)$

Reparemos que não aparecem as linhas correspondentes a $n = 3, 6, 9, ...$, porque estes números não são primos com 3.

Proposição 155 *Se (x, y, z) é um terno Pitagórico primitivo, então z é ímpar.*

Demonstração

Suponhamos que z é par. Então, $z^2 = x^2 + y^2$ é par. Então, x^2 e y^2 são ambos pares ou ambos ímpares, o mesmo acontecendo com x e y.

Se x e y são ambos pares, então (x, y, z) não é um terno Pitagórico primitivo.

Se x e y são ambos ímpares, então temos $x = 2t - 1$, $y = 2s - 1$ e $z = 2r$.

Então, $4r^2 = 4t^2 - 4t + 1 + 4s^2 - 4s + 1 = 4t^2 - 4t + 4s^2 - 4s + 2$, donde se conclui que 4 divide 2, o que é falso.

Em qualquer dos casos, obtivemos uma contradição. Logo, é absurdo supor que z é par, pelo que z tem de ser ímpar, pelo que está terminada a demonstração.

Observação

Se z é ímpar, podemos supor, sem perda de generalidade, que x é par e y é ímpar, pelo que $z - x = a$ é ímpar.

A questão de determinar todos os ternos Pitagóricos está resolvida, porque todo o terno Pitagórico pode ser obtido a partir dum TPP, multiplicando os seus elementos por um qualquer número inteiro positivo.

Então, podemos afirmar que todo o terno Pitagórico primitivo é da forma

$$\left((n+2s-1)^2 - n^2, 2n^2 + 2n(2s-1), 2n^2 + 2n(2s-1) + (2s-1)^2\right),$$

tendo-se que os ternos Pitagóricos desta forma são primitivos, se e só se $\text{mdc}(n, 2s-1) = 1$.

Finalmente, a expressão $\left(2ukv, ku^2 - kv^2, ku^2 + kv^2\right)$, com $k, u, v \in \mathbb{N}$ e $u > v$ gera todos os ternos Pitagóricos (à parte a ordem dos dois primeiros elementos dos ternos).

Proposição 156 *Para cada número natural n maior ou igual a 3, existe um terno Pitagórico que inclui n.*

Demonstração

Se n é ímpar e $n \geq 3$, então existe um natural s, tal que $n = 2s + 1$, pelo que nos basta considerar o terno Pitagórico $\left(2s+1, 2s^2+2s, 2s^2+2s+1\right)$.

Se existe um natural s, tal que $n = 4s + 2$, temos o terno Pitagórico $\left(4s+2, 4s^2+4s, 4s^2+4s+2\right)$.

Finalmente, se $n = 4s$, consideramos o terno $(3s, 4s, 5s)$.

Proposição 157 *Sejam $a, b, p \in \mathbb{N}$, com p primo, tais que (a, b, p) é um terno Pitagórico primitivo. Sejam (x_n) e (y_n) as sucessões definidas por* $\begin{cases} x_1 = a, y_1 = b \\ x_{n+1} = ax_n - by_n \\ y_{n+1} = bx_n + ay_n \end{cases}$ *. Então, verificam-se as seguintes propriedades:*

1. $x_{2n} = x_n^2 - y_n^2, y_{2n} = 2x_n y_n, \forall n \in \mathbb{N}$
2. $x_n^2 + y_n^2 = p^{2n}, \forall n \in \mathbb{N}$
3. $\text{mdc}\,(x_n, y_n, p^n) = 1, \forall n \in \mathbb{N}$
4. $(|x_n|, |y_n|, p^n)$ *é um terno Pitagórico primitivo, para todo o natural* n

Demonstração

1. Para $n = 1$, temos $\begin{cases} x_2 = ax_1 - by_1 = a^2 - b^2 = x_1^2 - y_1^2 \\ y_2 = bx_1 + ay_1 = ba + ab = 2x_1 y_1 \end{cases}$

   Hipótese de indução: $x_{2n} = x_n^2 - y_n^2, y_{2n} = 2x_n y_n$

   Tese: $x_{2n+2} = x_{n+1}^2 - y_{n+1}^2, y_{2n+2} = 2x_{n+1} y_{n+1}$

$$\begin{aligned} x_{2n+2} &= ax_{2n+1} - by_{2n+1} = a\,(ax_{2n} - by_{2n}) - b\,(bx_{2n} + ay_{2n}) \\ &= a^2 x_{2n} - aby_{2n} - b^2 x_{2n} - aby_{2n} = a^2 x_{2n} - b^2 x_{2n} - 2aby_{2n} \\ &= \left(a^2 - b^2\right) x_{2n} - 2aby_{2n} = \left(a^2 - b^2\right)\left(x_n^2 - y_n^2\right) - 4abx_n y_n \\ &= a^2 x_n^2 - a^2 y_n^2 - b^2 x_n^2 + b^2 y_n^2 - 2abx_n y_n - 2abx_n y_n \\ &= \left(a^2 x_n^2 - 2abx_n y_n + b^2 y_n^2\right) - \left(a^2 y_n^2 + 2abx_n y_n + b^2 x_n^2\right) \\ &= (ax_n - by_n)^2 - (bx_n + ay_n)^2 = x_{n+1}^2 - y_{n+1}^2 \end{aligned}$$

$$\begin{aligned} y_{2n+2} &= ay_{2n+1} + bx_{2n+1} = a\,(bx_{2n} + ay_{2n}) + b\,(ax_{2n} - by_{2n}) \\ &= abx_{2n} + a^2 y_{2n} + abx_{2n} - b^2 y_{2n} = \left(a^2 - b^2\right) y_{2n} + 2abx_{2n} \\ &= 2\left(a^2 - b^2\right) x_n y_n + 2ab\left(x_n^2 - y_n^2\right) = 2a^2 x_n y_n - 2b^2 x_n y_n + 2abx_n^2 - 2aby_n^2 \\ &= 2ax_n\,(ay_n + bx_n) - 2by_n\,(ay_n + bx_n) = 2ax_n y_{n+1} - 2by_n y_{n+1} \\ &= 2y_{n+1}\,(ax_n - by_n) = 2x_{n+1} y_{n+1} \end{aligned}$$

   Logo, $x_{2n} = x_n^2 - y_n^2, y_{2n} = 2x_n y_n, \forall n \in \mathbb{N}$

2. Para $n = 1$, temos $x_1^2 + y_1^2 = a^2 + b^2 = p^2$, porque (a, b, p) é um terno Pitagórico.

   Hipótese de indução: $x_n^2 + y_n^2 = p^{2n}$

   Tese: $x_{n+1}^2 + y_{n+1}^2 = p^{2n+2}$

$$\begin{aligned} x_{n+1}^2 + y_{n+1}^2 &= (ax_n - by_n)^2 + (ay_n + bx_n)^2 \\ &= a^2 x_n^2 - 2abx_n y_n + b^2 y_n^2 + a^2 y_n^2 + 2abx_n y_n + b^2 x_n^2 \\ &= a^2 x_n^2 + b^2 y_n^2 + a^2 y_n^2 + b^2 x_n^2 = a^2\left(x_n^2 + y_n^2\right) + b^2\left(x_n^2 + y_n^2\right) \\ &= \left(a^2 + b^2\right)\left(x_n^2 + y_n^2\right) = p^2 \times p^{2n} = p^{2n+2} \end{aligned}$$

   Logo, $x_n^2 + y_n^2 = p^{2n}, \forall n \in \mathbb{N}$

3. Comecemos por observar que $\text{mdc}\,(x_n, y_n, p^n) = 1$ se e só se $\text{mdc}\,(x_n, y_n, p) = 1$.

   Para $n = 1$, temos $\text{mdc}\,(x_1, y_1, p) = \text{mdc}\,(a, b, p) = 1$, porque (a, b, p) é um terno Pitagórico primitivo.

Suponhamos que existia $m \in \mathbb{N}$, tal que $\text{mdc}\,(x_m, y_m, p^m) \neq 1$. Então, $\text{mdc}\,(x_m, y_m, p) = p$, pelo que p dividia x_m e p dividia y_m. Então, p dividia x_{m+1} e p dividia y_{m+1}. Então, p dividia x_n e p dividia y_n, para todo o natural n tal que $n \geq m$.

Como $\text{mdc}\,(x_1, y_1, p) = 1$, existiria $t \in \mathbb{N}$, tal que $\text{mdc}\,(x_t, y_t, p) = 1$ e $\text{mdc}\,(x_{t+1}, y_{t+1}, p) = p$.

Então, $\text{mdc}\,(x_{2t}, y_{2t}, p) = p$. Mas:

$$\begin{aligned}
\text{mdc}\,(x_{2t}, y_{2t}, p) = p &\implies p\,|x_{2t} \wedge p\,|y_{2t} \implies p\,\left|x_t^2 - y_t^2 \wedge p\,\right|2x_t y_t \\
&\implies p\,\left|x_t^2 - y_t^2 \wedge (p\,|x_t \vee p\,|y_t\right) \\
&\implies \left(p\,\left|y_t^2 \wedge p\,\right|x_t\right) \vee \left(p\,|y_t \wedge p\,\left|x_t^2\right.\right) \implies p\,|x_t \wedge p\,|y_t
\end{aligned}$$

Então, teríamos $\text{mdc}\,(x_t, y_t, p) = p$, contrariamente à hipótese de que $\text{mdc}\,(x_t, y_t, p) = 1$.

Logo, é absurdo supor que existe $m \in \mathbb{N}$, tal que $\text{mdc}\,(x_m, y_m, p^m) \neq 1$.

Então, $\text{mdc}\,(x_n, y_n, p^n) = 1, \forall n \in \mathbb{N}$

4. A afirmação de que $(|x_n|, |y_n|, p^n)$ é um terno Pitagórico primitivo, para todo o natural n, é uma consequência imediata de 2. e 3.

Proposição 158 *Seja (x, y, z) um terno Pitagórico primitivo. Então, todo o factor primo de z é congruente com 1, módulo 4.*

Demonstração
Já sabemos que z tem de ser ímpar. Seja p um divisor primo de z. Então, p não divide x, nem divide y. Mas,

$$p \mid z \implies p \mid z^2 \implies p \mid x^2 + y^2 \implies x^2 \equiv -y^2 \pmod{p}$$

Então, -1 é resíduo quadrático, módulo p, pelo que $p \equiv 1 \pmod{4}$.

Proposição 159 *Sejam (a, b, c) e (d, e, f) dois ternos Pitagóricos primitivos com $\text{mdc}\,(c, f) = 1$. Então, há pelo menos, dois ternos Pitagóricos primitivos da forma (x, y, cf).*

Demonstração
Consideremos os ternos $(ad + be, |ae - bd|, cf)$ e $(|ad - be|, ae + bd, cf)$.
Ora:

$$\begin{aligned}
(ad + be)^2 + (ae - bd)^2 &= a^2d^2 + 2abde + b^2e^2 + a^2e^2 - 2abde + b^2d^2 \\
&= a^2d^2 + b^2e^2 + a^2e^2 + b^2d^2 = a^2\left(d^2 + e^2\right) + b^2\left(d^2 + e^2\right) \\
&= \left(a^2 + b^2\right)\left(d^2 + e^2\right) = c^2f^2
\end{aligned}$$

Logo, $(ad + be, |ae - bd|, cf)$ é um terno Pitagórico, a menos que se tenha $ae - bd = 0$.
Sem perda de generalidade, podemos supor que $1 < c < f$.
Suponhamos que $ae - bd = 0$. Então, $ad + be = cf$.

$$\begin{aligned}
\begin{cases} ae - bd = 0 \\ ad + be = cf \end{cases} &\implies \begin{cases} ade = bd^2 \\ ade + be^2 = cef \end{cases} \implies bd^2 + be^2 = cef \\
&\implies b\left(d^2 + e^2\right) = cef \implies bf^2 = cef \implies bf = ce
\end{aligned}$$

Então, c divide b, porque $\text{mdc}\,(c, f) = 1$. Mas, $\text{mdc}\,(b, c) = 1$, obtendo-se uma contradição. Então, é absurdo supor $ae - bd = 0$, pelo que

$(ad+be,|ae-bd|,cf)$ é um terno Pitagórico. Falta-nos, ainda, provar que este terno Pitagórico é primitivo.

Suponhamos que existe um número primo p, tal que p divide os números $ad+be$ e $ae-bd$.

$$\begin{aligned}
\left\{\begin{array}{l} p\,|ad+be \\ p\,|ae-bd \end{array}\right. &\implies \left\{\begin{array}{l} p\,\Big|ade+be^2 \\ p\,\Big|-ade+bd^2 \end{array}\right. \implies \left\{\begin{array}{l} p\,\Big|ade+be^2 \\ p\,\Big|-ade+bd^2 \end{array}\right. \\
&\implies p\,\Big|bd^2+be^2 \implies p\,\Big|b\left(d^2+e^2\right) \\
&\implies p\,\Big|bf^2 \implies p\,|b \vee p\,\Big|f^2 \implies p\,|b \vee p\,|f
\end{aligned}$$

Suponhamos que p divide b, além de dividir $ad+be$ e $ae-bd$. Então:

$$\begin{aligned}
\left\{\begin{array}{l} p\,|ad+be \\ p\,|ae-bd \\ p\,|b \end{array}\right. &\implies \left\{\begin{array}{l} p\,|ad \\ p\,|ae \\ p\,|b \end{array}\right. \implies \left\{\begin{array}{l} p\,|a \vee p\,|d \\ p\,|a \vee p\,|e \\ p\,|b \end{array}\right. \\
&\implies \left\{\begin{array}{l} p\,|a \\ p\,|b \end{array}\right. \vee \left\{\begin{array}{l} p\,|a \\ p\,|e \\ p\,|b \end{array}\right. \vee \left\{\begin{array}{l} p\,|d \\ p\,|a \\ p\,|b \end{array}\right. \vee \left\{\begin{array}{l} p\,|d \\ p\,|e \\ p\,|b \end{array}\right. \\
&\implies \left\{\begin{array}{l} p\,|a \\ p\,|b \end{array}\right. \vee \left\{\begin{array}{l} p\,|d \\ p\,|e \end{array}\right.
\end{aligned}$$

Obtivemos, assim, uma contradição, pois no primeiro caso, (a,b,c) não era um terno Pitagórico primitivo e, no segundo caso, (d,e,f) não era um terno Pitagórico primitivo. Então, terá de dividir f.

Suponhamos, então, que p divide f, que p divide $ae-bd$ e que p divide $ad+be$.

$$\begin{aligned}
\left\{\begin{array}{l} p\,|ad+be \\ p\,|ae-bd \\ p\,|f \end{array}\right. &\implies \left\{\begin{array}{l} p\,\Big|a^2d+abe \\ p\,\Big|-abe+b^2d \\ p\,|f \end{array}\right. \implies \left\{\begin{array}{l} p\,\Big|a^2d+b^2d \\ p\,|f \end{array}\right. \\
&\implies \left\{\begin{array}{l} p\,\Big|\left(a^2+b^2\right)d \\ p\,|f \end{array}\right. \implies \left\{\begin{array}{l} p\,\Big|c^2d \\ p\,|f \end{array}\right. \\
&\implies \left\{\begin{array}{l} p\,|c \vee p\,|d \\ p\,|f \end{array}\right. \implies \left\{\begin{array}{l} p\,|c \\ p\,|f \end{array}\right. \vee \left\{\begin{array}{l} p\,|d \\ p\,|f \end{array}\right.
\end{aligned}$$

Em qualquer dos casos obtemos uma contradição.

Logo, é absurdo supor que existe um número primo p, tal que p divide os números $ad+be$ e $ae-bd$.

Logo, $(ad+be,|ae-bd|,cf)$ é um terno Pitagórico primitivo.

Analogamente, se provava que $(|ad-be|,ae+bd,cf)$ é um terno Pitagórico primitivo.

Ainda falta mostrar que os dois ternos são distintos.

Como $ad+be \neq |ad-be|$, basta-nos verificar que $ad+be \neq ae+bd$:

Suponhamos que $ad+be=ae+bd$. Então, $ad-ae+be-bd=0$. Logo, $a\,(d-e)-b\,(d-e)=0$, donde se conclui que $(a-b)\,(d-e)=0$, ou seja, $a=b$ ou $d=e$, o que é uma contradição, pois não há ternos Pitagóricos da forma (x,x,z).

Logo, é absurdo supor que $ad+be=ae+bd$, pelo que os dois ternos Pitagóricos são distintos.

Proposição 160 *Sejam $n,p \in \mathbb{N}$, com p um número primo congruente com 1, módulo 4. Então, à parte a ordem dos dois primeiros elementos, existe um único terno Pitagórico primitivo da forma (x,y,p^n).*

Demonstração

Já sabemos que existe, pelo menos, um terno Pitagórico primitivo da forma (x, y, p^n). Então, $x^2 + y^2 = p^{2n}$. Como $p \equiv 1 \pmod 4$, temos $p = a^2 + b^2$, para certos naturais a e b. Consideremos os inteiros Gaussianos $x + yi$ e $a + bi$.

Como a norma de $x + yi$ é $x^2 + y^2 = p^{2n}$, então um dos inteiros Gaussianos $a + bi$ e $a - bi$ divide $x + yi$.

Mas não pode verificar-se que $a + bi$ e $a - bi$ dividam $x + yi$, pois, nesse caso, teríamos que p dividia $x + yi$, ou seja, p dividia x e p dividia y, pelo que (x, y, p^n) não era um terno Pitagórico primitivo. Suponhamos que $a + bi$ divide $x + yi$.

Então, $x + yi = (a + bi)(x_1 + iy_1)$ e $\mathrm{N}(x_1 + iy_1) = p^{2n-1}$.

E, mais uma vez, $a + bi$ divide $x_1 + iy_1$, pois, se $a - bi$ dividisse $(x_1 + iy_1)$, então p dividia $x + yi$.

A aplicação sucessiva deste raciocínio leva-nos a concluir que temos $x + yi = u(a + bi)^{2n}$, onde u é uma unidade de $\mathbb{Z}(i)$, ou seja, u é um dos quatro números $1, -1, i, -i$. Então, os números naturais x e y estão bem determinados, só havendo duas hipóteses. Na primeira, x é o módulo da parte real de $(a + bi)^{2n}$ e y é o módulo da parte imaginária de $(a + bi)^{2n}$, enquanto que, na segunda hipótese, temos a situação inversa.

Se $a-bi$ divide $x+yi$, chegamos a uma conclusão análoga, pois $(a - bi)^{2n}$ é o conjugado de $(a + bi)^{2n}$.

É claro que se tivéssemos considerado o número $y + xi$, em vez de $x + yi$, a conclusão seria a mesma.

Fica, assim, provado que, à parte a ordem de x e y, há um único terno Pitagórico da forma (x, y, p^n).

Proposição 161 *Sejam $p_1, ..., p_k$, k números primos congruentes com 1, módulo 4, distintos dois a dois. Sejam $n_1, ..., n_k \in \mathbb{N}$. Então, à parte a ordem dos números x e y, há, exactamente, 2^{k-1} ternos Pitagóricos primitivos da forma $\left(x, y, p_1^{n_1} ... p_k^{n_k}\right)$.*

Exemplo 162 *Vejamos como obter os ternos Pitagóricos primitivos da forma $\left(x, y, 5^4 \times 13^3 \times 17^2\right)$, ou seja, da forma$(x, y, 396\,833\,125)$:*

Como $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$ e $17 = 4^2 + 1^2$, começamos por calcular $(2 + i)^8$, $(3 + 2i)^6$ e $(4 + i)^4$:
$(2 + i)^8 = (3 + 4i)^4 = (-7 + 24i)^2 = -527 - 336i$
$(3 + 2i)^6 = (5 + 12i)^3 = (5 + 12i)(-119 + 120i) = -2035 - 828i$
$(4 + i)^4 = (15 + 8i)^2 = 225 + 240i - 64 = 161 + 240i$
E, agora, calculamos:

$$\begin{aligned}(2 + i)^8 (3 + 2i)^6 (4 + i)^4 &= (-527 - 336i)(-2035 - 828i)(161 + 240i) \\ &= (794\,237 + 1120\,116i)(161 + 240i) = -140\,955\,683 + 370\,955\,556i\end{aligned}$$

E, deste modo, obtivemos $(140\,955\,683, 370\,955\,556, 396\,833\,125)$, um dos ternos Pitagóricos primitivos procurados.

$$\begin{aligned}(2 + i)^8 (3 + 2i)^6 (4 - i)^4 &= (-527 - 336i)(-2035 - 828i)(161 - 240i) \\ &= (794\,237 + 1120\,116i)(161 - 240i) = 396\,699\,997 - 10\,278\,204i\end{aligned}$$

E, desta vez, obtivemos $(396\,699\,997, 10\,278\,204, 396\,833\,125)$, outro dos ternos Pitagóricos primitivos procurados.

$$\begin{aligned}(2 + i)^8 (3 - 2i)^6 (4 + i)^4 &= (-527 - 336i)(-2035 + 828i)(161 + 240i) \\ &= (1350\,653 + 247\,404i)(161 + 240i) = 158\,078\,173 + 363\,988\,764i\end{aligned}$$

E, assim, obtivemos $(158\,078\,173, 363\,988\,764, 396\,833\,125)$.

$$\begin{aligned}(2+i)^8(3-2i)^6(4-i)^4 &= (-527-336i)(-2035+828i)(161-240i)\\ &= (1350\,653+247\,404i)(161-240i) = 276\,832\,093-284\,324\,676i\end{aligned}$$

E, assim, obtivemos $(276\,832\,093, 284\,324\,676, 396\,833\,125)$, o útimo terno Pitagórico procurado.

Se pretendermos distinguir a ordem dos dois primeiros elementos dos ternos Pitagóricos primitivos da forma $(x, y, 396\,833\,125)$, temos os oito ternos:

$(140\,955\,683, 370\,955\,556, 396\,833\,125)$	$(370\,955\,556, 140\,955\,683, 396\,833\,125)$
$(10\,278\,204, 396\,699\,997, 396\,833\,125)$	$(396\,699\,997, 10\,278\,204, 396\,833\,125)$
$(158\,078\,173, 363\,988\,764, 396\,833\,125)$	$(363\,988\,764, 158\,078\,173, 396\,833\,125)$
$(276\,832\,093, 284\,324\,676, 396\,833\,125)$	$(284\,324\,676, 276\,832\,093, 396\,833\,125)$

4.2 A trigonometria e os ternos Pitagóricos

Vamos, agora, abordar o tema dos ternos Pitagóricos ao nível de 12^o Ano, utilizando conhecimentos elementares de trigonometria.

Consideremos o terno Pitagórico $(3, 4, 5)$. Da igualdade $3^2+4^2 = 25$, podemos obter a nova igualdade $\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$, que nos faz recordar a fórmula fundamental da trigonometria. Concluimos, então, que existe um número real α, tal que $\cos\alpha = \frac{3}{5}$ e $\sin\alpha = \frac{4}{5}$.

Então, $\begin{cases} \cos(2\alpha) = \cos^2\alpha - \sin^2\alpha = \frac{9}{25} - \frac{16}{25} = -\frac{7}{25} \\ \sin(2\alpha) = 2\sin\alpha\cos\alpha = 2\times\frac{3}{5}\times\frac{4}{5} = \frac{24}{25} \end{cases}$

E como $\cos^2(2\alpha) + \sin^2(2\alpha) = 1$, temos que $\left(-\frac{7}{25}\right)^2 + \left(\frac{24}{25}\right)^2 = 1$.

Da igualdade anterior vem que $7^2 + 24^2 = 25^2$, ou seja, $(7, 24, 25)$ é um novo terno Pitagórico (primitivo).

E podemos continuar, de modo a obter mais ternos Pitagóricos primitivos:

$\begin{cases} \cos(3\alpha) = \cos(2\alpha)\cos\alpha - \sin(2\alpha)\sin\alpha = -\frac{7}{25}\times\frac{3}{5} - \frac{24}{25}\times\frac{4}{5} = -\frac{117}{125} \\ \sin(3\alpha) = \sin(2\alpha)\cos\alpha + \sin\alpha\cos(2\alpha) = \frac{24}{25}\times\frac{3}{5} - \frac{4}{5}\times\frac{7}{25} = \frac{44}{125} \end{cases}$

Das igualdades anteriores, obtemos o ternos Pitagórico primitivo $(44, 117, 125)$.

$\begin{cases} \cos(4\alpha) = \cos^2(2\alpha) - \sin^2(2\alpha) = \frac{49}{625} - \frac{576}{625} = -\frac{527}{625} \\ \sin(4\alpha) = 2\sin(2\alpha)\cos(2\alpha) = 2\times\frac{24}{25}\times\left(-\frac{7}{25}\right) = -\frac{336}{625} \end{cases}$

Das igualdades anteriores, obtemos o ternos Pitagórico primitivo $(336, 527, 625)$.

$\begin{cases} \cos(5\alpha) = \cos(4\alpha)\cos\alpha - \sin(4\alpha)\sin\alpha = -\frac{527}{625}\times\frac{3}{5} + \frac{336}{625}\times\frac{4}{5} = -\frac{237}{3125} \\ \sin(5\alpha) = \sin(4\alpha)\cos\alpha + \sin\alpha\cos(4\alpha) = -\frac{336}{625}\times\frac{3}{5} - \frac{4}{5}\times\frac{527}{625} = -\frac{3116}{3125} \end{cases}$

Das igualdades anteriores, obtemos o ternos Pitagórico primitivo $(237, 3116, 3125)$.

Mas podemos ir mais além: Suponhamos que, pelo processo anterior, temos os números x_n e y_n, dados por $\begin{cases} \cos(n\alpha) = \frac{x_n}{5^n} \\ \sin(n\alpha) = \frac{y_n}{5^n} \end{cases}$.

Então, temos:

$\begin{cases} \cos((n+1)\alpha) = \cos(n\alpha)\cos\alpha - \sin(n\alpha)\sin\alpha = \frac{3}{5}\times\frac{x_n}{5^n} - \frac{4}{5}\times\frac{y_n}{5^n} \\ \sin((n+1)\alpha) = \sin(n\alpha)\cos\alpha + \sin\alpha\cos(n\alpha) = \frac{3}{5}\times\frac{y_n}{5^n} + \frac{4}{5}\times\frac{x_n}{5^n} \end{cases}$

Das igualdades anteriores obtemos $\begin{cases} x_{n+1} = 3x_n - 4y_n \\ y_{n+1} = 4x_n + 3y_n \end{cases}$, o que define, por recorrência, as sucessões (x_n) e (y_n), uma vez que são conhecidos x_1 e y_1.

E é relativamente fácil demonstrar por indução que $(x_n, y_n, 5^n)$ é um terno Pitagórico, sendo a parte mais complicada mostrar que $\text{mdc}(x_n, y_n, 5^n) = 1$, o que prova que o terno Pitagórico é primitivo.

Neste exemplo, consideramos o número primo 5, mas podemos utilizar qualquer primo congruente com 1, módulo 4, como, por exemplo, 13,17, 29 ou outro.

Exemplo 163 *Suponhamos que temos dois ternos Pitagóricos e vejamos como obter um terceiro terno Pitagórico, a partir dos dois ternos anteriores.*

Consideremos os ternos Pitagóricos $(3,4,5)$ e $(5,12,13)$. Sejam $\alpha,\beta \in \mathbb{R}$, tais que $\cos\alpha = \frac{3}{5}$, $\sin\alpha = \frac{4}{5}$, $\cos\beta = \frac{5}{13}$ e $\sin\beta = \frac{12}{13}$. Então:

$$\begin{cases} \cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta = \frac{3}{5}\times\frac{5}{13} - \frac{4}{5}\times\frac{12}{13} = -\frac{33}{65} \\ \sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha = \frac{4}{5}\times\frac{5}{13} + \frac{3}{5}\times\frac{12}{13} = \frac{56}{65} \\ \cos(\alpha-\beta) = \cos\alpha\cos\beta + \sin\alpha\sin\beta = \frac{3}{5}\times\frac{5}{13} + \frac{4}{5}\times\frac{12}{13} = \frac{63}{65} \\ \sin(\alpha-\beta) = \sin\alpha\cos\beta - \sin\beta\cos\alpha = \frac{4}{5}\times\frac{5}{13} - \frac{3}{5}\times\frac{12}{13} = -\frac{16}{65} \end{cases}$$

E daqui se obtêm os ternos Pitagóricos primitivos $(33,56,65)$ e $(16,63,65)$.

E podemos continuar:

$$\begin{cases} \cos(2\alpha) = \cos^2\alpha - \sin^2\alpha = \frac{9}{25} - \frac{16}{25} = -\frac{7}{25} \\ \sin(2\alpha) = 2\sin\alpha\cos\alpha = 2\times\frac{3}{5}\times\frac{4}{5} = \frac{24}{25} \\ \cos(2\beta) = \cos^2\beta - \sin^2\beta = \frac{25}{169} - \frac{144}{169} = -\frac{119}{169} \\ \sin(2\beta) = 2\sin\beta\cos\beta = 2\times\frac{12}{13}\times\frac{5}{13} = \frac{120}{169} \end{cases}$$

E, ainda:

$$\begin{cases} \cos(2\alpha+\beta) = \cos(2\alpha)\cos\beta - \sin(2\alpha)\sin\beta = -\frac{7}{25}\times\frac{5}{13} - \frac{24}{25}\times\frac{12}{13} = -\frac{323}{325} \\ \sin(2\alpha+\beta) = \sin(2\alpha)\cos\beta + \sin\beta\cos(2\alpha) = \frac{24}{25}\times\frac{5}{13} - \frac{7}{25}\times\frac{12}{13} = \frac{36}{325} \\ \cos(2\alpha-\beta) = \cos(2\alpha)\cos\beta + \sin(2\alpha)\sin\beta = -\frac{7}{25}\times\frac{5}{13} + \frac{24}{25}\times\frac{12}{13} = \frac{253}{325} \\ \sin(2\alpha-\beta) = \sin(2\alpha)\cos\beta - \sin\beta\cos(2\alpha) = \frac{24}{25}\times\frac{5}{13} + \frac{7}{25}\times\frac{12}{13} = \frac{204}{325} \\ \cos(\alpha+2\beta) = \cos\alpha\cos(2\beta) - \sin\alpha\sin(2\beta) = -\frac{3}{5}\times\frac{119}{169} - \frac{4}{5}\times\frac{120}{169} = -\frac{837}{845} \\ \sin(\alpha+2\beta) = \sin\alpha\cos(2\beta) + \sin(2\beta)\cos\alpha = -\frac{4}{5}\times\frac{119}{169} + \frac{120}{169}\times\frac{3}{5} = -\frac{116}{845} \\ \cos(\alpha-2\beta) = \cos\alpha\cos(2\beta) + \sin\alpha\sin(2\beta) = -\frac{3}{5}\times\frac{119}{169} + \frac{4}{5}\times\frac{120}{169} = \frac{123}{845} \\ \sin(\alpha-2\beta) = \sin\alpha\cos(2\beta) - \sin(2\beta)\cos\alpha = -\frac{4}{5}\times\frac{119}{169} - \frac{120}{169}\times\frac{3}{5} = -\frac{836}{845} \end{cases}$$

E daqui obtemos os ternos Pitagóricos primitivos $(36,323,325)$, $(204,253,325)$, $(116,837,845)$ e $(123,836,845)$.

É claro que o processo pode prolongar-se.

4.3 Os números complexos e os ternos Pitagóricos

Podemos, também, utilizar conhecimentos elementares dos números complexos, para tratar o tema dos ternos Pitagóricos.

Consideremos o número complexo $3+4i$. O módulo deste complexo é dado por $\sqrt{3^2+4^2} = 5$, o que significa que $3^2+4^2 = 5^2$, obtendo-se, assim, o terno Pitagórico $(3,4,5)$.

E, pelo cálculo das sucessivas potências de $3+4i$, obtemos novos ternos Pitagóricos, uma vez que o módulo do produto de um número finito de números complexos é o produto dos módulos desse números.

$$\begin{cases} (3+4i)^2 = 9+24i+16i^2 = -7+24i \\ |-7+24i| = \sqrt{(-7)^2+24^2} = \sqrt{625} = 5^2 \end{cases}$$

Das igualdades anteriores, descobrimos o terno Pitagórico primitivo $(7,24,25)$.

$$\begin{cases} (3+4i)^3 = (-7+24i)(3+4i) = -21-28i+72i+96i^2 = -117+44i \\ |-117+44i| = 5^3 \end{cases}$$

Das duas igualdades anteriores, descobrimos o terno Pitagórico primitivo $(44,117,125)$.

Vejamos, agora, como obter duas sucessões que vão definir os sucessivos ternos Pitagóricos:

Suponhamos que $(3+4i)^n = x_n + iy_n$, com $x_n + iy_n \in \mathbb{N}$. Então:

$$(3+4i)^{n+1} = (x_n+iy_n)(3+4i) = 3x_n + 4ix_n + 3iy_n - 4y_n = 3x_n - 4y_n + i(4x_n+3y_n)$$

E daqui, obtemos a sucessão definida por $\begin{cases} x_1 = 3, y_1 = 4 \\ x_{n+1} = 3x_n - 4y_n \\ y_{n+1} = 4x_n + 3y_n \end{cases}$

Estão, assim definidos infinitos ternos Pitagóricos primitivos da forma $(x^n, y^n, 5^n)$.

Utilizando uma Calculadora gráfica, podemos definir as funções anteriores e, assim, obter os ternos Pitagóricos.

Consideremos o número complexo $5 + 12i$. O módulo deste complexo é dado por $\sqrt{5^2 + 12^2} = 13$, o que significa que $5^2 + 12^2 = 13^2$, obtendo-se, assim, o terno Pitagórico $(5, 12, 13)$.

E, pelo cálculo das sucessivas potências de $5 + 12i$, obtemos novos ternos Pitagóricos, uma vez que o módulo do produto de um número finito de números complexos é o produto dos módulos desse números.

$$\begin{cases} (5 + 12i)^2 = 25 + 120i + 144i^2 = -119 + 120i \\ |-119 + 120i| = \sqrt{(-119)^2 + 120^2} = \sqrt{28\,561} = 169 = 13^2 \end{cases}$$

Das igualdades anteriores, descobrimos o terno Pitagórico primitivo $\left(119, 120, 13^2\right)$.

$$\begin{cases} (5 + 12i)^3 = (-119 + 120i)(5 + 12i) = -595 - 1428i + 600i + 1440i^2 = -2035 - 828i \\ |-2035 - 828i| = \sqrt{(-2035)^2 + (-828)^2} = 2197 = 13^3 \end{cases}$$

Das duas igualdades anteriores, descobrimos o terno Pitagórico primitivo $\left(828, 2035, 13^3\right)$.

Vejamos, agora, como obter duas sucessões que vão definir os sucessivos ternos Pitagóricos:

Suponhamos que $(5 + 12i)^n = x_n + iy_n$, com $x_n + iy_n \in \mathbb{N}$. Então:

$$(5 + 12i)^{n+1} = (x_n + iy_n)(5 + 12i) = 5x_n + 12ix_n + 5iy_n - 12y_n = 5x_n - 12y_n + i(12x_n + 5y_n)$$

E daqui, obtemos a sucessão definida por $\begin{cases} x_1 = 3, y_1 = 4 \\ x_{n+1} = 5x_n - 12y_n \\ y_{n+1} = 12x_n + 5y_n \end{cases}$

Consideremos os ternos Pitagóricos $(3, 4, 5)$ e $(5, 12, 13)$. A partir destes dois ternos, podemos obter outros ternos Pitagóricos:

$$\begin{cases} (3 + 4i)(5 - 12i) = 15 - 36i + 20i - 48i^2 = 63 - 16i \\ |63 - 16i| = \sqrt{63^2 + 16^2} = \sqrt{4225} = 65 = 5 \times 13 \\ (3 + 4i)(5 + 12i) = 15 + 36i + 20i + 48i^2 = -33 + 56i \\ |-33 + 56i| = \sqrt{33^2 + 56^2} = \sqrt{4225} = 65 = 5 \times 13 \end{cases}$$

E, assim, obtivemos os dois ternos Pitagóricos $(16, 63, 5 \times 13)$ e $(33, 56, 5 \times 13)$.

Para obter os ternos Pitagóricos da forma $\left(x, y, 5^2 \times 13\right)$, calculamos $(3 + 4i)^2(5 - 12i) = 253 + 204i$ e $(3 + 4i)^2(5 + 12i) = -323 + 36i$, pelo que obtemos os ternos Pitagóricos $\left(204, 253, 5^2 \times 13\right)$ e $\left(36, 323, 5^2 \times 13\right)$.

Não podemos deixar de chamar a atenção para o importante facto deste assunto estar intimamente relacionado com a decomposição dum número natural numa soma de dois quadrados.

Assim, $5 = 2^2 + 1^2, 13 = 3^2 + 2^2$, enquanto que 7 não pode decompor-se numa soma de menos de quatro quadrados: $7 = 2^2 + 1^2 + 1^2 + 1^2$.

Finalizamos, realçando o facto da Trigonometria estar intimamente relacionada com os Números Complexos, pelo que era de esperar o paralelismo existente entre as duas maneiras de abordar este Tema, a nível de 12^o Ano.

Capítulo 5

O Anel dos Quaterniões

É bem conhecido o facto do corpo dos complexos ser isomorfo a $\mathbb{R}^2$, com as operações adição e multiplicação definidas por $(a,b)+(c,d)=(a+c,b+d)$ e por $(a,b)\times(c,d)=(ac-bd,ad+bc)$. Tal facto levou alguns matemáticos a pensar na possibilidade de algum outro $\mathbb{R}^n$, nomeadamente $\mathbb{R}^4$, poder ser corpo.

Hamilton definiu, em $\mathbb{R}^4$, a adição usual e uma multiplicação dum modo que adiante se verá, mas não obteve um corpo, embora só não se verificasse um dos axiomas (a comutatividade da multiplicação). A um anel nestas condições é costume chamar anel de divisão, havendo, no entanto, quem lhe chame corpo (e neste caso teremos corpos não comutativos e corpos comutativos). O anel encontrado por Hamilton é conhecido por anel dos quaterniões e pode ser definido dum modo semelhante ao corpo dos complexos. Em vez da unidade imaginária , temos três elementos i, j, k, tais que $i^2=j^2=k^2=-1$, $ij=k$, $jk=i$, $ki=j$, $ji=-k$, $kj=-i$ e $ik=-j$ .A multiplicação, antes de ser definida formalmente é usada, intuitivamente, da maneira usual, embora satisfazendo as condições acima referidas.

Representaremos o anel dos quaterniões por Q e teremos, então, $Q=\{a+bi+cj+dk\colon a,b,c,d\in\mathbb{R}\}$.

Exemplo 164 *Considere o conjunto* $Q=\{a+bi+cj+dk : a,b,c,d\in\mathbb{R}\}$ *algebrizado com as operações* $\oplus$ *e* $\otimes$ *definidas por:*

$$(a+bi+cj+dk)\oplus(A+Bi+Cj+Dk) = (a+A)+(b+B)\,i+(c+C)\,j+(d+D)\,k$$

$$(a+bi+cj+dk)\otimes(A+Bi+Cj+Dk) = X+Yi+Zj+Wk,\ com \begin{cases} X=aA-bB-cC-dD \\ Y=aB+bA+cD-dC \\ Z=aC+cA+dB-bD \\ W=aD+dA+bC-cB \end{cases}$$

Este exemplo, embora muito trabalhoso, é muito interessante, pois trata-se dum Anel não comutativo, em que existe elemento neutro para a operação $\oplus$ (que é chamado identidade do Anel) e em que o zero do Anel é o único elemento que não tem oposto para a operação $\otimes$.

Logo, a única propriedade que falha para que $(Q,\oplus,\otimes)$ seja Corpo é a comutatividade da operação $\otimes$.

O Anel $(Q,\oplus,\otimes)$ é conhecido por Anel dos quaterniões e, é claro, não tem nada a ver com o Anel $(\mathbb{Q},+,\times)$ dos números racionais.

A demonstração de que $(Q,\oplus,\otimes)$ é Anel é muito trabalhosa, embora seja pura rotina, pelo que não apresentamos essa demonstração.

Uma maneira cómoda de trabalhar com produtos no Anel dos quaterniões consiste em aplicar a propriedade distributiva, como habitualmente, e aplicar a seguinte regra:

$$i\otimes j=k; j\otimes k=i; k\otimes i=j; j\otimes i=-k; k\otimes j=-i; i\otimes k=-j$$

Além disso, temos $i^2 = j^2 = k^2 = -1$, conforme pode ser verificado, utilizando a definição da operação $\otimes$.

Habitualmente, utilizamos os sinais $+$ e $\times$, em vez de $\oplus$ e $\otimes$. Note-se, ainda, que o Corpo dos números complexos, $(\mathbb{C}, +, \times)$, é um subanel de $(Q, +, \times)$. Digamos, que subanel dum Anel é uma parte do Anel que ainda é Anel.

Vejamos como calcular $(1 + 2i + 2j + 3k) \otimes (4 + 3i + 5j + 2k)$, expressão esta que vamos substituir por E, por questões de falta de espaço:

$$\begin{aligned}
E &= (1 + 2i + 2j + 3k) \otimes (4 + 3i + 5j + 2k) = (1 + 2i + 2j + 3k) \times (4 + 3i + 5j + 2k) \\
&= (1 + 2i + 2j + 3k)\,(4 + 3i + 5j + 2k) \\
&= 4 + 3i + 5j + 2k + 8i + 6i^2 + 10ij + 4ik + 8j + 6ji + 10j^2 + 4jk + 12k + 9ki + 15kj + 6k^2 \\
&= 4 + 3i + 5j + 2k + 8i - 6 + 10ij - 4ki + 8j - 6ij - 10 + 4jk + 12k + 9ki - 15jk - 6 \\
&= 4 - 6 - 10 - 6 + 3i + 8i + 5j + 2k + 10ij - 6ij - 4ki + 9ki + 8j + 4jk - 15jk + 12k \\
&= -18 + 3i + 8i + 5j + 2k + 4ij + 5ki + 8j - 11jk + 12k \\
&= -18 + 11i + 5j + 2k + 4k + 5j + 8j - 11i + 12k \\
&= -18 + 0i + 18j + 18k = -18 + 18j + 18k
\end{aligned}$$

Se quisermos, apenas, encontrar o valor final, podemos utilizar o EXCEL. Segue-se uma simulação:

	A	B	C	D	E	F	G	H	I	J	K	L
1	1^o Factor				2^o Factor				Produto			
2	1	i	j	k	1	i	j	k	1	i	j	k
3									$= A_3 * E_3 - B_3 * F_3 - C_3 * G_3 - D_3 * H_3$			
4	1	2	2	3	4	3	5	2	-18	0	18	18

Na célula I3, está escrita a fórmula que nos dá o número que iremos multiplicar por 1. Ao copiarmos esta célula para I4, aparece o valor -18.

Se escrevermos as fórmulas correspondentes ao coeficientes de i, j e k, obteremos, à direita de -18, os valores 0, 18 e 18. Tal significa que $(1 + 2i + 2j + 3k) \otimes (4 + 3i + 5j + 2k) = -18 + 0i + 18j + 18k$.

É claro que não se apresentaram as restantes fórmulas por uma questão de falta espaço.

De modo análogo ao Corpo dos Complexos, podemos falar no conjugado e obter fórmulas interessantes, como, por exemplo, o conjugado do produto de dois factores é o produto dos conjugados desses factores, mas por ordem inversa. Registe-se que o conjugado de $a + bi + cj + dk$ (com $a, b, c, d \in \mathbb{R}$) é $a - bi - cj - dk$.

Outra maneira de obter os resultados é trabalhar com a seguinte função de 8 variáveis, sendo que as primeiras 4 variáveis correspondem ao primeiro factor e as últimas 4 correspondem ao segundo factor:

$$\begin{cases} g\,(a, b, c, d, A, B, C, D) = (x, y, z, w) \\ (x, y, z, w) = (aA - bB - cC - dD, aB + bA + cD - dC, aC + cA + dB - bD, aD + dA + bC - cB) \end{cases}$$

$g\,(1, 2, 2, 3, 4, 3, 5, 2) = (-18, 0, 18, 18)$

$g\,(4, -3, -5, -2, 1, -2, -2, -3) = (-18, 0, -18, -18)$

$g\,(4, 3, 5, 2, 1, 2, 2, 3) = (-18, 22, 8, 10)$

$g\,(1, -2, -2, -3, 4, -3, -5, -2) = (-18, -22, -8, -10)$

$g\,(a, b, c, d, a, -b, -c, -d) = \left(a^2 + b^2 + c^2 + d^2, 0, 0, 0\right)$

$g\,(a, -b, -c, -d, a, b, c, d) = \left(a^2 + b^2 + c^2 + d^2, 0, 0, 0\right)$

Convém referir de modo especial que, devido à não comutatividade da multiplicação, há dificuldades em definir a divisão.

Recordemos que dividir 8 por 2 consiste em encontrar o número que multiplicado por 2 dá 8. Tal número é 4, uma vez que $4 \times 2 = 2 \times 4 = 8$. Neste caso, não há problemas, porque a multiplicação é comutativa. Vejamos a situação no Anel dos Quaterniões:

$$\begin{cases} (1+2i+2j+3k) \otimes (4+3i+5j+2k) = -18+0i+18j+18k \\ (4+3i+5j+2k) \otimes (1+2i+2j+3k) = -18+22i-8j-10k \end{cases}$$

Qual será o quociente de $-18+0i+18j+18k$ por $1+2i+2j+3k$? Teria de ser "algo"que multiplicado por $1+2i+2j+3k$ desse $-18+0i+18j+18k$. Mas, multiplicado como? À esquerda? Ou à direita?

Comecemos por verificar como calcular o inverso de $a+bi+cj+dk$:

$$\begin{aligned} \frac{1}{a+bi+cj+dk} &= \frac{a-bi-cj-dk}{(a+bi+cj+dk)\otimes(a-bi-cj-dk)} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2} \\ &= \frac{a}{a^2+b^2+c^2+d^2} - \frac{b}{a^2+b^2+c^2+d^2}i - \frac{c}{a^2+b^2+c^2+d^2}j - \frac{d}{a^2+b^2+c^2+d^2}k \end{aligned}$$

$$\begin{aligned} \frac{1}{a+bi+cj+dk} &= \frac{a-bi-cj-dk}{(a+bi+cj+dk)\otimes(a-bi-cj-dk)} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2} \\ &= \frac{a}{a^2+b^2+c^2+d^2} - \frac{b}{a^2+b^2+c^2+d^2}i - \frac{c}{a^2+b^2+c^2+d^2}j - \frac{d}{a^2+b^2+c^2+d^2}k \end{aligned}$$

Ora,

$$g\left(a,b,c,d,\frac{a}{a^2+b^2+c^2+d^2},\frac{b}{a^2+b^2+c^2+d^2},\frac{c}{a^2+b^2+c^2+d^2},\frac{d}{a^2+b^2+c^2+d^2}\right) = (x,y,z,w)$$

com

$$\begin{aligned} (x,y,z,w) &= \left(\frac{a^2}{a^2+b^2+c^2+d^2}+\frac{b^2}{a^2+b^2+c^2+d^2}+\frac{c^2}{a^2+b^2+c^2+d^2}+\frac{d^2}{a^2+b^2+c^2+d^2},0,0,0\right) \\ &= (1,0,0,0) \end{aligned}$$

E,

$$g\left(\frac{a}{a^2+b^2+c^2+d^2},\frac{-b}{a^2+b^2+c^2+d^2},\frac{-c}{a^2+b^2+c^2+d^2},\frac{-d}{a^2+b^2+c^2+d^2},a,b,c,d\right) = (1,0,0,0)$$

Observe-se que $(a+bi+cj+dk)\otimes(a-bi-cj-dk) = (a-bi-cj-dk)\otimes(a+bi+cj+dk)$, pelo que faz sentido escrever $\dfrac{1}{a+bi+cj+dk} = \dfrac{a-bi-cj-dk}{(a+bi+cj+dk)\otimes(a-bi-cj-dk)}$.

Neste caso, não há perigo em escrever $\dfrac{1}{a+bi+cj+dk}$, embora se deva escrever $(a+bi+cj+dk)^{-1}$.

No caso geral, fala-se em quociente à esquerda e quociente à direita. Assim, $\alpha\beta^{-1}$ é o quociente de α por β à direita e $\beta^{-1}\alpha$ é o quociente de α por β à esquerda. Em Anéis em que a multiplicação é comutativa, os dois quocientes coincidem.

Definição 165 *Seja $\alpha = a+bi+cj+dk$, com $a,b,c,d \in \mathbb{R}$. Ao elemento de Q, $a-bi-cj-dk$, chamamos conjugado de α e escrevemos $\overline{\alpha}$.*

Proposição 166 *Sejam $\alpha, \beta \in Q$. Então, $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$.*

Demonstração
Sejam $\alpha = a + bi + cj + dk$ e $\beta = A + Bi + Cj + Dk$, com $a, b, c, d, A, B, C, D \in \mathbb{R}$.
Então,

$$\alpha\beta = (a + bi + cj + dk) \times (A + Bi + Cj + Dk) = X + Yi + Zj + Wk,$$

com

$$\begin{cases} X = aA - bB - cC - dD \\ Y = aB + bA + cD - dC \\ Z = aC + cA + dB - bD \\ W = aD + dA + bC - cB \end{cases}$$

Então,

$$\overline{\alpha\beta} = (aA - bB - cC - dD) - (aB + bA + cD - dC)\, i - (aC + cA + dB - bD)\, j - (aD + dA + bC - cB)$$

E, agora, temos $\overline{\beta} = A - Bi - Cj - Dk$ e $\overline{\alpha} = a - bi - cj - dk$.
Então,

$$\begin{aligned} \overline{\beta}\overline{\alpha} &= (A - Bi - Cj - Dk) \times (a - bi - cj - dk) \\ &= (-A + Bi + Cj + Dk) \times (-a + bi + cj + dk) \\ &= X_1 + Y_1 i + Z_1 j + W_1 k \end{aligned}$$

Para calcular $\overline{\beta}\overline{\alpha}$, basta trocar os sinais a A e a e trocar as letras maiúsculas pelas miúsculas e reciprocamente. Assim,

$$\overline{\beta}\overline{\alpha} = (A - Bi - Cj - Dk) \times (a - bi - cj - dk) = X_1 + Y_1 i + Z_1 j + W_1 k,$$

com

$$\begin{cases} X_1 = Aa - Bb - Cc - Dd \\ Y_1 = -Ab - Ba + Cd - Dc = -(aB + bA + cD - dC) \\ Z_1 = -Ac - Ca + Db - Bd = -(aC + cA + dB - bD) \\ W_1 = -Ad - Da + Bc - Cb = -(aD + dA + bC - cBk) \end{cases}$$

Logo, $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}, \forall \alpha, \beta \in Q$.

Definição 167 *Seja $\alpha = a + bi + cj + dk$, com $a, b, c, d \in \mathbb{R}$. Ao produto $\alpha\overline{\alpha}$, chamamos norma de α, escrevendo-se* $\mathrm{N}(\alpha)$.

Observação 168 *Se $\alpha = a + bi + cj + dk$, com $a, b, c, d \in \mathbb{R}$, então*

$$\mathrm{N}(\alpha) = a^2 + b^2 + c^2 + d^2 = a^2 + (-b)^2 + (-c)^2 + (-d)^2 = \mathrm{N}(\overline{\alpha})$$

Além disso, temos que a norma de um elemento de Q é um número real positivo ou nulo, sendo nulo, apenas no caso de termos $\alpha = 0 + 0i + 0j + 0k$.

Observação 169 *Note-se que, para $\alpha = a + bi + cj + dk$, com $a, b, c, d \in \mathbb{R}$, temos*

$$\begin{aligned}(a+bi+cj+dk)^{-1} &= \frac{a-bi-cj-dk}{(a+bi+cj+dk)\times(a-bi-cj-dk)} \\ &= \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2} = \frac{a-bi-cj-dk}{\mathrm{N}(\alpha)} \\ &= \frac{a}{\mathrm{N}(\alpha)} - \frac{b}{\mathrm{N}(\alpha)}i - \frac{c}{\mathrm{N}(\alpha)}j - \frac{d}{\mathrm{N}(\alpha)}k\end{aligned}$$

Observação 170 *Se não tivéssemos efectuado os cálculos anteriormente, podíamos calcular α^{-1} da seguinte maneira: pretendemos encontrar $\beta \in Q$, tal que $\alpha\beta = \beta\alpha = 1$. Ora, se $\alpha\beta = 1$, então $\overline{\alpha}(\alpha\beta) = \overline{\alpha}$, donde $(\overline{\alpha}\alpha)\beta = \overline{\alpha}$. Então, $\beta = \frac{1}{\mathrm{N}(\alpha)}\overline{\alpha}$.*

Por outro lado, $\beta\alpha = \left(\frac{1}{\mathrm{N}(\alpha)}\overline{\alpha}\right)\alpha = \frac{1}{\mathrm{N}(\alpha)}(\overline{\alpha}\alpha) = \frac{1}{\mathrm{N}(\alpha)} \times \mathrm{N}(\overline{\alpha}) = \frac{1}{\mathrm{N}(\alpha)} \times \mathrm{N}(\alpha) = 1$, o que termina a demonstração.

Proposição 171 *Sejam $\alpha, \beta \in Q$. Então, $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.*

Demonstração

$$\begin{aligned}\mathrm{N}(\alpha\beta) &= (\alpha\beta)\times\overline{\alpha\beta} = (\alpha\beta)\times\left(\overline{\beta}\overline{\alpha}\right) = \alpha\left(\beta\overline{\beta}\right)\overline{\alpha} \\ &= \alpha\,\mathrm{N}(\beta)\,\overline{\alpha} = \alpha\overline{\alpha}\,\mathrm{N}(\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)\end{aligned}$$

Note-se que, na multiplicação, os números reais (e só estes) comutam com qualquer elemento de Q. Isso significa que $\mathbb{R}$ é o centro do Anel Q.

Corolário 172 *O produto da soma dos quadrados de quatro números inteiros por outra soma de quatro quadrados de números inteiros ainda é uma soma de quatro quadrados de números inteiros.*

Sejam $x, y, a, b, c, d, r, s, t, u$ números inteiros que satisfazem as condições $x = a^2 + b^2 + c^2 + d^2$ e $y = r^2 + sb^2 + t^2 + u^2$.

Sejam $\alpha = a + bi + cj + dk$ e $\beta = r + si + tj + uk$.Então,

$$\begin{aligned}xy &= \left(a^2+b^2+c^2+d^2\right)\left(r^2+sb^2+t^2+u^2\right) \\ &= \mathrm{N}(\alpha)\,\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta)\end{aligned}$$

Mas, $\mathrm{N}(\alpha\beta)$ é uma soma de quatro quadrados de números inteiros, pelo que terminou a demonstração.

De qualquer modo, a demonstração anterior não nos indica a maneira de obter os quatro quadrados. Se pretendermos essa informação, temos de calcular $\mathrm{N}(\alpha\beta)$.

Sejam $\alpha = a + bi + cj + dk$ e $\beta = A + Bi + Cj + Dk$, com $a, b, c, d, A, B, C, D \in \mathbb{Z}$.

Já vimos que $\alpha\beta = X + Yi + Zj + Wk$, com $\begin{cases} X = aA - bB - cC - dD \\ Y = aB + bA + cD - dC \\ Z = aC + cA + dB - bD \\ W = aD + dA + bC - cB \end{cases}$.

Então, $\mathrm{N}(\alpha\beta)$ é dada por

$$(aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 + (aC + cA + dB - bD)^2 + (aD + dA + bC - cB)^2$$

Exemplo 173 *Transforme* $\left(2^2+3^2+4^2+5^2\right)\times\left(1^2+2^2+3^2+4^2\right)$ *numa soma de quatro quadrados, de acordo com o Corolário anterior.*

Resolução

Sejam $\alpha = 2+3i+4j+5k$ e $\beta = 1+2i+3j+4k$.

Ora, $\begin{cases} 2\left(1+2i+3j+4k\right) = 2+4i+6j+8k \\ 3i\left(1+2i+3j+4k\right) = 3i-6+9ij+12ik = -6+3i+9k-12j \\ 4j\left(1+2i+3j+4k\right) = 4j+8ji-12+16jk = -12+16i+4j-8k \\ 5k\left(1+2i+3j+4k\right) = 5k+10ki+15kj-20 = -20-15i+10j+5k \end{cases}$.

Então,

$$\begin{aligned} \alpha\beta &= 2+4i+6j+8k-6+3i+9k-12j-12+16i+4j-8k-20-15i+10j+5k \\ &= -36+8i+8j+14k \end{aligned}$$

Logo,

$$\left(2^2+3^2+4^2+5^2\right)\times\left(1^2+2^2+3^2+4^2\right) = 36^2+8^2+8^2+14^2$$

Note-se que $\begin{cases} 2^2+3^2+4^2+5^2 = 54 \\ 1^2+2^2+3^2+4^2 = 30 \\ 54\times 30 = 1620 \\ 36^2+8^2+8^2+14^2 = 1620 \end{cases}$.

Capítulo 6

Formas Quadráticas

Definição 174 *Sejam $k, n \in \mathbb{N}$. Forma k-ária de grau n é um polinómio homogéneo de k variáveis (ou indeterminadas) e grau n.*

Observações

Por exemplo, $x_1^2 + x_2^2$ e $x_1^2 + 2x_2^2 - 6x_1x_2 + x_3^2$ são formas quadráticas, sendo a primeira binária e a segunda ternária. Estas duas formas quadráticas têm coeficientes em $\mathbb{Z}$, pelo que lhes chamaremos formas quadráticas inteiras.

As formas quadráticas podem ser escritas matricialmente, embora não de modo único. Se exigirmos que a matriz A seja simétrica, então a representação matricial de uma forma quadrática é única. Assim,

$$x_1^2 + 2x_2^2 - 6x_1x_2 + x_3^2 = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} 1 & -3 & 0 \\ -3 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = x^T A x$$

sendo $A = \begin{bmatrix} 1 & -3 & 0 \\ -3 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ uma matriz simétrica.

Neste capítulo, vamos usar as variáveis $x_1, x_2, x_3, y_1, y_2, y_3, \ldots$, escrevendo-se $x = (x_1, x_2, x_3) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ e $x^T = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}$.

Dada uma forma quadrática inteira $Q(x_1, x_2, \cdots, x_n) = x^T A x$, com A matriz simétrica, os elementos $a_{i\,i}$ da matriz são números inteiros, mas os elementos $a_{i\,j}$, com $i \neq j$, não têm de ser inteiros; para $i \neq j$, teremos que $2a_{i\,j}$ é um inteiro, pelo que cada elemento $a_{i\,j}$ é da forma $\frac{m}{2}$, com $m \in \mathbb{Z}$. No entanto, vamos tratar, essencialmente, de casos em que todos os elementos da matriz são números inteiros. No caso das formas quadráticas ternárias inteiras, supomos sempre que os termos rectangulares têm coeficiente par, ou seja, a matriz é constituída por números inteiros.

Chamaremos discriminante da forma quadrática $Q(x_1, x_2, \cdots, x_n) = x^T A x$, ao determinante da matriz A.

Observe-se, também, que as formas quadráticas estão relacionadas com o chamado produto interno usual de $\mathbb{R}^n$:

$$Q(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} a_{i\,j} x_i x_j = \langle x, Ax \rangle$$

Note-se que o produto interno usual de $\mathbb{R}^n$ (e não só o usual) é uma forma quadrática, mas nem toda a forma quadrática define um produto interno.

Suponhamos que $x_i = \sum_{j=1}^{n} c_{i\,j} x_i x_j (i = 1, \ldots, n)$, sendo $C = (c_{i\,j})$ uma matriz de tipo $n \times n$ e entradas em $\mathbb{Z}$.

Se $\det C = 1$, então a matriz C é invertível, tendo-se que as entradas da matriz inversa $D = C^{-1}$ são números inteiros.

Se $x = Cy$, então

$$\begin{aligned} Q(x_1, x_2, \cdots, x_n) &= x^T Ax = (Cy)^T ACy = y^T C^T ACy \\ &= y^T By = Q_1(y_1, y_2, \cdots, y_n) \end{aligned}$$

Note-se que $y_i = \sum_{j=1}^{n} d_{i\,j} x_j$, para $i = 1, \ldots, n$ e que $D = C^{-1}$.

As duas formas quadráticas $Q(x_1, x_2, \cdots, x_n)$ e $Q_1(y_1, y_2, \cdots, y_n)$ têm coeficientes inteiros e, devido ao modo como estão relacionadas, diremos que são formas equivalentes. Note-se que a matriz $B = C^T AC$ é simétrica, pois A é simétrica.

Observe-se que formas equivalentes têm o mesmo discriminante (determinante da matriz associada), o que não significa que matrizes com o mesmo determinante correspondam a formas quadráticas equivalentes.

Exemplo 175 *Consideremos a forma quadrática binária* $Q(x_1, x_2) = x_1^2 + 4x_1x_2 + 2x_2^2$ *e a matriz* $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Note-se que $\det C = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1$.

Substituindo, em $Q(x_1, x_2)$, $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ por $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} y_1 + y_2 \\ y_2 \end{bmatrix}$, obtemos:

$$\begin{aligned} (y_1 + y_2)^2 + 4(y_1 + y_2) y_2 + 2y_2^2 &= y_1^2 + 2y_1y_2 + y_2^2 + 4y_1y_2 + 4y_2^2 + 2y_2^2 \\ &= y_1^2 + 6y_1y_2 + 7y_2^2 \\ &= Q_1(y_1, y_2) \end{aligned}$$

Seja $A = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}$. Matricialmente, temos

$$Q(x_1, x_2) = \begin{bmatrix} x_1 & x_2 \end{bmatrix} A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$\begin{aligned} Q_1(y_1, y_2) &= \begin{bmatrix} y_1 & y_2 \end{bmatrix} C^T AC \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \\ &= \begin{bmatrix} y_1 & y_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \\ &= \begin{bmatrix} y_1 & y_2 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \end{aligned}$$

Ora, não podemos afirmar que $x_1^2 + 4x_1x_2 + 2x_2^2 = Q(x_1, x_2) = Q_1(y_1, y_2) = y_1^2 + 6y_1y_2 + 7y_2^2$. Então, diremos que $Q(x_1, x_2) \sim Q_1(y_1, y_2)$.

Em rigor, deveríamos dizer: "Se, na forma quadrática $Q(x_1, x_2)$, substituirmos $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ por $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$, obtemos a forma quadrática $Q_1(y_1, y_2)$". No entanto, vamos escrever $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$, para simplificar.

Sejam $Q(x_1, x_2, \cdots, x_n)$ e $Q_1(y_1, y_2, \cdots, y_n)$ duas formas quadráticas.

Diremos que $Q(x_1, x_2, \cdots, x_n) \sim Q_1(y_1, y_2, \cdots, y_n)$, se existir C, uma matriz quadrada de inteiros e determinante 1, tal que $x = Cy$ e $Q_1(y_1, y_2, \cdots, y_n)$ é obtida de $Q(x_1, x_2, \cdots, x_n)$, substituindo $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ por $C \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$.

Proposição 176 *A relação $\sim$, acima definida, é uma relação de equivalência.*

Demonstração

1. $Q(x_1, x_2, \cdots, x_n) \sim Q(x_1, x_2, \cdots, x_n)$, porque $Q(x_1, x_2, \cdots, x_n)$ obtém-se de $Q(x_1, x_2, \cdots, x_n)$, substituindo $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ por $I_n \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, sendo I_n a matriz identidade, a qual é uma matriz de inteiros e de determinante 1.

   Logo, a relação $\sim$ é reflexiva.

2. Suponhamos que $Q(x_1, x_2, \cdots, x_n) \sim Q_1(y_1, y_2, \cdots, y_n)$. Então, existe C, uma matriz quadrada de inteiros e determinante 1, tal que $x = Cy$ e $Q_1(y_1, y_2, \cdots, y_n)$ é obtida de $Q(x_1, x_2, \cdots, x_n)$, substituindo $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ por $C \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$.

   Então, $Q_1(y_1, y_2, \cdots, y_n) = \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} C^T A C \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$. Note-se que $C^T AC$ é uma matriz simétrica.

   Substituindo, em $Q_1(y_1, y_2, \cdots, y_n)$, $\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ por $C^{-1} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, obtemos:

$$\begin{aligned} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \left(C^{-1}\right)^T C^T A C C^{-1} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} &= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \left(CC^{-1}\right)^T A \left(CC^{-1}\right) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \\ &= \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \\ &= Q(x_1, x_2, \cdots, x_n) \end{aligned}$$

É claro que C^{-1} é uma matriz de inteiros de determinante 1 (basta recordar um dos processos de encontrar a matriz inversa: através da adjunta).

Então, se $Q(x_1, x_2, \cdots, x_n) \sim Q_1(y_1, y_2, \cdots, y_n)$, podemos concluir que $Q_1(y_1, y_2, \cdots, y_n) \sim Q(x_1, x_2, \cdots, x_n)$. Logo, a relação $\sim$ é simétrica.

3. Suponhamos que $Q(x_1, x_2, \cdots, x_n) \sim Q_1(y_1, y_2, \cdots, y_n) \sim Q_2(z_1, z_2, \cdots, z_n)$.

$Q_1(y_1, y_2, \cdots, y_n)$ obtém-se de $Q(x_1, x_2, \cdots, x_n)$, substituindo $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ por $C \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$, com $\det C = 1$ e as entradas da matriz C pertencentes a $\mathbb{Z}$.

$Q_2(z_1, z_2, \cdots, z_n)$ obtém-se de $Q_1(y_1, y_2, \cdots, y_n)$, substituindo $\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ por $D \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$, com $\det D = 1$ e as entradas da matriz D pertencentes a $\mathbb{Z}$.

$$Q(x_1, x_2, \cdots, x_n) = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$$Q_1(y_1, y_2, \cdots, y_n) = \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} C^T A C \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$$Q_2(z_1, z_2, \cdots, z_n) = \begin{bmatrix} z_1 & \cdots & z_n \end{bmatrix} D^T C^T A C D \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} z_1 & \cdots & z_n \end{bmatrix} (CD)^T A (CD) \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}.$$

Ora, $\det(CD) = \det(C) \times \det(D) = 1 \times 1 = 1$, tendo-se que CD é uma matriz de entradas em $\mathbb{Z}$.

Logo, $Q_2(z_1, z_2, \cdots, z_n)$ obtém-se de $Q(x_1, x_2, \cdots, x_n)$, substituindo $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ por $CD \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$.

Logo, a relação $\sim$ é transitiva. Então, $\sim$ é uma relação de equivalência.

Observação

Se $Q(x_1, x_2, \cdots, x_n) = m$, para certos inteiros $m, x_1, x_2, \cdots, x_n$, diremos que m é representável pela forma quadrática $Q(x_1, x_2, \cdots, x_n)$, sendo que formas quadráticas equivalentes representam os mesmos números, isto é, se duas formas quadráticas Q_1 e Q_2 são equivalentes, então todo o número inteiro representável por uma das formas é representável pela outra.

Este é um exemplo em que o termo rectangular tem coeficiente ímpar.

Exercício 177 *Sejam* $Q(x_1, x_2) = 3x_1^2 + 2x_1x_2 + x_2^2$ *e* $C = \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}$. *Determine a forma quadrática* $Q_1(y_1, y_2)$ *que se obtém de* $Q(x_1, x_2)$, *substituindo* $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ *por* $C \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$.

Resolução

Ora, $A = \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}$ e $\det C = \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 3 - 2 = 1$.

Mas,

$$\begin{aligned} C^TAC &= \begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix}^T \begin{bmatrix}3 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix} = \begin{bmatrix}1 & 2\\ 1 & 3\end{bmatrix}\begin{bmatrix}3 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix} \\ &= \begin{bmatrix}1 & 2\\ 1 & 3\end{bmatrix}\begin{bmatrix}5 & 6\\ 3 & 4\end{bmatrix} = \begin{bmatrix}11 & 14\\ 14 & 18\end{bmatrix} \end{aligned}$$

Então,

$$\begin{aligned} \begin{bmatrix}y_1 & y_2\end{bmatrix} C^TAC \begin{bmatrix}y_1\\ y_2\end{bmatrix} &= \begin{bmatrix}y_1 & y_2\end{bmatrix} \begin{bmatrix}11 & 14\\ 14 & 18\end{bmatrix} \begin{bmatrix}y_1\\ y_2\end{bmatrix} \\ &= 11y_1^2 + 28y_1y_2 + 18y_2^2 \end{aligned}$$

Note-se que $\det A = \begin{vmatrix}3 & 1\\ 1 & 1\end{vmatrix} = 3 - 1 = 2 = 198 - 196 = \begin{vmatrix}11 & 14\\ 14 & 18\end{vmatrix}$.

Teorema de Dirichlet

Proposição 178 *Sejam a e b, dois números naturais, tais que* $\operatorname{mdc}(a,b) = 1$. *Então, na progressão aritmética de 1º termo b e razão a, há infinitos primos.*

Observação

Este Teorema de Dirichlet é essencial para este capítulo.
Será usado sem apresentarmos a sua demonstração.

Antes de passarmos aos lemas seguintes, vejamos um exemplo:

Exemplo 179 *Seja* $Q(x_1,x_2) = 3x_1^2 - 14x_1x_2 + 18x_2^2 = \begin{bmatrix}x_1 & x_2\end{bmatrix}\begin{bmatrix}3 & -7\\ -7 & 18\end{bmatrix}\begin{bmatrix}x_1\\ x_2\end{bmatrix}$. *Qual será o menor inteiro positivo a representável por $Q(x_1,x_2)$? E haverá alguma forma quadrática equivalente a $Q(x_1,x_2)$, cuja matriz associada tenha, na primeira linha e primeira coluna esse elemento a?*

$$3Q(x_1,x_2) = 9x_1^2 - 42x_1x_2 + 54x_2^2 = (3x_1 - 7x_2)^2 + 5x_2^2$$

Então, $Q(x_1,x_2) = \frac{1}{3}(3x_1 - 7x_2)^2 + \frac{5}{3}x_2^2$. Se $x_2 = 0$, então o menor inteiro representável por $Q(x_1,x_2)$ é 3. Se $x_2 = \pm 1$, então o menor inteiro representável por $Q(x_1,x_2)$ é 2. Assim, por exemplo, $Q(2,1) = \begin{bmatrix}2 & 1\end{bmatrix}\begin{bmatrix}3 & -7\\ -7 & 18\end{bmatrix}\begin{bmatrix}2\\ 1\end{bmatrix} = 2$.

Logo, 2 é representável por $Q(x_1,x_2)$. E é fácil verificar que 1 não é representável por $Q(x_1,x_2)$. Logo, 2 é o menor inteiro positivo representável por $Q(x_1,x_2)$.

Seja $M = \begin{bmatrix} 2 & s \\ 1 & u \end{bmatrix}$, com $\det M = 2u - s = 1$. Então, podemos escolher $u = 0 \wedge s = -1$.

Seja $B = \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 3 & -7 \\ -7 & 18 \end{bmatrix} \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 4 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}$.

Então, $b_{11} = 2$, como pretendido.

Mas, suponhamos que fazíamos $u = 3 \wedge s = 5$. Então, $M_1 = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$.

E $B_1 = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \begin{bmatrix} 3 & -7 \\ -7 & 18 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} -1 & 4 \\ -6 & 19 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 7 & 27 \end{bmatrix}$.

Lema 180 *Uma forma quadrática binária $Q(x_1, x_2) = x^T Ax = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$ é definida positiva se e só se os dois menores principais da matriz (simétrica) A são positivos, isto é, se $a_{11} > 0$ e $a_{11}a_{22} - a_{12}^2 > 0$.*

Demonstração

Uma forma quadrática binária é positiva se $Q(x_1, x_2) \geq 0$, para quaisquer x_1, x_2, tendo-se que se $Q(x_1, x_2) = 0$, então $(x_1, x_2) = (0, 0)$

Seja $Q(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$ uma forma quadrática binária definida positiva. Então, $0 < Q(1, 0) = a_{11}$.

Além disso, devemos ter $Q(\lambda, 1) > 0, \forall \lambda \in \mathbb{R}$. Então, $a_{11}\lambda^2 + 2a_{12}\lambda + a_{22} > 0, \forall \lambda \in \mathbb{R}$.

Logo, $\triangle' = a_{12}^2 - a_{11}a_{22} < 0$, pelo que deve ser $a_{11}a_{22} - a_{12}^2 > 0$.

Reciprocamente, suponhamos que $a_{11} > 0$ e $a_{11}a_{22} - a_{12}^2 > 0$. Então,

$$\begin{aligned} a_{11}Q(x_1, x_2) &= a_{11}^2x_1^2 + 2a_{11}a_{12}x_1x_2 + a_{11}a_{22}x_2^2 \\ &= (a_{11}x_1 + a_{12}x_2)^2 + a_{11}a_{22}x_2^2 - a_{12}^2x_2^2 \\ &= (a_{11}x_1 + a_{12}x_2)^2 + \left(a_{11}a_{22} - a_{12}^2\right)x_2^2 \end{aligned}$$

Então, $a_{11}Q(x_1, x_2) \geq 0, \forall x_1, x_2 \in \mathbb{R}$. Logo, $Q(x_1, x_2) \geq 0, \forall x_1, x_2 \in \mathbb{R}$, porque $a_{11} > 0$.

Suponhamos, agora, que $Q(x_1, x_2) = 0$. Então, $(a_{11}x_1 + a_{12}x_2)^2 + \left(a_{11}a_{22} - a_{12}^2\right)x_2^2$.

Logo, $a_{11}x_1 + a_{12}x_2 = 0$ e $\left(a_{11}a_{22} - a_{12}^2\right)x_2^2 = 0$.

Então, $x_2 = 0$ e $a_{11}x_1 + a_{12}x_2 = 0$. Logo, $x_1 = 0$.

Logo, $Q(x_1, x_2)$ é uma forma quadrática definida positiva.

Lema 181 *Em cada classe das formas quadráticas inteiras binárias e definidas positivas, existe uma forma que satisfaz $2|a_{12}| \leq a_{11} \leq a_{22}$. Tal forma é chamada reduzida e, numa forma reduzida, $a_{11} \leq \frac{2}{\sqrt{3}}\sqrt{d_2}$, onde $d_2 = a_{11}a_{22} - a_{12}^2$.*

Demonstração

Consideremos a forma quadrática inteira binária e definida positiva dada por $Q(x_1, x_2) = a'_{11}x_1^2 + 2a'_{12}x_1x_2 + a'_{22}x_2^2$. Seja a o menor inteiro positivo representável pela forma $Q(x_1, x_2)$. Então, existem números inteiros x'_1, x'_2, tais que $a = Q(x'_1, x'_2) = a'_{11}x_1'^2 + 2a'_{12}x'_1x'_2 + a'_{22}x_2'^2$.

Seja $d = \text{mdc}(x'_1, x'_2)$. Então, temos, obrigatoriamente, $d = 1$, pois, se a é representável pela forma $Q(x_1, x_2)$, então $\frac{a}{d^2}$ também é representável por $Q(x_1, x_2)$ e, devido à minimalidade de a, temos $\frac{a}{d^2} = a$.

Mas se $\text{mdc}(x'_1, x'_2) = 1$, então existem certos números inteiros u_0, s_0, tais que $u_0x'_1 - s_0x'_2$, sendo a solução geral desta equação Diofantina dada por $u = u_0 + tx'_2 \wedge s = s_0 + tx'_1$, com $t \in \mathbb{Z}$.

Sejam $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}, M = \begin{bmatrix} x'_1 & s \\ x'_2 & u \end{bmatrix}$. Então, $\det M = ux'_1 - sx'_2$. Então, a equação $ux'_1 - sx'_2 = 1$ tem solução, porque $\text{mdc}(x'_1, x'_2) = 1$.

Seja, $M(t) = M = \begin{bmatrix} x'_1 & s_0 + tx'_1 \\ x'_2 & u_0 + tx'_2 \end{bmatrix}$.

Suponhamos, agora, que $x = My$. Substituindo, em $Q(x_1, x_2)$, $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ por My, obtemos $Q_1(y_1, y_2)$.

Então, $Q(x_1, x_2) \sim Q_1(y_1, y_2)$, pelo que as formas quadráticas Q e Q_1 estão na mesma classe de equivalência e, por isso, representam os mesmos inteiros.

Suponhamos que $Q_1(y_1, y_2) = a_{11}y_1^2 + 2a_{12}y_1y_2 + a_{22}y_2^2$. Ora:

$$\begin{aligned} A'M &= \begin{bmatrix} a'_{11} & a'_{12} \\ a'_{12} & a'_{22} \end{bmatrix} M = \begin{bmatrix} a'_{11} & a'_{12} \\ a'_{12} & a'_{22} \end{bmatrix} \begin{bmatrix} x'_1 & s_0 + tx'_1 \\ x'_2 & u_0 + tx'_2 \end{bmatrix} \\ &= \begin{bmatrix} x'_1a'_{11} + x'_2a'_{12} & a'_{11}s_0 + a'_{11}tx'_1 + a'_{12}u_0 + a'_{12}tx'_2 \\ x'_1a'_{12} + x'_2a'_{22} & a'_{12}s_0 + a'_{12}tx'_1 + a'_{22}u_0 + a'_{22}tx'_2 \end{bmatrix} \end{aligned}$$

Logo,

$$M^TA'M = A = \begin{bmatrix} x'_1 & x'_2 \\ s_0 + tx'_1 & u_0 + tx'_2 \end{bmatrix} \begin{bmatrix} x'_1a'_{11} + x'_2a'_{12} & a'_{11}s_0 + a'_{11}tx'_1 + a'_{12}u_0 + a'_{12}tx'_2 \\ x'_1a'_{12} + x'_2a'_{22} & a'_{12}s_0 + a'_{12}tx'_1 + a'_{22}u_0 + a'_{22}tx'_2 \end{bmatrix}$$

Então,

$$\begin{aligned} a_{11} &= x'_1\left(x'_1a'_{11} + x'_2a'_{12}\right) + x'_2\left(x'_1a'_{12} + x'_2a'_{22}\right) \\ &= a'_{11}(x'_1)^2 + 2a'_{12}x'_1x'_2 + a'_{22}(x'_2)^2 \\ &= a \end{aligned}$$

Então, $Q_1(y_1, y_2) = a_{11}y_1^2 + 2a_{12}y_1y_2 + a_{22}y_2^2 = ay_1^2 + 2a_{12}y_1y_2 + a_{22}y_2^2$.
Logo, $Q_1(1, 0) = a$.
Continuando, temos

$$\begin{aligned} a_{12} &= a_{21} = x'_1\left(a'_{11}s_0 + a'_{11}tx'_1 + a'_{12}u_0 + a'_{12}tx'_2\right) + x'_2\left(a'_{12}s_0 + a'_{12}tx'_1 + a'_{22}u_0 + a'_{22}tx'_2\right) \\ &= x'_1a'_{11}s_0 + (x'_1)^2a'_{11}t + x'_2a'_{12}s_0 + 2x'_2a'_{12}tx'_1 + x'_1a'_{12}u_0 + x'_2a'_{22}u_0 + (x'_2)^2a'_{22}t \\ &= \left((x'_1)^2a'_{11} + 2a'_{12}x'_1x'_2 + (x'_2)^2a'_{22}\right)t + x'_1a'_{11}s_0 + x'_2a'_{12}s_0 + x'_1a'_{12}u_0 + x'_2a'_{22}u_0 \\ &= at + x'_1a'_{11}s_0 + x'_2a'_{12}s_0 + x'_1a'_{12}u_0 + x'_2a'_{22}u_0 \end{aligned}$$

E, agora, podemos escolher $t \in \mathbb{Z}$, de modo que $|a_{12}| \leq \frac{a}{2} = \frac{a_{11}}{2}$.
Ora, $0 < Q_1(0, 1) = a_{22} \geq a = a_{11}$, devido à minimalidade de a.
De $0 < a_{11} \leq a_{22}$, vem $a_{11}^2 \leq a_{11}a_{22}$. Então, $a_{11}^2 \leq a_{11}a_{22} - a_{12}^2 + a_{12}^2$.
Logo, $a_{11}^2 \leq d_2 + a_{12}^2 \leq d_2 + \frac{a_{11}^2}{4}$, donde vem $\frac{3}{4}a_{11}^2 \leq d_2$ e, por isso, $a_{11}^2 \leq \frac{4}{3}d_2$.
Então, $a_{11} \leq \frac{2}{\sqrt{3}}\sqrt{d_2}$.

Corolário 182 *Toda a forma quadrática binária inteira e definida positiva de discriminante $d_2 = 1$ é equivalente a uma soma de dois quadrados.*

Demonstração

Pelo lema anterior, sabemos que toda a forma quadrática binária definida positiva é equivalente a uma forma quadrática reduzida (binária e definida positiva) $Q_1(y_1, y_2) = a_{11}y_1^2 + 2a_{12}y_1y_2 + a_{22}y_2^2$, com $a_{11} \leq \frac{2}{\sqrt{3}}\sqrt{d_2}$.

Como estamos a supor que $d_2 = 1$, então $a_{11} \leq \frac{2}{\sqrt{3}}$. Logo, $a_{11} = 1$.

Mas, $|a_{12}| \leq \frac{a_{11}}{2} = \frac{1}{2}$, pelo que $a_{12} = 0 \vee a_{12} = \frac{1}{2}$ (note-se que $2a_{12} \in \mathbb{Z}$).
E, como $d_2 = a_{11}a_{22} - a_{12}^2 = 1$, vem $a_{22} - a_{12}^2 = 1$, pelo que $a_{12} = 0$ e $a_{22} = 1$.
Logo, $Q_1(y_1, y_2) = y_1^2 + y_2^2$.

Lema 183 *A forma quadrática ternária* $Q(x_1,x_2,x_3)=\begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}A\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}$, $A=\begin{bmatrix}a_{11} & a_{12} & a_{13}\\a_{12} & a_{22} & a_{23}\\a_{13} & a_{23} & a_{33}\end{bmatrix}$, *é definida positiva se e só se os três menores principais da matriz* A *são positivos, isto é, se tivermos* $a_{11}>0$, $a_{11}a_{22}-a_{12}^2>0$, $\det A=d_3>0$.

Demonstração

Suponhamos que $Q(x_1,x_2,x_3)=\begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}A\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}=\sum_{i,j=1}^{3}a_{ij}x_ix_j$ é uma forma quadrática definida positiva e que A é uma matriz simétrica (de inteiros).

Pretendemos provar que $a_{11}>0$, $a_{11}a_{22}-a_{12}^2>0$, $\det A=d_3>0$.

Ora, $0<Q(1,0,0)=\begin{bmatrix}1 & 0 & 0\end{bmatrix}\begin{bmatrix}a_{11} & a_{12} & a_{13}\\a_{12} & a_{22} & a_{23}\\a_{13} & a_{23} & a_{33}\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix}=a_{11}$.

Como $a_{11}>0$, $Q(x_1,x_2,x_3)$ é uma forma quadrática definida positiva, se e só se o mesmo acontece com a forma quadrática $a_{11}Q(x_1,x_2,x_3)$. Mas:

$$\begin{aligned}a_{11}Q(x_1,x_2,x_3) &= a_{11}\begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}\begin{bmatrix}a_{11} & a_{12} & a_{13}\\a_{12} & a_{22} & a_{23}\\a_{13} & a_{23} & a_{33}\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}\\ &= a_{11}\begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}\begin{bmatrix}a_{11}x_1+a_{12}x_2+a_{13}x_3\\a_{12}x_1+a_{22}x_2+a_{23}x_3\\a_{13}x_1+a_{23}x_2+a_{33}x_3\end{bmatrix}\\ &= a_{11}^2x_1^2+2a_{11}a_{12}x_1x_2+2a_{11}a_{13}x_1x_3+a_{11}a_{22}x_2^2+2a_{11}a_{23}x_2x_3+a_{11}a_{33}x_3^2\end{aligned}$$

Consideremos a forma linear $L(x_1,x_2,x_3)=a_{11}x_1+a_{12}x_2+a_{13}x_3$. Então,

$$\begin{aligned}(L(x_1,x_2,x_3))^2 &= (a_{11}x_1+a_{12}x_2+a_{13}x_3)^2\\ &= a_{11}^2x_1^2+2a_{11}x_1a_{12}x_2+2a_{11}x_1a_{13}x_3+a_{12}^2x_2^2+2a_{12}x_2a_{13}x_3+a_{13}^2x_3^2\end{aligned}$$

Calculemos $Q_1(x_1,x_2,x_3)=a_{11}Q(x_1,x_2,x_3)-(L(x_1,x_2,x_3))^2$:

$$\begin{aligned}Q_1(x_1,x_2,x_3) &= a_{11}Q(x_1,x_2,x_3)-(L(x_1,x_2,x_3))^2\\ &= a_{11}a_{22}x_2^2+2a_{11}a_{23}x_2x_3+a_{11}a_{33}x_3^2-a_{12}^2x_2^2-2a_{12}a_{13}x_2x_3-a_{13}^2x_3^2\\ &= \left(a_{11}a_{22}-a_{12}^2\right)x_2^2+2\left(a_{11}a_{23}-a_{12}a_{13}\right)x_2x_3+\left(a_{11}a_{33}-a_{13}^2\right)x_3^2\end{aligned}$$

Então, $Q_1(x_1,x_2,x_3)$ é uma forma quadrática binária que só depende de x_2 e x_3, pelo que escreveremos, apenas, $Q_1(x_2,x_3)$. Então:

$$Q_1(x_2,x_3)=\begin{bmatrix}x_2 & x_3\end{bmatrix}\begin{bmatrix}a_{11}a_{22}-a_{12}^2 & a_{11}a_{23}-a_{12}a_{13}\\a_{11}a_{23}-a_{12}a_{13} & a_{11}a_{33}-a_{13}^2\end{bmatrix}\begin{bmatrix}x_2\\x_3\end{bmatrix}$$

Seguidamente, vamos verificar que, curiosamente, $Q_1(x_2,x_3)$ é uma forma quadrática binária definida positiva se e só se $a_{11}Q(x_1,x_2,x_3)$ também é uma forma quadrática definida positiva. Assim, bastará ver quando é que $Q_1(x_2,x_3)$ é definida positiva, ficando o problema simplificado e reduzido ao caso anterior.

Suponhamos que $Q_1(x_2,x_3)$ é definida positiva.

Então, $Q_1(x_2,x_3)+(L(x_1,x_2,x_3))^2=a_{11}Q(x_1,x_2,x_3)$ é uma forma positiva definida.

Reciprocamente, suponhamos que $a_{11}Q(x_1,x_2,x_3)$ é positiva definida.

Suponhamos, ainda, que $Q_1(x_2',x_3') \leq 0$, para certos inteiros x_2' e x_3'.

Sejam x_2'' e x_3'' dois inteiros tais que $x_2'' = a_{11}x_2'$ e $x_3'' = a_{11}x_3'$. Como uma forma quadrática é um polinómio homogéneo de grau 2, então $Q_1(x_2'',x_3'') = Q_1(a_{11}x_2', a_{11}x_3') = a_{11}^2 Q_1(x_2',x_3') \leq 0$, uma vez que, por hipótese, temos $Q_1(x_2',x_3') \leq 0$.

Agora, escolhemos um número inteiro x_1'', de modo que $L(x_1'',x_2'',x_3'') = 0$. Ora,

$$\begin{aligned} L\left(x_1'',x_2'',x_3''\right) = 0 &\iff a_{11}x_1'' + a_{12}x_2'' + a_{13}x_3'' = 0 \\ &\iff a_{11}x_1'' + a_{11}a_{12}x_2' + a_{11}a_{13}x_3' = 0 \\ &\iff x_1'' + a_{12}x_2' + a_{13}x_3' = 0 \\ &\iff x_1'' = -a_{12}x_2' - a_{13}x_3' \end{aligned}$$

Então,

$$\begin{aligned} a_{11}Q\left(x_1'',x_2'',x_3''\right) &= Q_1\left(x_2'',x_3''\right) + \left(L\left(x_1'',x_2'',x_3''\right)\right)^2 \\ &= Q_1\left(x_2'',x_3''\right) + 0 \\ &= a_{11}^2 Q_1\left(x_2',x_3'\right) \end{aligned}$$

Então, $a_{11}Q(x_1'',x_2'',x_3'') \leq 0$. Mas, estamos a supor que $a_{11}Q(x_1,x_2,x_3)$ é uma forma positiva definida. Então, tem de ser $x_1'' = x_2'' = x_3'' = 0$.

Logo, se $Q_1(x_2',x_3') \leq 0$, tem de ser $x_2'' = x_3'' = 0$. Então, $a_{11}x_2' = a_{11}x_3' = 0$, donde se conclui que $x_2' = x_3' = 0$.

Então, a forma binária $Q_1(x_2,x_3)$ é positiva definida.

Ficou, assim, provado que $Q_1(x_2,x_3)$ é uma forma quadrática binária definida positiva se e só se $a_{11}Q(x_1,x_2,x_3)$ é definida positiva. Mas:

$$\begin{aligned} Q_1(x_2,x_3) &= \left(a_{11}a_{22} - a_{12}^2\right)x_2^2 + 2\left(a_{11}a_{23} - a_{12}a_{13}\right)x_2x_3 + \left(a_{11}a_{33} - a_{13}^2\right)x_3^2 \\ &= \begin{bmatrix} x_2 & x_3 \end{bmatrix} \begin{bmatrix} a_{11}a_{22} - a_{12}^2 & a_{11}a_{23} - a_{12}a_{13} \\ a_{11}a_{23} - a_{12}a_{13} & a_{11}a_{33} - a_{13}^2 \end{bmatrix} \begin{bmatrix} x_2 \\ x_3 \end{bmatrix} \end{aligned}$$

Mas, $Q_1(x_2,x_3)$ é definida positiva, se e só se $a_{11}a_{22} - a_{12}^2 > 0$ e $d_2 > 0$.

Ora,

$$\begin{aligned} d_2 &= \left(a_{11}a_{22} - a_{12}^2\right)\left(a_{11}a_{33} - a_{13}^2\right) - \left(a_{11}a_{23} - a_{12}a_{13}\right)^2 \\ &= a_{11}^2a_{22}a_{33} - a_{11}a_{22}a_{13}^2 - a_{11}a_{12}^2a_{33} + a_{12}^2a_{13}^2 - a_{11}^2a_{23}^2 + 2a_{11}a_{12}a_{13}a_{23} - a_{12}^2a_{13}^2 \\ &= a_{11}^2a_{22}a_{33} - a_{11}a_{22}a_{13}^2 - a_{11}a_{12}^2a_{33} - a_{11}^2a_{23}^2 + 2a_{11}a_{12}a_{13}a_{23} \\ &= a_{11}\left(a_{11}a_{22}a_{33} - a_{22}a_{13}^2 - a_{12}^2a_{33} - a_{11}a_{23}^2 + 2a_{23}a_{12}a_{13}\right) \end{aligned}$$

E, por outro lado,

$$\begin{aligned} \det A &= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{vmatrix} = a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{12} & a_{23} \\ a_{13} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{12} & a_{22} \\ a_{13} & a_{23} \end{vmatrix} \\ &= a_{11}a_{22}a_{33} - a_{22}a_{13}^2 - a_{12}^2a_{33} - a_{11}a_{23}^2 + 2a_{23}a_{12}a_{13} \end{aligned}$$

Então, $d_2 = a_{11}\det A$, pelo que d_2 e $a_{11}\det A$ têm o mesmo sinal, porque $a_{11} > 0$.

Está, assim terminada a demonstração.

Lema 184 *Sejam a,b,c três inteiros não nulos. Então,* $\operatorname{mdc}(\operatorname{mdc}(a,b),c) = \operatorname{mdc}(a,\operatorname{mdc}(b,c))$.

Demonstração

A demonstração está feita no primeiro Capítulo.

Devido à igualdade anterior é costume escrever, apenas $\text{mdc}\,(a,b,c)$.

Lema 185 *Sejam* m_{11}, m_{21}, m_{31}, *tais que* $\text{mdc}\,(m_{11}, m_{21}, m_{31}) = 1$. *Então é possível construir uma matriz* M *de inteiros, de tipo* 3×3, *cuja primeira coluna é constituída pelos números* m_{11}, m_{21}, m_{31} *e tal que* $\det M = 1$.

Demonstração

Observe-se que o facto de termos $\text{mdc}\,(m_{11}, m_{21}, m_{31}) = 1$ não implica que, necessariamente, algum dos números $\text{mdc}\,(m_{11}, m_{21})$, $\text{mdc}\,(m_{11}, m_{31})$, $\text{mdc}\,(m_{21}, m_{31})$ tenha que ser 1. Para justificar esta afirmação, basta considerar os números 6, 10 e 15.

Vejamos alguns casos particulares, antes de fazermos a demonstração para o caso mais geral.

1^o caso: dois dos números m_{11}, m_{21}, m_{31} são nulos.

Se $m_{11} = 1, m_{21} = m_{31} = 0$, então $M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Se $m_{11} = m_{31} = 0, m_{21} = 1$, então $M = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

Se $m_{11} = m_{21} = 0, m_{31} = 1$, então $M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$.

2^o caso: apenas um dos números m_{11}, m_{21}, m_{31} é nulo.

Suponhamos que $m_{31} = 0$.

Então, $\text{mdc}\,(m_{11}, m_{21}) = 1$, pelo que existem $\alpha_1, \alpha_2 \in \mathbb{Z}$, tais que $\alpha_1 m_{11} + \alpha_2 m_{21} = 1$.

Então, $M = \begin{bmatrix} m_{11} & -\alpha_2 & 0 \\ m_{21} & \alpha_1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ é uma solução.

As outras duas situações são análogas, tendo-se, por exemplo:

$M = \begin{bmatrix} m_{11} & 0 & -\alpha_3 \\ 0 & 1 & 0 \\ m_{31} & 0 & \alpha_1 \end{bmatrix}$, se $\alpha_1 m_{11} + \alpha_3 m_{31} = 1$.

$M = \begin{bmatrix} 0 & 0 & 1 \\ m_{21} & -\alpha_3 & 0 \\ m_{31} & \alpha_2 & 0 \end{bmatrix}$, se $\alpha_2 m_{21} + \alpha_3 m_{31} = 1$.

3^o caso: nenhum dos números m_{11}, m_{21}, m_{31} é nulo.

Seja $d = \text{mdc}\,(m_{11}, m_{21})$. Então, existem números inteiros α_1, α_2, que $\alpha_1 m_{11} + \alpha_2 m_{21} = d$, com $\text{mdc}\,(\alpha_1, \alpha_2) = 1$.

Então, existem $\lambda_1, \lambda_2 \in \mathbb{Z}$, tais que $\lambda_1 \alpha_1 + \lambda_2 \alpha_2 = 1$.

Então,

$$1 = \text{mdc}\,(m_{11}, m_{21}, m_{31}) = \text{mdc}\,(\text{mdc}\,(m_{11}, m_{21}), m_{31}) = \text{mdc}\,(d, m_{31})$$

Então, $1 = \beta_1 d + \beta_2 m_{31}$, para certos inteiros β_1, β_2.

Logo, $1 = \beta_1 (\alpha_1 m_{11} + \alpha_2 m_{21}) + \beta_2 m_{31} = \beta_1 \alpha_1 m_{11} + \beta_1 \alpha_2 m_{21} + \beta_2 m_{31}$.

Seja $M = \begin{bmatrix} m_{11} & -\alpha_2 & -\beta_2\lambda_1 \\ m_{21} & \alpha_1 & -\beta_2\lambda_2 \\ m_{31} & 0 & \beta_1 \end{bmatrix}$. Então:

$$\begin{aligned} \det M &= \begin{vmatrix} m_{11} & -\alpha_2 & -\beta_2\lambda_1 \\ m_{21} & \alpha_1 & -\beta_2\lambda_2 \\ m_{31} & 0 & \beta_1 \end{vmatrix} = m_{31} \begin{vmatrix} -\alpha_2 & -\beta_2\lambda_1 \\ \alpha_1 & -\beta_2\lambda_2 \end{vmatrix} + \beta_1 \begin{vmatrix} m_{11} & -\alpha_2 \\ m_{21} & \alpha_1 \end{vmatrix} \\ &= m_{31}\left(\alpha_2\beta_2\lambda_2 + \alpha_1\beta_2\lambda_1\right) + \beta_1\left(\alpha_1 m_{11} + \alpha_2 m_{21}\right) \\ &= m_{31}\beta_2\left(\alpha_2\lambda_2 + \alpha_1\lambda_1\right) + \beta_1 d \\ &= m_{31}\beta_2 \times 1 + \beta_1 d = m_{31}\beta_2 + \beta_1 d = 1 \end{aligned}$$

Está, assim, terminada a demonstração do lema.

Lema 186 *Seja* $Q'\left(x'_1, x'_2, x'_3\right) = \sum_{i,j=1}^{3} a'_{ij} x'_i x'_j$, *com* A' *uma matriz simétrica de inteiros, uma forma quadrática definida positiva. Seja* a *o menor inteiro positivo representável por* Q'. *Então, existe uma forma quadrática* $Q\left(x_1, x_2, x_3\right)$, *tal que* $Q'\left(x'_1, x'_2, x'_3\right) \sim Q\left(x_1, x_2, x_3\right)$ *e* $Q\left(1, 0, 0\right) = a$.

Demonstração

$Q'\left(x'_1, x'_2, x'_3\right) = \sum_{i,j=1}^{3} a'_{ij} x'_i x'_j$. Seja a o menor inteiro positivo representável por $Q'\left(x'_1, x'_2, x'_3\right)$.

Então, $a = Q'\left(m_{11}, m_{21}, m_{31}\right)$, para certos inteiros m_{11}, m_{21}, m_{31} não todos nulos.

Além disso, $\operatorname{mdc}\left(m_{11}, m_{21}, m_{31}\right) = 1$, pois, se tivéssemos $\operatorname{mdc}\left(m_{11}, m_{21}, m_{31}\right) = d > 1$, então seria $0 < Q'\left(\frac{m_{11}}{d}, \frac{m_{21}}{d}, \frac{m_{31}}{d}\right) < Q'\left(m_{11}, m_{21}, m_{31}\right) = a$. Então, a não era o menor inteiro positivo representável por Q'.

Vejamos que existe uma forma quadrática definida positiva $Q\left(x_1, x_2, x_3\right) = \sum_{i,j=1}^{3} a_{ij} x_i x_j = x^T A x$, com A uma matriz simétrica de inteiros, tal que $Q'\left(x'_1, x'_2, x'_3\right) \sim Q\left(x_1, x_2, x_3\right)$ e $a_{11} = a = Q\left(1, 0, 0\right)$.

Ora, pelo lema anterior, existe uma matriz M, de tipo 3×3, cuja primeira coluna é formada pelos números inteiros m_{11}, m_{21}, m_{31}, ficando nas outras duas colunas números inteiros, de modo que $\det M = 1$. Então, fazendo $\begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, isto é, $x' = Mx$, temos $Q'\left(x'_1, x'_2, x'_3\right) = Q'\left(Mx\right) = Q\left(x\right) = Q\left(x_1, x_2, x_3\right)$. Logo, $Q\left(x_1, x_2, x_3\right) \sim Q'\left(x'_1, x'_2, x'_3\right)$.

Então,

$$\begin{aligned} a &= Q'\left(m_{11}, m_{21}, m_{31}\right) \\ &= \begin{bmatrix} m_{11} & m_{21} & m_{31} \end{bmatrix} \begin{bmatrix} a'_{11} & a'_{12} & a'_{13} \\ a'_{12} & a'_{22} & a'_{23} \\ a'_{13} & a'_{23} & a'_{33} \end{bmatrix} \begin{bmatrix} m_{11} \\ m_{21} \\ m_{31} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} m_{11} & m_{21} & m_{31} \\ m_{12} & m_{22} & m_{32} \\ m_{13} & m_{23} & m_{33} \end{bmatrix} \begin{bmatrix} a'_{11} & a'_{12} & a'_{13} \\ a'_{12} & a'_{22} & a'_{23} \\ a'_{13} & a'_{23} & a'_{33} \end{bmatrix} \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = a_{11} \end{aligned}$$

Lema 187 *Em cada classe de formas quadráticas ternárias definidas positivas existe uma forma que satisfaz* $0 < a_{11} \leq \frac{4\sqrt[3]{d_3}}{3}, 2|a_{12}| \leq a_{11}$ *e* $2|a_{13}| \leq a_{11}$. *Tal forma diz-se reduzida.*

Demonstração

Seja $Q'(x'_1, x'_2, x'_3) = \begin{bmatrix} x'_1 & x'_2 & x'_3 \end{bmatrix} \begin{bmatrix} a'_{11} & a'_{12} & a'_{13} \\ a'_{12} & a'_{22} & a'_{23} \\ a'_{13} & a'_{23} & a'_{33} \end{bmatrix} \begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \end{bmatrix} = (x')^T A' x$, com A' uma matriz simétrica de inteiros, Seja a o menor inteiro positivo representável por $Q'(x'_1, x'_2, x'_3)$.

Pelo lema anterior, existe uma forma quadrática inteira definida positiva $Q(x_1, x_2, x_3)$, equivalente a $Q'(x'_1, x'_2, x'_3)$, tal que $Q(1, 0, 0) = c_{11} = a$:

$$Q(x_1, x_2, x_3) = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{12} & c_{22} & c_{23} \\ c_{13} & c_{23} & c_{33} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = x^T C x$$

Seja $N = \begin{bmatrix} 1 & v & w \\ 0 & b_{11} & b_{12} \\ 0 & b_{12} & b_{22} \end{bmatrix}$, com v, w inteiros a determinar e tal que $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{bmatrix}$ seja uma matriz de inteiros de determinante 1. Então, $\det N = 1$.

Seja $x = Ny$. Então, $Q(x_1, x_2, x_3) = Q(x) = Q(Ny) = Q_1(y) = Q_1(y_1, y_2, y_3)$.

E temos $Q'(x'_1, x'_2, x'_3) \sim Q(x_1, x_2, x_3) \sim Q_1(y_1, y_2, y_3)$, pelo que estas três formas representam os mesmos números.

Note-se que $Ny = \begin{bmatrix} 1 & v & w \\ 0 & b_{11} & b_{12} \\ 0 & b_{12} & b_{22} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} y_1 + vy_2 + wy_3 \\ b_{11}y_2 + b_{12}y_3 \\ b_{12}y_2 + b_{22}y_3 \end{bmatrix}$

Então,

$$Q(x_1, x_2, x_3) = x^T C x = y^T N^T C N y = y^T H y = Q_1(y) = Q_1(y_1, y_2, y_3)$$

Ora,

$$\begin{aligned} H &= N^T A N = \begin{bmatrix} 1 & 0 & 0 \\ v & b_{11} & b_{12} \\ w & b_{12} & b_{22} \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{12} & c_{22} & c_{23} \\ c_{13} & c_{23} & c_{33} \end{bmatrix} \begin{bmatrix} 1 & v & w \\ 0 & b_{11} & b_{12} \\ 0 & b_{12} & b_{22} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ v & b_{11} & b_{12} \\ w & b_{12} & b_{22} \end{bmatrix} \begin{bmatrix} c_{11} & c_{11}v + c_{12}b_{11} + c_{13}b_{12} & c_{11}w + c_{12}b_{12} + c_{13}b_{22} \\ c_{12} & c_{12}v + c_{22}b_{11} + c_{23}b_{12} & c_{12}w + c_{22}b_{12} + c_{23}b_{22} \\ c_{13} & c_{13}v + c_{23}b_{11} + c_{33}b_{12} & c_{13}w + c_{23}b_{12} + c_{33}b_{22} \end{bmatrix} \\ &= \begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{12} & h_{22} & h_{23} \\ h_{13} & h_{23} & h_{33} \end{bmatrix} \end{aligned}$$

Por falta de espaço, vamos definir a matriz H, da seguinte maneira:

$h_{11} = c_{11} = a$

$h_{12} = c_{11}v + b_{11}c_{12} + b_{12}c_{13}$

$h_{13} = c_{11}w + b_{12}c_{12} + b_{22}c_{13}$

$h_{22} = v(c_{11}v + b_{11}c_{12} + b_{12}c_{13}) + b_{11}(c_{12}v + b_{11}c_{22} + b_{12}c_{23}) + b_{12}(c_{13}v + b_{11}c_{23} + b_{12}c_{33})$

$h_{23} = w(c_{11}v + b_{11}c_{12} + b_{12}c_{13}) + b_{12}(c_{12}v + b_{11}c_{22} + b_{12}c_{23}) + b_{22}(c_{13}v + b_{11}c_{23} + b_{12}c_{33})$

$h_{33} = w(c_{11}w + b_{12}c_{12} + b_{22}c_{13}) + b_{12}(c_{12}w + b_{12}c_{22} + b_{22}c_{23}) + b_{22}(c_{13}w + b_{12}c_{23} + b_{22}c_{33})$

Então, podemos escolher v e w de modo que $|h_{12}| \leq \frac{a}{2}$ e $|h_{13}| \leq \frac{a}{2}$.

Mas , h_{22} é um elemento da diagonal principal, pelo que é representável por $Q_1(y_1, y_2, y_3)$, tendo-se $h_{22} = Q_1(0, 1, 0) > 0$.

Então, $h_{22} \geq a = h_{11}$, devido à minimalidade de a.
E, como verificado na demonstração dum dos lemas anteriores, temos $h_{11}d_3 = h_{11}h_{22} - h_{12}^2$.
Então:

$$\begin{aligned}
h_{11} \leq h_{22} &\implies h_{11}^2 \leq h_{11}h_{22} \implies h_{11}^2 \leq h_{11}h_{22} - h_{12}^2 + h_{12}^2 \\
&\implies h_{11}^2 \leq \frac{2\sqrt{h_{11}d_3}}{\sqrt{3}} + h_{12}^2 \implies h_{11}^2 \leq \frac{2\sqrt{h_{11}d_3}}{\sqrt{3}} + \frac{h_{11}^2}{4} \\
&\implies \frac{3}{4}h_{11}^2 \leq \frac{2\sqrt{h_{11}d_3}}{\sqrt{3}} \implies \frac{3}{8}h_{11}^2 \leq \frac{\sqrt{h_{11}d_3}}{\sqrt{3}} \\
&\implies \frac{9}{64}h_{11}^4 \leq \frac{h_{11}d_3}{3} \implies \frac{27}{64}h_{11}^3 \leq d_3 \\
&\implies h_{11}^3 \leq \frac{64}{27}d_3 \implies h_{11} \leq \frac{4}{3}\sqrt[3]{d_3}
\end{aligned}$$

Está, assim terminada a demonstração (H é a matriz A do enunciado).

Corolário 188 *Toda a forma quadrática ternária definida positiva, de discriminante* 1*, é equivalente a uma soma de três quadrados.*

Demonstração

Seja $Q'(x_1', x_2', x_3') = \begin{bmatrix} x_1' & x_2' & x_3' \end{bmatrix} \begin{bmatrix} a_{11}' & a_{12}' & a_{13}' \\ a_{12}' & a_{22}' & a_{23}' \\ a_{13}' & a_{23}' & a_{33}' \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \\ x_3' \end{bmatrix} = (x')^T A' x$, com A' uma matriz simétrica de inteiros tal que $\det A' = 1$.

Pelo lema anterior, existe uma forma quadrática $Q(x_1, x_2, x_3)$, equivalente a $Q'(x_1', x_2', x_3')$, tal que

$$Q(x_1, x_2, x_3) = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},$$

com $0 < a_{11} \leq \frac{4}{3}\sqrt[3]{d_3} = \frac{4}{3}$. Logo, $a_{11} = 1$.

Além disso, temos $|a_{12}| \leq \frac{1}{2}$. Como a_{12} é um número inteiro, vem $a_{12} = 0$.

Analogamente, $|a_{13}| \leq \frac{1}{2}$, pelo que $a_{13} = 0$.

Então, $Q(x_1, x_2, x_3) = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ 0 & a_{23} & a_{33} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, com $\begin{vmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{vmatrix} = 1$.

Então, $Q(x_1, x_2, x_3) = x_1^2 + \begin{bmatrix} x_2 & x_3 \end{bmatrix} \begin{bmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{bmatrix} \begin{bmatrix} x_2 \\ x_3 \end{bmatrix}$, com $\begin{vmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{vmatrix} = 1$.

Então, $\begin{bmatrix} x_2 & x_3 \end{bmatrix} \begin{bmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{bmatrix} \begin{bmatrix} x_2 \\ x_3 \end{bmatrix}$ é equivalente a uma soma de dois quadrados, porque temos $a_{22} > 0$ e $\begin{vmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{vmatrix} = 1$.

Então, $Q(x_1, x_2, x_3)$ é equivalente a uma soma de três quadrados, como se pretendia provar.

Proposição 189 *A equação $x_1^2 + x_2^2 + x_3^2 = n$ tem solução, isto é, dado o número natural n, existem inteiros x_1, x_2, x_3, tais que $x_1^2 + x_2^2 + x_3^2 = n$, se e só se, n não é da forma $4^a(8k+7)$, com $a, k \in \mathbb{N}_0$.*

Demonstração

Já vimos que nenhum número natural da forma $8m - 1$ (logo da forma $8k + 7$) é soma de três quadrados.

Suponhamos, agora, que $x_1^2+x_2^2+x_3^2=n=4^a\,(8k+7)$, com $a,k\in\mathbb{N}_0$ e $a\geq 1$.

Como n é par, x_1, x_2, x_3 são todos pares ou um deles é par e os outros dois são ímpares. Neste último caso, era $n=x_1^2+x_2^2+x_3^2\equiv 0+1+1\equiv 2\,(\mathrm{mod}\,4)$, o que contradizia o facto de n ser um múltiplo de 4.

Logo, x_1, x_2 e x_3 são todos pares. Então teremos $x_1=2^{a_1}y_1$, $x_2=2^{a_2}y_2$ e $x_3=2^{a_3}y_3$, com y_1, y_2, y_3 todos ímpares e, sem perda de generalidade, $a_1\leq a_2\leq a_3$. Então:

$$\begin{aligned} n &= x_1^2+x_2^2+x_3^2=4^{a_1}y_1^2+4^{a_2}y_2^2+4^{a_3}y_3^2\\ &= 4^{a_1}\left(y_1^2+4^{a_2-a_1}y_2^2+4^{a_3-a_1}y_3^2\right)\end{aligned}$$

Fazendo $a_1=a$, $a_2-a_1=b\geq 0$ e $a_3-a_1=c\geq b\geq 0$, temos

$$n=4^a\left(y_1^2+4^by_2^2+4^cy_3^2\right)$$

Se $b\geq 2$, então $c\geq 2$, pelo que $y_1^2+4^by_2^2+4^cy_3^2\equiv 1\,(\mathrm{mod}\,8)$.
Se $b=1$ e $c\geq 2$, então $y_1^2+4^by_2^2+4^cy_3^2\equiv 5\,(\mathrm{mod}\,8)$.
Se $b=1$ e $c=1$, então $y_1^2+4^by_2^2+4^cy_3^2\equiv 1\,(\mathrm{mod}\,8)$.
Se $b=0$ e $c\geq 2$, então $y_1^2+4^by_2^2+4^cy_3^2\equiv 2\,(\mathrm{mod}\,8)$.
Se $b=0$ e $c=1$, então $y_1^2+4^by_2^2+4^cy_3^2\equiv 6\,(\mathrm{mod}\,8)$.
Se $b=0$ e $c=0$, então $y_1^2+4^by_2^2+4^cy_3^2\equiv 3\,(\mathrm{mod}\,8)$.
Então, n não é da forma $4^a\,(8k+7)$, com $a,k\in\mathbb{N}_0$.

Reciprocamente, suponhamos que n não é da forma $4^a\,(8k+7)$, com $a,k\in\mathbb{N}_0$.

Se n é múltiplo de 4 e $n=x_1^2+x_2^2+x_3^2$, então x_1, x_2 e x_3 são todos números pares, pelo que existem certos números naturais y_1, y_2, y_3, tais que $n=4y_1^2+4y_2^2+4y_3^2=4\left(y_1^2+y_2^2+y_3^2\right)=4n_1$, com $n_1=y_1^2+y_2^2+y_3^2$, uma soma de três quadrados. E o processo prossegue até obtermos um certo n_i que não seja múltiplo de 4.

Então, interessa-nos, apenas, considerar os casos em que $n=8k+m$, com $m\in\{1,2,3,5,6\}$.

Pretendemos encontrar uma forma quadrática $Q\,(x_1,x_2,x_3)=x^TAx$, tal que n seja representável por Q. Como pretendemos que a matriz A seja simétrica, temos, no total, 9 parâmetros (6 entradas de A e os valores x_1,x_2,x_3).

Se o problema tiver solução, então terá uma infinidade de soluções, pois há infinitas formas quadráticas equivalentes.

Seja $Q\,(x_1,x_2,x_3)=a_{11}x_1^2+2a_{12}x_1x_2+2x_1x_3+a_{22}x_2^2+nx_3^2$.

Então,

$$Q\,(x_1,x_2,x_3)=\begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}\begin{bmatrix}a_{11} & a_{12} & 1\\ a_{12} & a_{22} & 0\\ 1 & 0 & n\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}=x^TAx$$

Para que A seja positiva definida, deverão ser verificadas as condições $a_{11}>0$, $a_{11}a_{22}-a_{12}^2>0$ e $d_3=\begin{vmatrix}a_{11} & a_{12} & 1\\ a_{12} & a_{22} & 0\\ 1 & 0 & n\end{vmatrix}=\left(a_{11}a_{22}-a_{12}^2\right)n-a_{22}>0$.

E se $d_3=1$, ou seja, se $a_{22}=\left(a_{11}a_{22}-a_{12}^2\right)n-1$, então $Q\,(x_1,x_2,x_3)$ será equivalente a uma soma de três quadrados.

Seja $b=a_{11}a_{22}-a_{12}^2$. Então, $a_{22}=nb-1$.

Se $n=1=1^2+0^2+0^2$, então n é soma de três quadrados, pelo que podemos supor $n\geq 2$.

Se $n\geq 2$, então $a_{22}=nb-1\geq 2b-1>0$.

Mas, se $a_{11}a_{22}-a_{12}^2>0$, podemos concluir que $a_{11}>0$, pelo que nos basta considerar as duas condições $b=a_{11}a_{22}-a_{12}^2>0$ e $\left(a_{11}a_{22}-a_{12}^2\right)n-a_{22}>0$.

Mas, de $b = a_{11}a_{22} - a_{12}^2$, conclui-se que $a_{11}a_{22} = b + a_{12}^2$, donde vem $a_{11} = \frac{b+a_{12}^2}{a_{22}}$.

A dificuldade principal consiste em fazer com que a_{11} seja um número natural.

Para que isso aconteça, devemos ter $-b \equiv a_{12}^2 \pmod{a_{22}}$, ou seja, pretendemos que $-b$ seja um resíduo quadrático, módulo a_{22}, para podermos escolher a_{12}, como uma solução da congruência quadrática $x^2 \equiv -b \pmod{a_{22}}$.

Como encontrar a_{22}?

1^o caso: $n \equiv 2 \pmod 4$

Então, $n = 4a + 2$, para certo inteiro a.

Vejamos que $\text{mdc}\,(4n, n-1) = 1$:

Seja $d = \text{mdc}\,(4n, n-1)$. Então, d divide $4n$ e d divide $n-1$. Então, d divide $4n - 4\,(n-1)$. Logo, d divide 4. Mas, d não pode ser par (porque $n-1$ é ímpar). Logo, $d = 1$.

Então, pelo importante Teorema devido a Dirichlet já antes referido, na progressão aritmética de 1^o termo $n-1$ e razão $4n$, há infinitos primos. Seja p um desses primos.

Então, $p = n - 1 + 4nm = n\,(4m+1) - 1$, com m inteiro, ou seja, $p = nb - 1$, com $b = 4m + 1$, donde vem $b \equiv 1 \pmod 4$.

E, como $n \equiv 1 \pmod 4$, então $p = nb - 1 \equiv 2 \times 1 - 1 \equiv 1 \pmod 4$.

Então, $\left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right) \times \left(\frac{b}{p}\right) = 1 \times \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right) = \left(\frac{nb-1}{b}\right) = \left(\frac{-1}{4m+1}\right) = 1$.

Note-se que o número de factores congruentes com 3, módulo 4, que ocorrem em $4m+1$, tem de ser par.

Logo, $-b$ é resíduo quadrático, módulo p, pelo que existe $a_{12} \in \mathbb{Z}$, tal que p divide $b + a_{12}^2$, pelo que podemos fazer $a_{11} = \frac{b+a_{12}^2}{p}$ e $a_{22} = p = nb - 1$.

2^o caso: $n \equiv 1 \pmod 8$

Então, $n = 8t + 1$, para certo inteiro t.

Vejamos que $\text{mdc}\left(4n, \frac{3n-1}{2}\right) = 1$:

Como $n = 8t + 1$, então $4n = 32t + 4$ e $\frac{3(8t+1)-1}{2} = 12t + 1$.

Suponhamos que d divide $4n$ e d divide $\frac{3n-1}{2}$.

Então, d divide $32t + 4$ e d divide $12t + 1$. Então, d é ímpar.

Então, d divide $8t + 1$ e d divide $12t + 1$.

Logo, d divide $4t$, pelo que d divide t. Mas, se d divide t e d divide $12t + 1$, então d divide 1.

Logo, $\text{mdc}\left(4n, \frac{3n-1}{2}\right) = 1$.

Então, na progressão aritmética de 1^o termo $\frac{3n-1}{2}$ e razão $4n$, há infinitos números primos. Seja p um desses primos. Então, $p = \frac{3n-1}{2} + 4nm$, com m inteiro.

Então, $2p = 3n - 1 + 8nm = n\,(8m+3) - 1 = nb - 1$, com $b = 8m + 3 = \frac{2p+1}{n}$. Então, $b \equiv 3 \pmod 8$.

Logo, $2p \equiv 3 \times 1 - 1 \equiv 2 \pmod 8$, donde vem $p \equiv 1 \pmod 4$.

Então:

$\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right) \times \left(\frac{2}{b}\right) = (-1) \times (-1) = 1$

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

Então,

$$\left(\frac{-b}{p}\right) = \left(\frac{-2}{b}\right) \times \left(\frac{-b}{p}\right) = \left(\frac{-2}{b}\right) \times \left(\frac{p}{b}\right) = \left(\frac{-2p}{b}\right) = \left(\frac{1-nb}{b}\right) = \left(\frac{1}{b}\right) = 1$$

Logo, $-b$ é resíduo quadrático, módulo p.

Como as congruências $x^2 \equiv -b \pmod p$ e $x^2 \equiv -b \pmod 2$ têm solução, então a congruência $x^2 \equiv -b \pmod{2p}$ também tem solução. Uma tal solução será a_{12}, sendo $a_{22} = 2p$ e $a_{11} = \frac{b+a_{12}^2}{2p}$.

3^o caso: $n \equiv 5 \pmod 8$

Então, $n = 5 + 8t$, para certo inteiro t. Vejamos que que $\text{mdc}\left(4n, \frac{3n-1}{2}\right) = 1$:

Como $n = 8t + 1$, então $4n = 32t + 4$ e $\frac{3(8t+1)-1}{2} = 12t + 1$.

Suponhamos que d divide $4n$ e d divide $\frac{3n-1}{2}$.

Então, d divide $32t+4$ e d divide $12t+1$. Então, d é ímpar.

Então, d divide $8t+1$ e d divide $12t+1$.

Logo, d divide $4t$, pelo que d divide t. Mas, se d divide t e d divide $12t+1$, então d divide 1.

Logo, $\text{mdc}\left(4n, \frac{3n-1}{2}\right) = 1$.

Então, na progressão aritmética de 1^o termo $\frac{3n-1}{2}$ e razão $4n$, há infinitos números primos. Seja p um desses primos. Então, $p = \frac{3n-1}{2} + 4nm$, com m inteiro.

Então, $2p = 3n - 1 + 8nm = n(8m+3) - 1 = nb - 1$, com $b = 8m+3 = \frac{2p+1}{n}$.

Então, $b \equiv 3 \pmod 8$, donde se conclui que $b \equiv 3 \pmod 4$.

Logo, $2p \equiv 3 \times 5 - 1 \equiv 6 \pmod 8$, donde vem $p \equiv 3 \pmod 4$.

Então:

$\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right) \times \left(\frac{2}{b}\right) = (-1) \times (-1) = 1$

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

Então,

$$\left(\frac{-b}{p}\right) = \left(\frac{p}{b}\right) \times 1 = \left(\frac{-b}{p}\right) \times \left(\frac{-2}{b}\right) = \left(\frac{p}{b}\right) \times \left(\frac{-2}{b}\right) = \left(\frac{-2p}{b}\right) = \left(\frac{1-nb}{b}\right) = \left(\frac{1}{b}\right) = 1$$

Logo, $-b$ é resíduo quadrático, módulo p.

Como as congruências $x^2 \equiv -b \pmod p$ e $x^2 \equiv -b \pmod 2$ têm solução, então a congruência $x^2 \equiv -b \pmod{2p}$ também tem solução. Uma tal solução será a_{12}, sendo $a_{22} = 2p$ e $a_{11} = \frac{b+a_{12}^2}{2p}$.

4^o caso: $n \equiv 3 \pmod 8$

Então, $n = 8t+3$, para certo inteiro t. Vejamos que $\text{mdc}\left(4n, \frac{n-1}{2}\right) = 1$:

Como $n = 8t+3$, então $4n = 32t+12$ e $\frac{n-1}{2} = \frac{8t+2}{2} = 4t+1$.

Suponhamos que d divide $4n$ e d divide $\frac{n-1}{2}$.

Então, d divide $32t+4$ e d divide $4t+1$. Então, d é ímpar. Então, d divide $8t+1$ e d divide $8t+2$. Logo, d divide 1. Logo, $\text{mdc}\left(4n, \frac{3n-1}{2}\right) = 1$.

Então, na progressão aritmética de 1^o termo $\frac{n-1}{2}$ e razão $4n$, há infinitos números primos. Seja p um desses primos. Então, $p = \frac{n-1}{2} + 4nm$, com m inteiro.

Então, $2p = n - 1 + 8nm = n(8m+1) - 1 = nb - 1$, com $b = 8m+1 = \frac{2p+1}{n}$. Então, $b \equiv 1 \pmod 8$.

Logo, $2p \equiv 2 \pmod 8$, donde vem $p \equiv 1 \pmod 4$.

Então:

$\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right) \times \left(\frac{2}{b}\right) = 1 \times 1 = 1$

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

Então,

$$\left(\frac{-b}{p}\right) = \left(\frac{p}{b}\right) \times 1 = \left(\frac{p}{b}\right) \times \left(\frac{-2}{b}\right) = \left(\frac{-2p}{b}\right) = \left(\frac{1-nb}{b}\right) = \left(\frac{1}{b}\right) = 1$$

Logo, $-b$ é resíduo quadrático, módulo p.

Como as congruências $x^2 \equiv -b \pmod p$ e $x^2 \equiv -b \pmod 2$ têm solução, então a congruência $x^2 \equiv -b \pmod{2p}$ também tem solução. Uma tal solução será a_{12}, sendo $a_{22} = 2p$ e $a_{11} = \frac{b+a_{12}^2}{2p}$.

Em qualquer dos casos obtivemos uma matriz de inteiros, cujo determinante é 1.

Então, (a correspondente forma quadrática, que é definida positiva), é equivalente a uma soma de três quadrados.

Está, assim, terminada a demonstração da proposição.

Exemplo 190 *Vejamos como decompor* 33 *numa soma de três quadrados, aplicando o processo descrito nas demonstrações anteriores.*

Seja $A' = \begin{bmatrix} a'_{11} & a'_{12} & 1 \\ a'_{12} & a'_{22} & 0 \\ 1 & 0 & 33 \end{bmatrix}$.

Como $33 \equiv 1 \pmod 8$ e $\text{mdc}\left(4 \times 33, \frac{3\times 33-1}{2}\right) = \text{mdc}\,(4 \times 33, 49) = 1$, escolhemos um número primo congruente com 49, módulo 132. O menor primo p nessas condições é $p = 181$.

Então, $2p = 362 = a'_{22}$ e $b = \frac{2\times 181+1}{33} = 11$.

Seguidamente, procuramos uma solução da congruência quadrática $x^2 \equiv -11 \pmod{181}$, o que pode ser feito numa calculadora gráfica ou numa folha de cálculo, encontrando-se para x, o valor ímpar 129.

Note-se que pretendemos uma solução ímpar, para que a solução da congruência $x^2 \equiv -11 \pmod{181}$, também seja solução da congruência $x^2 \equiv -11 \pmod{362}$. Repare-se que $\frac{129^2+11}{362} = 46$, pelo que $129^2 \equiv -11 \pmod{362}$.

Logo, $a'_{12} = 129$ e $a'_{11} = 46$. Então, $A' = \begin{bmatrix} 46 & 129 & 1 \\ 129 & 362 & 0 \\ 1 & 0 & 33 \end{bmatrix}$.

Logo, $\det A' = \begin{vmatrix} 46 & 129 & 1 \\ 129 & 362 & 0 \\ 1 & 0 & 33 \end{vmatrix} = 1$, conforme podemos verificar:

$$\begin{aligned} \begin{vmatrix} 46 & 129 & 1 \\ 129 & 362 & 0 \\ 1 & 0 & 33 \end{vmatrix} &= 33 \begin{vmatrix} 46 & 129 \\ 129 & 362 \end{vmatrix} + \begin{vmatrix} 129 & 1 \\ 362 & 0 \end{vmatrix} = 33\left(46 \times 362 - 129^2\right) - 362 \\ &= 33\,(16\,652 - 16\,641) - 362 = 33 \times 11 - 362 = 363 - 362 = 1 \end{aligned}$$

Seja $Q'\,(x'_1, x'_2, x'_3) = \begin{bmatrix} x'_1 & x'_2 & x'_3 \end{bmatrix} \begin{bmatrix} 46 & 129 & 1 \\ 129 & 362 & 0 \\ 1 & 0 & 33 \end{bmatrix} \begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \end{bmatrix}$.

Então $Q'\,(x'_1, x'_2, x'_3) = 46\,(x'_1)^2 + 362\,(x'_2)^2 + 33\,(x'_3)^2 + 258x'_1x'_2 + 2x'_1x'_3$.

Mas, $46 > 0$, $\begin{vmatrix} 46 & 129 \\ 129 & 362 \end{vmatrix} = 11 > 0$ e $\begin{vmatrix} 46 & 129 & 1 \\ 129 & 362 & 0 \\ 1 & 0 & 33 \end{vmatrix} = 1 > 0$.

Então, $Q'\,(x'_1, x'_2, x'_3)$ é uma forma quadrática ternária definida positiva e A' é uma matriz simétrica de inteiros, cujo determinante é 1.

Logo,

$$\begin{aligned} 46Q'\left(x'_1, x'_2, x'_3\right) &= 46^2\left(x'_1\right)^2 + 362 \times 46\left(x'_2\right)^2 + 33 \times 46\left(x'_3\right)^2 + 258 \times 46x'_1x'_2 + 92x'_1x'_3 \\ &= \left(46x'_1 + 129x'_2 + x'_3\right)^2 + 11(x'_2)^2 + 1517(x'_3)^2 - 258x'_2x'_3 \end{aligned}$$

Então, $Q'_1\,(x'_2, x'_3) = 11(x'_2)^2 + 1517(x'_3)^2 - 258x'_2x'_3 = \begin{bmatrix} x'_2 & x'_3 \end{bmatrix} \begin{bmatrix} 11 & 129 \\ 129 & 1517 \end{bmatrix} \begin{bmatrix} x'_2 \\ x'_3 \end{bmatrix}$.

Então:

$$11Q'_1\left(x'_2, x'_3\right) = 121(x'_2)^2 + 16\,687(x'_3)^2 - 2838x'_2x'_3$$

$46\,(-28)^2 + 362\,(10)^2 + 33\,(1)^2 + 258\,(-28)\,10 - 56 = 1$

E, com algumas contas, chegamos à conclusão que $Q'\,(-28, 10, 1) = 1$.

Logo, 1 é o menor inteiro positivo representável por Q'.

Seja $M=\begin{bmatrix}-28 & 1 & 0\\ 10 & 0 & 1\\ 1 & 0 & 0\end{bmatrix}$. Então, $\det M=1$. Seja $A=M^TA'M$. Então:

$$\begin{aligned}A &= \begin{bmatrix}-28 & 10 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}\begin{bmatrix}46 & 129 & 1\\ 129 & 362 & 0\\ 1 & 0 & 33\end{bmatrix}\begin{bmatrix}-28 & 1 & 0\\ 10 & 0 & 1\\ 1 & 0 & 0\end{bmatrix}\\ &= \begin{bmatrix}-28 & 10 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}\begin{bmatrix}3 & 46 & 129\\ 8 & 129 & 362\\ 5 & 1 & 0\end{bmatrix}=\begin{bmatrix}1 & 3 & 8\\ 3 & 46 & 129\\ 8 & 129 & 362\end{bmatrix}\end{aligned}$$

Seja,

$$\begin{aligned}Q_1(x_1,x_2,x_3) &= \begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}\begin{bmatrix}-28 & 10 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}\begin{bmatrix}46 & 129 & 1\\ 129 & 362 & 0\\ 1 & 0 & 33\end{bmatrix}\begin{bmatrix}-28 & 1 & 0\\ 10 & 0 & 1\\ 1 & 0 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}\\ &= \begin{bmatrix}x_1 & x_2 & x_3\end{bmatrix}\begin{bmatrix}1 & 3 & 8\\ 3 & 46 & 129\\ 8 & 129 & 362\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}\end{aligned}$$

É claro que $Q'(0,0,1)=33$. Ora, $Q_1(1,0,0)=1$ e $Q_1(1,28,-10)=33$.
Para descobrir que $Q_1(1,28,-10)=33$, faz-se

$$\begin{bmatrix}0\\ 0\\ 1\end{bmatrix}=\begin{bmatrix}-28 & 1 & 0\\ 10 & 0 & 1\\ 1 & 0 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}=\begin{bmatrix}-28x_1+x_2\\ 10x_1+x_3\\ x_1\end{bmatrix}$$

Logo, $x_1=1$, $10+x_3=0$ e $-28+x_2=0$. Então, $x_1=1$, $x_2=28$ e $x_3=-10$.
Continuemos:
Ora, $Q_1(x_1,x_2,x_3)=x_1^2+46x_2^2+362x_3^2+6x_1x_2+16x_1x_3+258x_2x_3$.
E $[L(x_1,x_2,x_3)]^2=(x_1+3x_2+8x_3)^2=x_1^2+6x_1x_2+16x_1x_3+9x_2^2+48x_2x_3+64x_3^2$.
Então,

$$\begin{aligned}\widetilde{Q}_1(x_2,x_3) &= Q_1(x_1,x_2,x_3)-[L(x_1,x_2,x_3)]^2\\ &= 37x_2^2+298x_3^2+210x_2x_3\end{aligned}$$

Então, $37\widetilde{Q}_1(x_2,x_3)=37^2x_2^2+298\times 37x_3^2+210\times 37x_2x_3$.
Ora,

$$\begin{aligned}37^2x_2^2+298\times 37x_3^2+210\times 37x_2x_3 &= (37x_2+105x_3)^2-11025x_3^2+11\,026x_3^2\\ &= (37x_2+105x_3)^2+x_3^2\end{aligned}$$

E daqui se conclui que $37\widetilde{Q}_1(3,-1)=37$, pelo que $\widetilde{Q}_1(3,-1)=1$.
Seja $B=\begin{bmatrix}3 & s\\ -1 & u\end{bmatrix}$. Pretendemos que $=1$. Logo, $3u+s=1$.
Uma solução particular da equação anterior é $u=0, s=1$, enquanto que a solução geral é dada por $u=0-t, s=1+3t$. Logo, $B=\begin{bmatrix}3 & 1+3t\\ -1 & -t\end{bmatrix}$.

Fazendo $\begin{bmatrix} x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 3 & 1+3t \\ -1 & -t \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}$, obtemos:

$$\begin{aligned} \widetilde{Q}_2(y_2, y_3) &= \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}^T \begin{bmatrix} 3 & -1 \\ 1+3t & -t \end{bmatrix} \begin{bmatrix} 37 & 105 \\ 105 & 298 \end{bmatrix} \begin{bmatrix} 3 & 1+3t \\ -1 & -t \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} \\ &= \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}^T \begin{bmatrix} 3 & -1 \\ 1+3t & -t \end{bmatrix} \begin{bmatrix} 6 & 37+6t \\ 17 & 105+17t \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} \\ &= \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}^T \begin{bmatrix} 1 & 6+t \\ 6+t & 37+12t+t^2 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} \end{aligned}$$

Para $t = -6$, temos $\widetilde{Q}_2(y_2, y_3) = \begin{bmatrix} y_2 & y_3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} = y_2^2 + y_3^2$.

Além disso, temos $B = \begin{bmatrix} 3 & 1+3t \\ -1 & -t \end{bmatrix} = \begin{bmatrix} 3 & -17 \\ -1 & 6 \end{bmatrix}$.

Seja $N = \begin{bmatrix} 1 & v & w \\ 0 & 3 & -17 \\ 0 & -1 & 6 \end{bmatrix}$, com v, w inteiros a escolher mais tarde. Então:

$$\begin{aligned} N^T A N &= \begin{bmatrix} 1 & 0 & 0 \\ v & 3 & -1 \\ w & -17 & 6 \end{bmatrix} \begin{bmatrix} 1 & 3 & 8 \\ 3 & 46 & 129 \\ 8 & 129 & 362 \end{bmatrix} \begin{bmatrix} 1 & v & w \\ 0 & 3 & -17 \\ 0 & -1 & 6 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ v & 3 & -1 \\ w & -17 & 6 \end{bmatrix} \begin{bmatrix} 1 & v+1 & w-3 \\ 3 & 3v+9 & 3w-8 \\ 8 & 8v+25 & 8w-21 \end{bmatrix} \end{aligned}$$

Fazendo $v = -1$ e $w = 3$, obtemos

$$N^T A N = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 3 & -1 \\ 3 & -17 & 6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 3 & 6 & 1 \\ 8 & 17 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Então, a matriz inversa de $\begin{bmatrix} 1 & 0 & 0 \\ -1 & 3 & -1 \\ 3 & -17 & 6 \end{bmatrix}$ é $\begin{bmatrix} 1 & 0 & 0 \\ 3 & 6 & 1 \\ 8 & 17 & 3 \end{bmatrix}$.

Logo, a matriz inversa de $\begin{bmatrix} 1 & -1 & 3 \\ 0 & 3 & -17 \\ 0 & -1 & 6 \end{bmatrix}$ é $\begin{bmatrix} 1 & 3 & 8 \\ 0 & 6 & 17 \\ 0 & 1 & 3 \end{bmatrix}$.

Então, $\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 8 \\ 0 & 6 & 17 \\ 0 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 28 \\ -10 \end{bmatrix} = \begin{bmatrix} 5 \\ -2 \\ -2 \end{bmatrix}$.

Logo, $33 = 5^2 + (-2)^2 + (-2)^2 = 5^2 + 2^2 + 2^2$.

Exemplo 191 *Vejamos como decompor* 30 *numa soma de três quadrados, aplicando o processo descrito nas demonstrações anteriores.*

Seja $A' = \begin{bmatrix} a'_{11} & a'_{12} & 1 \\ a'_{12} & a'_{22} & 0 \\ 1 & 0 & 30 \end{bmatrix}$.

Como $30 \equiv 2 \pmod 4$ e $\text{mdc}\,(4 \times 30, 30-1) = \text{mdc}\,(120, 29) = 1$, escolhemos um número primo congruente com 29, módulo 120. O menor primo p nessas condições é $p = 29$.

Então, $p = 29 = a'_{22}$ e $b = \frac{29+1}{30} = 1$. Uma solução da congruência $x^2 \equiv -1 \pmod{29}$ é 14!. Ora:

$5! \equiv 120 \equiv 4 \pmod{29}$ $\quad$ $9! \equiv 72 \times (-6) \equiv 3 \pmod{29}$ $\quad$ $13! \equiv 11 \times 156 \equiv 5 \pmod{29}$
$7! \equiv 42 \times 4 \equiv -6 \pmod{29}$ $\quad$ $11! \equiv 110 \times 3 \equiv 11 \pmod{29}$ $\quad$ $14! \equiv 14 \times 5 \equiv 12 \pmod{29}$

Logo, $a'_{12} = 12$ e $a'_{11} = \frac{12^2+1}{29} = 5$. Então, $A' = \begin{bmatrix} 5 & 12 & 1 \\ 12 & 29 & 0 \\ 1 & 0 & 30 \end{bmatrix}$.

Seja $Q'(x'_1, x'_2, x'_3) = \begin{bmatrix} x'_1 & x'_2 & x'_3 \end{bmatrix} \begin{bmatrix} 5 & 12 & 1 \\ 12 & 29 & 0 \\ 1 & 0 & 30 \end{bmatrix} \begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \end{bmatrix}$.

Então $Q'(x'_1, x'_2, x'_3) = 5(x'_1)^2 + 29(x'_2)^2 + 30(x'_3)^2 + 24x'_1x'_2 + 2x'_1x'_3$.

Mas, $\begin{vmatrix} 5 & 12 & 1 \\ 12 & 29 & 0 \\ 1 & 0 & 30 \end{vmatrix} = 1 > 0, \begin{vmatrix} 5 & 12 \\ 12 & 29 \end{vmatrix} = 1 > 0, a'_{11} = 5 > 0.$

Logo, $Q'(x'_1, x'_2, x'_3)$ é uma forma quadrática positiva definida e A' é uma matriz de inteiros, simétrica e de determinante 1. Ora,

$$\begin{aligned} 5Q'(x'_1, x'_2, x'_3) &= 25(x'_1)^2 + 145(x'_2)^2 + 150(x'_3)^2 + 120x'_1x'_2 + 10x'_1x'_3 \\ &= (5x'_1 + 12x'_2 + x'_3)^2 + Q'_1(x'_2, x'_3) \end{aligned}$$

Logo,

$$\begin{aligned} Q'_1(x'_2, x'_3) &= 25(x'_1)^2 + 145(x'_2)^2 + 150(x'_3)^2 + 120x'_1x'_2 + 10x'_1x'_3 - (5x'_1 + 12x'_2 + x'_3)^2 \\ &= (x'_2)^2 + 149(x'_3)^2 - 24x'_2x'_3 = (x'_2 - 12x'_3)^2 + 5(x'_3)^2 \end{aligned}$$

Então, $Q'_1(1, 0) = 1$ e $5Q'(x'_1, 1, 0) = (5x'_1 + 12)^2 + 1$.

O mínimo não nulo de $5Q'(x'_1, x'_2, x'_3)$ ocorre para $x'_1 = -2, x'_2 = 1, x'_3 = 0$, sendo $5Q'(-2, 1, 0) = 5$, pelo que $Q'(-2, 1, 0) = 1$.

Logo, 1 é representável por $Q'(x'_1, x'_2, x'_3)$. E é claro que $Q'(0, 0, 1) = 30$.

Seja $M = \begin{bmatrix} -2 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Então, $\begin{vmatrix} -2 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1.$

Seja $A = M^T A' M$. Então,

$$\begin{aligned} A &= \begin{bmatrix} -2 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 12 & 1 \\ 12 & 29 & 0 \\ 1 & 0 & 30 \end{bmatrix} \begin{bmatrix} -2 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} -2 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & -7 & 1 \\ 5 & -17 & 0 \\ -2 & 1 & 30 \end{bmatrix} = \begin{bmatrix} 1 & -3 & -2 \\ -3 & 10 & 1 \\ -2 & 1 & 30 \end{bmatrix} \end{aligned}$$

Logo,

$$\begin{aligned}
Q'\left(x_1', x_2', x_3'\right) &= \begin{bmatrix} x_1' & x_2' & x_3' \end{bmatrix} \begin{bmatrix} 5 & 12 & 1 \\ 12 & 29 & 0 \\ 1 & 0 & 30 \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \\ x_3' \end{bmatrix} \\
&= \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} 1 & -3 & -2 \\ -3 & 10 & 1 \\ -2 & 1 & 30 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \\
&= \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} x_1 - 3x_2 - 2x_3 \\ -3x_1 + 10x_2 + x_3 \\ -2x_1 + x_2 + 30x_3 \end{bmatrix} \\
&= x_1^2 + 10x_2^2 + 30x_3^2 - 6x_1x_2 - 4x_1x_3 + 2x_2x_3 \\
&= \left(x_1 - 3x_2 - 2x_3\right)^2 + Q_1\left(x_2, x_3\right)
\end{aligned}$$

Então,

$$\begin{aligned}
\widetilde{Q}_1\left(x_2, x_3\right) &= x_1^2 + 10x_2^2 + 30x_3^2 - 6x_1x_2 - 4x_1x_3 + 2x_2x_3 - \left(x_1 - 3x_2 - 2x_3\right)^2 \\
&= x_2^2 + 26x_3^2 - 10x_2x_3
\end{aligned}$$

Logo, $Q_1\left(x_1, x_2, x_3\right) = x_1^2 + 10x_2^2 + 30x_3^2 - 6x_1x_2 - 4x_1x_3 + 2x_2x_3$.
E, $\widetilde{Q}_1\left(x_2, x_3\right) = x_2^2 + 26x_3^2 - 10x_2x_3$.
Então, $Q_1\left(1, 0, 0\right) = 1$ e $Q_1\left(0, 0, 1\right) = 30$.
Por outro lado, $\widetilde{Q}_1\left(x_2, x_3\right) = x_2^2 + 26x_3^2 - 10x_2x_3 = \left(x_2 - 5x_3\right)^2 + x_3^2$.
Então, $\widetilde{Q}_1\left(1, 0\right) = 1$.
Seja $B = \begin{bmatrix} 1 & s \\ 0 & u \end{bmatrix}$. Pretendemos $\det B = 1$, pelo que $u = 1$ e s pode ser qualquer.
Logo, $B = \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}$. Fazendo $\begin{bmatrix} x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}$, obtemos:

$$\begin{aligned}
\widetilde{Q}_2\left(y_2, y_3\right) &= \begin{bmatrix} y_2 & y_3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ s & 1 \end{bmatrix} \begin{bmatrix} 1 & -5 \\ -5 & 26 \end{bmatrix} \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} \\
&= \begin{bmatrix} y_2 & y_3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ s & 1 \end{bmatrix} \begin{bmatrix} 1 & s - 5 \\ -5 & -5s + 26 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} \\
&= \begin{bmatrix} y_2 & y_3 \end{bmatrix} \begin{bmatrix} 1 & s - 5 \\ s - 5 & s^2 - 10s + 26 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}
\end{aligned}$$

Fazendo $s = 5$, obtemos $\widetilde{Q}_2\left(y_2, y_3\right) = \begin{bmatrix} y_2 & y_3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix} = y_2^2 + y_3^2$.

Além disso, $B = \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}$. Seja $N = \begin{bmatrix} 1 & v & w \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{bmatrix}$, com v, w inteiros a determinar.

Então:

$$\begin{aligned}
N^T A N &= \begin{bmatrix} 1 & 0 & 0 \\ v & 1 & 0 \\ w & 5 & 1 \end{bmatrix} \begin{bmatrix} 1 & -3 & -2 \\ -3 & 10 & 1 \\ -2 & 1 & 30 \end{bmatrix} \begin{bmatrix} 1 & v & w \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & -3 & -2 \\ v - 3 & -3v + 10 & -2v + 1 \\ w - 17 & -3w + 51 & -2w + 35 \end{bmatrix} \begin{bmatrix} 1 & v & w \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{bmatrix}
\end{aligned}$$

Para $v=3, w=17$, obtemos $N^TAN = \begin{bmatrix}1 & -3 & -2\\ 0 & 1 & -5\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 3 & 17\\ 0 & 1 & 5\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}$.

Então, $N^{-1} = \begin{bmatrix}1 & 3 & 17\\ 0 & 1 & 5\\ 0 & 0 & 1\end{bmatrix}^{-1} = \begin{bmatrix}1 & -3 & -2\\ 0 & 1 & -5\\ 0 & 0 & 1\end{bmatrix}$. Para $x = Ny$, temos $\begin{bmatrix}0\\ 0\\ 1\end{bmatrix} = \begin{bmatrix}1 & 3 & 17\\ 0 & 1 & 5\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}y_1\\ y_2\\ y_3\end{bmatrix}$.

Então, $\begin{bmatrix}y_1\\ y_2\\ y_3\end{bmatrix} = \begin{bmatrix}1 & -3 & -2\\ 0 & 1 & -5\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\ 0\\ 1\end{bmatrix} = \begin{bmatrix}-2\\ -5\\ 1\end{bmatrix}$

Logo, $30 = (-2)^2 + (-5)^2 + 1^2 = 2^2 + 5^2 + 1^2 = 5^2 + 2^2 + 1^2$.

Corolário 192 *Todo o número natural pode ser escrito como soma de três números triangulares, não necessariamente diferentes de zero.*

Demonstração

Observemos, em primeiro lugar, que número triangular é um número da forma $\frac{n(n+1)}{2}$, com $n \in \mathbb{N}_0$, isto é, da forma $\frac{n(n-1)}{2}$, com $n \in \mathbb{N}$.

Seja $u \in \mathbb{N}$. Consideremos o número natural $m = 8u+3$ que é ímpar e não é congruente com 7, módulo 8.

Então, m é soma de três quadrados. Como m é ímpar, essas três parcelas têm de ser todas ímpares ou uma delas é ímpar e as outras duas são pares. Neste último caso teríamos que m era congruente com 1, módulo 4, o que é falso, porque m é congruente com 3, módulo 4.

Então, m é soma de três quadrados ímpares, pelo que existem números naturais a, b, c, tais que $m = (2a-1)^2 + (2b-1)^2 + (2c-1)^2$.

Logo,

$$\begin{aligned} m &= 4a^2 - 4a + 1 + 4b^2 - 4b + 1 + 4c^2 - 4c + 1 \\ &= 4a^2 - 4a + 4b^2 - 4b + 4c^2 - 4c + 3 \end{aligned}$$

Então,

$$\begin{aligned} u &= \frac{m-3}{8} = \frac{4a^2 - 4a + 4b^2 - 4b + 4c^2 - 4c}{8} \\ &= \frac{a^2 - a + b^2 - b + c^2 - c}{2} = \frac{a^2-a}{2} + \frac{b^2-b}{2} + \frac{c^2-c}{2} \\ &= \frac{a\,(a-1)}{2} + \frac{b\,(b-1)}{2} + \frac{c\,(c-1)}{2} \end{aligned}$$

Logo, u é uma soma de três números triangulares.

Está, assim terminada a demonstração, uma vez que u pode ser um número natural qualquer.

Exercício 193 *Decomponha* 1235 *numa soma de três números triangulares.*

Resolução

Seja $m = 8 \times 1235 + 3 = 9883$. Então, $m = 9801 + 81 + 1 = 99^2 + 9^2 + 1^2$.

Então, $\begin{cases} 2a-1 = 99 \\ 2b-1 = 9 \\ 2c-1 = 1 \end{cases}$, donde vem $\begin{cases} a = 50 \\ b = 5 \\ c = 1 \end{cases}$. Então,

$$1235 = \frac{50 \times 49}{2} + \frac{5 \times 4}{2} + \frac{1 \times 0}{2} = 1225 + 10 + 0$$

É claro que a única dificuldade consiste em obter a decomposição de m numa soma de três quadrados.

Capítulo 7

Somas de quadrados não nulos

Lema 194 *O número* 169 *pode decompor-se como soma de n quadrados não nulos, para todo o número natural tal que* $1 \leq n \leq 155$.

Demonstração

Apresentamos 155 decomposições de 169, uma para cada número natural n, tal que $1 \leq n \leq 155$, em anexo intitulado "Decomposição de 169 em somas de quadrados não nulos".

Proposição 195 *Todo o número natural maior ou igual a* 169 *pode ser escrito como soma de n quadrados não nulos, com* $5 \leq n \leq 155$.

Demonstração

É claro que a afirmação anterior é válida para 169. Seja m um número natural maior que 169.

Então, $m = 169 + (m - 169)$. Mas, qualquer número natural é soma de quatro quadrados, pelo que $m - 169$ é uma soma de quatro quadrados não necessariamente diferentes de zero. Temos, então, quatro casos possíveis: $m - 169$ é um quadrado, ou uma soma de dois, três ou quatro quadrados não nulos.

Se $m - 169$ é um quadrado, então $m = 169 + (m - 169)$ pode ser escrito como soma de n quadrados não nulos, com $5 \leq n \leq 155$, para o que basta escolher as decomposições convenientes de 169 em soma de quadrados não nulos $(4, 5, \ldots, 154$ quadrados).

Se $m - 169$ é uma soma de dois quadrados não nulos, então o número $m = 169 + (m - 169)$ também pode ser escrito como soma de n quadrados não nulos, com $5 \leq n \leq 155$, para o que basta escolher as decomposições convenientes de 169 em soma de quadrados não nulos $(3, 4, \ldots, 153$ quadrados).

Se $m - 169$ é uma soma de três quadrados não nulos, então $m = 169 + (m - 169)$ também pode ser escrito como soma de n quadrados não nulos, com $5 \leq n \leq 155$, para o que basta escolher as decomposições convenientes de 169 em soma de quadrados não nulos $(2, 3, \ldots, 152$ quadrados).

Finalmente, se $m - 169$ é uma soma de quatro quadrados não nulos, então o número $m = 169 + (m - 169)$ também pode ser escrito como soma de n quadrados não nulos, com $5 \leq n \leq 155$, para o que basta escolher as decomposições convenientes de 169 em soma de quadrados não nulos $(1, 2, \ldots, 151$ quadrados).

Está, assim, terminada a demonstração.

Proposição 196 *Os números naturais que não se podem decompor numa soma de* 5 *quadrados não nulos são* 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33.

Demonstração

A demonstração desta proposição consiste, simplesmente, em calcular $a^2 + b^2 + c^2 + d^2 + e^2$ para os diferentes valores inteiros de a, b, c, d, e tais que $1 \leq a, b, c, d, e < 13$. Isso pode ser feito em Computador, através dum programa elaborado para o efeito.

Como $5^{12} = 244\,140\,625$, não é conveniente usar o Excel. Mas, se repararmos que o maior número da lista dada é 33, o número de hipóteses a testar é muito inferior. Assim, teremos $1 \leq a, b, c, d, e \leq 5$. Ora, $5^5 = 3125$, o que mostra que podemos usar o Excel, embora dê algum trabalho. No entanto, sem usar computadores, podemos verificar que 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33 não podem decompor-se numa soma de cinco quadrados não nulos. Assim, é claro que 1, 2, 3, 4 não podem decompor-se numa soma de cinco quadrados não nulos.

Como $1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8$, então 6 e 7 não podem decompor-se dessa forma. E, assim por diante.

Em anexo intitulado "Decomposição dos números inferiores a 169 em somas de 5 quadrados não nulos", podem ser vistas as decomposições dos naturais menores que 169 e diferentes de 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33.

Proposição 197 *Os números naturais que não se podem decompor numa soma de 6 quadrados não nulos são* 1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 16, 19.

Demonstração

Já vimos que todo o número inteiro maior ou igual a 169 é soma de 6 quadrados não nulos. Além disso, se um número inteiro n é soma de 5 quadrados não nulos, então o número $n + 1$ é soma de 6 quadrados não nulos.

Logo, os números inteiros que não podem decompor-se numa soma de 6 quadrados não nulos são 1, 2, 3, 4, 5 e, eventualmente, os números 7, 8, 10, 11, 13, 16, 19, 34. Mas, $34 = 2^2 + 2^2 + 2^2 + 2^2 + 3^2 + 3^2$.

E, se algum dos restantes fosse soma de 6 quadrados não nulos, um desses quadrados teria de ser 1, porque $6 \times 2^2 = 24$, e então algum dos números 6, 7, 9, 10, 12, 15, 18 seria uma soma de 5 quadrados não nulos, o que é falso.

Logo, 1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 16, 19 são os únicos números que não são decomponíveis numa soma de 6 quadrados não nulos.

Proposição 198 *Seja $k \in \mathbb{N}$, tal que $k \geq 6$. Seja $B = \{1, 2, 4, 5, 7, 10, 13\}$. Então, os números naturais que não se podem decompor numa soma de k quadrados não nulos são $1, 2, \ldots, k-1$ e $k+b$, com $b \in B$.*

Demonstração

Pela proposição anterior, a afirmação é válida para $k = 6$.

Suponhamos que a afirmação é válida para k, com $k \geq 6$.

É claro que $1, 2, \ldots, k-1$ não se podem decompor numa soma de k quadrados não nulos. Além disso, se um dado número natural n se decompõe numa soma de k quadrados não nulos, então $n + 1$ decompõe-se numa soma de $k + 1$ quadrados não nulos. Logo, apenas falta ver o que se passa com os números naturais da forma $k + 1 + b$, com $b \in B$.

Suponhamos que existia $b \in B$, tal que $k + 1 + b$ era uma soma de $k + 1$ quadrados não nulos. Então, um dos quadrados tem de ser 1, pois se todos os quadrados fossem maiores que 1, teríamos $k + 1 + b \geq (k + 1) \times 2^2$. Ora:

$$\begin{aligned} k + 1 + b \geq (k + 1) \times 2^2 &\implies k + 1 + b \geq 4k + 4 \implies b \geq 3k + 3 \\ &\implies 13 \geq 3k + 3 \implies 10 \geq 3k \implies k \leq 3 \end{aligned}$$

Mas $k \leq 3$ vai contra a hipótese $k \geq 6$.

Mas, se um dos quadrados é 1, então $k + b$ é uma soma de k quadrados não nulos, o que contradiz a hipótese de indução. Logo, a afirmação é válida para $k + 1$, pelo que a proposição está demonstrada (por indução em k).

Lema 199 *Os números naturais inferiores a* 169 *que não são múltiplos de* 8 *e que não se podem decompor numa soma de quatro quadrados não nulos são* 1, 2, 3, 5, 6, 9, 11, 14, 17, 29 *e* 41.

Os números naturais inferiores a 676 *e congruentes com* 1, *módulo* 4, *que não se decompõem numa soma de* 4 *quadrados não nulos são* 1, 5, 9, 17, 29 *e* 41, *o que não acrescenta nenhum número à lista anterior.*

Demonstração

Este lema, que irá ser utilizado em demonstrações posteriores, pode ser comprovado através de cálculos laboriosos ou através dum programa de computador, que foi o processo utilizado.

A decomposição dos números até 676, numa soma de quatro quadrados não nulos, está apresentada em anexo.

Lema 200 *Todo o número natural da forma* $n = 4^a m$, *com* $a \in \mathbb{N}$ *e* $m \in \{1, 3, 5, 9, 11, 17, 29, 41\}$, *pode decompor-se numa soma de quatro quadrados não nulos.*

Demonstração

1. Se $n = 4^a$, com $a \in \mathbb{N}$, então

$$n = 4 \times 4^{a-1} = 4 \times \left(2^{a-1}\right)^2 = \left(2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 + \left(2^{a-1}\right)^2$$

   Então, n é uma soma de quatro quadrados não nulos.

2. Se $n = 4^a \times 3$, com $a \in \mathbb{N}$, então

$$\begin{aligned} n &= 4 \times 4^{a-1} \times 3 = 12 \times \left(2^{a-1}\right)^2 = (9 + 1 + 1 + 1) \times \left(2^{a-1}\right)^2 \\ &= \left(3 \times 2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 \end{aligned}$$

   Logo, n é uma soma de quatro quadrados não nulos.

3. Se $n = 4^a \times 5$, com $a \in \mathbb{N}$, então

$$n = 20 \times 4^{a-1} = (9 + 9 + 1 + 1) \times 4^{a-1} = \left(3 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 + \left(2^{a-1}\right)^2$$

   Logo, n é uma soma de quatro quadrados não nulos.

4. Consideremos as igualdades seguintes:

$$\begin{cases} 4 \times 9 = 3^2 + 3^2 + 3^2 + 3^2 \\ 4 \times 11 = 5^2 + 3^2 + 3^2 + 1^2 \\ 4 \times 17 = 5^2 + 5^2 + 3^2 + 3^2 \\ 4 \times 29 = 7^2 + 7^2 + 3^2 + 3^2 \\ 4 \times 41 = 9^2 + 9^2 + 1^2 + 1^2 \end{cases}$$

   Então,

$$\begin{cases} n = 4^a \times 9 = 36 \times 4^{a-1} = \left(3 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 \\ n = 4^a \times 11 = 44 \times 4^{a-1} = \left(5 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 \\ n = 4^a \times 17 = 68 \times 4^{a-1} = \left(5 \times 2^{a-1}\right)^2 + \left(5 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 \\ n = 4^a \times 29 = 116 \times 4^{a-1} = \left(7 \times 2^{a-1}\right)^2 + \left(7 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 + \left(3 \times 2^{a-1}\right)^2 \\ n = 4^a \times 41 = 164 \times 4^{a-1} = \left(9 \times 2^{a-1}\right)^2 + \left(9 \times 2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 + \left(2^{a-1}\right)^2 \end{cases}$$

Lema 201 *Nenhum número da forma 2×4^a, com $a \in \mathbb{N}_0$, é soma de quatro quadrados não nulos.*

Demonstração
Suponhamos que $n = 2 \times 4^a$, com $a \in \mathbb{N}_0$, é soma de quatro quadrados não nulos.
Então, $n = 2 \times 4^a = x^2 + y^2 + z^2 + w^2$, para certos naturais x, y, z, w e, sem perda de generalidade, temos três hipóteses a considerar:

1. x, y, z, w são ímpares
2. x, y são pares e z, w são ímpares
3. x, y, z, w são pares

Vejamos que todas as hipóteses conduzem a uma contradição:

1. Se x, y, z, w fossem números ímpares, então $x^2 + y^2 + z^2 + w^2$ era congruente com 4, módulo 8, o que é falso, pois $n = 2 \times 4^a$ é múltiplo de 8, qualquer que seja $a \in \mathbb{N}$. Logo, é absurdo supor que x, y, z, w são todos ímpares.
2. Se x, y fossem pares e z, w ímpares, então $x^2 + y^2 + z^2 + w^2$ era congruente com 2, módulo 4, o que é falso, pois $n = 2 \times 4^a$ é múltiplo de 4, qualquer que seja $a \in \mathbb{N}$. Logo, é absurdo supor que x, y são pares e z, w são ímpares.
3. Se x, y, z, w fossem pares, então $\frac{n}{4} = \frac{x^2}{4} + \frac{y^2}{4} + \frac{z^2}{4} + \frac{w^2}{4}$ também era uma soma de quatro quadrados não nulos. Além disso, $\frac{n}{4} = 2 \times 4^{a-1}$, com $a - 1 \in \mathbb{N}$. E os números naturais $\frac{x}{2}$, $\frac{y}{2}$, $\frac{z}{2}$, $\frac{w}{2}$ teriam de ser todos pares para que não obtivéssemos uma contradição.

   Continuando o processo, chegaríamos (num número finito de passos) à igualdade

$$2 = \frac{n}{4^a} = \frac{x^2}{4^a} + \frac{y^2}{4^a} + \frac{z^2}{4^a} + \frac{w^2}{4^a}$$

   Então, 2 seria uma soma de quatro quadrados não nulos, o que é falso. Logo, é absurdo supor que x, y, z, w são pares. Então, é absurdo supor que $n = 2 \times 4^a$, com $a \in \mathbb{N}$, é soma de quatro quadrados não nulos, pelo que está terminada a demonstração.

Note-se que a demonstração pode ser feita por indução em a.

Lema 202 *Nenhum número da forma $n = 6 \times 4^a$, com $a \in \mathbb{N}_0$, é soma de quatro quadrados não nulos.*

Demonstração
Vamos fazer a demonstração por indução em a.
Para $a = 0$, temos $n = 6$ que não se pode escrever como soma de quatro quadrados não nulos.
Suponhamos que 6×4^a não pode decompor-se numa soma de quatro quadrados não nulos.
Queremos provar que $6 \times 4^{a+1}$ não pode decompor-se numa soma de quatro quadrados não nulos.
Suponhamos que $6 \times 4^{a+1} = x^2 + y^2 + z^2 + w^2$, para certos naturais x, y, z, w.
Então, temos três hipóteses a considerar:

1. Se x, y, z, w forem todos ímpares, então $6 \times 4^{a+1} = x^2 + y^2 + z^2 + w^2$ era congruente com 4, módulo 8, o que é falso, pois $n = 6 \times 4^{a+1}$ é múltiplo de 8, qualquer que seja $a \in \mathbb{N}_0$. Logo, é absurdo supor que x, y, z, w são todos ímpares.

2. Se x, y forem pares e z, w forem ímpares, então $x^2+y^2+z^2+w^2$ era congruente com 2, módulo 4, o que é falso, pois $n=6\times 4^{a+1}$ é múltiplo de 4, qualquer que seja $a\in\mathbb{N}_0$.

3. Se x, y, z, w fossem pares, então $\frac{n}{4}=\frac{x^2}{4}+\frac{y^2}{4}+\frac{z^2}{4}+\frac{w^2}{4}$ também era uma soma de quatro quadrados não nulos. Então, $\frac{6\times 4^{a+1}}{4}=6\times 4^a$ podia decompor-se numa soma de quatro quadrados não nulos, o que vai contra a hip´tese de indução.

Então, é absurdo supor que $6\times 4^{a+1}$ pode decompor-se numa soma de quatro quadrados não nulos. Está, assim, terminada a demonstração do lema.

Lema 203 *Nenhum número da forma $n=14\times 4^a$, com $a\in\mathbb{N}_0$, é soma de quatro quadrados não nulos.*

Demonstração
A demonstração é análoga a uma das anteriores.

Proposição 204 *Os únicos números naturais que não se podem decompor numa soma de quatro quadrados não nulos são $1,2,3,5,6,9,11,14,17,29,41$ e os infinitos números da forma $n_1\times 4^a$, com $a\in\mathbb{N}$ e $n_1=2$ ou 6 ou 14, ou seja, da forma $n\times 2^{2a+1}$, com $a\in\mathbb{N}$ e $n=1$ ou 3 ou 7.*

Demonstração
Na presente demonstração, feita por casos, chamaremos números excepcionais àqueles que não podem ser decompostos numa soma de quatro quadrados não nulos. Seja n um número natural.

1º caso: Suponhamos que $n>169$ e que $n\equiv 2\vee n\equiv 3\vee n\equiv 4\vee n\equiv 6\vee n\equiv 7\,(\mathrm{mod}\,8)$.

Então, $n-1\geq 169$ e $n-169\equiv 1\vee n\equiv 2\vee n\equiv 3\vee n\equiv 5\vee n\equiv 6\,(\mathrm{mod}\,8)$, pelo que $n-169$ não é da forma $4^a\,(8m+7)$. Logo, $n-169$ pode decompor-se numa soma de três quadrados, pelo que há três hipóteses: $n-169$ é um quadrado não nulo ou $n-169$ é uma soma de dois quadrados não nulos ou $n-169$ é uma soma de três quadrados não nulos.

Em qualquer dos casos, utilizando a decomposição conveniente de 169 numa soma de quadrados não nulos, temos que $n=169+n-169$ pode decompor-se numa soma de quatro quadrados não nulos.

2º caso: Suponhamos que $n>676$ e que $n\equiv 1\vee n\equiv 5\,(\mathrm{mod}\,8)$. Consideremos $n=676+(n-676)$.

Como $676\equiv 4\,(\mathrm{mod}\,8)$ e $n\equiv 1\vee n\equiv 5\,(\mathrm{mod}\,8)$, então, $n-676\equiv 1\,(\mathrm{mod}\,8)$ ou $n-676\equiv 1\,(\mathrm{mod}\,8)$.

Logo, $n-676$ não é da forma $4^a\,(8m+7)$. Logo, $n-676$ pode decompor-se numa soma de três quadrados, pelo que há três hipóteses: $n-676$ é um quadrado não nulo ou $n-169$ é uma soma de dois quadrados não nulos ou $n-169$ é uma soma de três quadrados não nulos.

Mas, $676=26^2=10^2+26^2=6^2+8^2+24^2$. Então, $n=676+(n-676)$ pode decompor-se numa soma de quatro quadrados não nulos.

3º caso: Suponhamos que $n\equiv 0\,(\mathrm{mod}\,8)$. Então, $n=2^{a+2}$, com $a,m\in\mathbb{N}$ e m ímpar. Se m é ímpar e m é uma soma de quatro quadrados não nulos, então $x=4^bm$ é uma soma de quatro quadrados não nulos. Logo, os únicos números da forma 4^bm, com m ímpar, que podem ser excepcionais são os números da forma 4^bm, com m um dos números 1, 3, 5, 9, 11, 17, 29, 41.

Mas, por um dos lemas demonstrados, todos esses números podem decompor-se numa soma de quatro quadrados não nulos.

Se $x=2\times 4^bm$ (com m ímpar) e $2m$ não é excepcional, então x também não é excepcional. Se $2m$ é excepcional, então $2m=2\vee 2m=6\vee 2m=14$, pelo que $m=1\vee m=3\vee m=7$.

Logo, 2×4^b, $x=6\times 4^b$, $x=14\times 4^b$ são possíveis números excepcionais. Mas, todos eles são excepcionais, como verificado anteriormente.

Está, assim, terminada a demonstração.

Proposição 205 *Os únicos números naturais que se podem decompor numa soma de dois quadrados não nulos são os números da forma* $n = 2^a p_1 \cdots p_r q_1^2 \cdots q_s^2$, *onde* $a \in \mathbb{N}_0$, $p_1, \ldots, p_r$ *são primos congruentes com* 1, *módulo* 4, *não necessariamente distintos e* $q_1, \ldots, q_s$ *são primos congruentes com* 3, *módulo* 4, *também não necessariamente distintos, a menos que* n *seja da forma* $n = 2^{2a} q_1^2 \cdots q_s^2$, *com* $a \in \mathbb{N}_0$, *caso em que não é soma de dois quadrados não nulos. Neste enunciado estamos a admitir que um ou ambos os produtos* $p_1 \cdots p_r$ *e* $q_1^2 \cdots q_s^2$ *podem ser vazios, caso em que o produto se considera igual a* 1.

Demonstração

1. Suponhamos que $n = 2^{2b}$, com $b \in \mathbb{N}_0$.

   Se $b = 0$, então $n = 1$ que não é soma de dois quadrados não nulos.

   Suponhamos, como hipótese de indução, que 2^{2b} não é soma de dois quadrados não nulos.

   Suponhamos, com vista a um absurdo, que 2^{2b+2} era uma soma de dois quadrados não nulos. Então esses quadrados tinham de ser pares, porque 2^{2b+2} é um múltiplo de 4. Mas, nesse caso, 2^{2b} também seria uma soma de dois quadrados não nulos, o que contradiz a hipótese de indução. Logo, 2^{2b+2} não é soma de dois quadrados não nulos.

   Logo, 2^{2b} não pode decompor-se numa soma de dois quadrados não nulos.

2. Suponhamos que $n = 2^{2b} q_1^2 \cdots q_s^2$, com $b \in \mathbb{N}_0$. Suponhamos, com vista a um absurdo, que n é uma soma de dois quadrados não nulos, digamos $n = x^2 + y^2$. Então, q_1 divide x^2 e q_1 divide y^2, pelo que q_1 divide x e q_1 divide y. Analogamente se mostra que q_j divide x e q_j divide y, para $j = 1, \ldots, s$. Logo, $q_1 \cdots q_s$ divide x e $q_1 \cdots q_s$ divide y.

   Então, $2^{2b} = \dfrac{n}{q_1^2 \cdots q_s^2} = \dfrac{x^2}{q_1^2 \cdots q_s^2} + \dfrac{y^2}{q_1^2 \cdots q_s^2} = \left(\dfrac{x}{q_1 \cdots q_s}\right)^2 + \left(\dfrac{y}{q_1 \cdots q_s}\right)^2$.

   Então, 2^{2b} seria uma soma de dois quadrados não nulos, o que é falso. Então, é absurdo supor que $n = 2^{2b} q_1^2 \cdots q_s^2$ é soma de dois quadrados não nulos.

3. Suponhamos que $n = 2^a p_1 \cdots p_r q_1^2 \cdots q_s^2$, com $r \in \mathbb{N}$.

   Como são primos congruentes com 1, módulo 4, e qualquer produto de primos nessas condições é uma soma de dois quadrados não nulos, temos que $p_1 \cdots p_r$ é uma soma de dois quadrados não nulos. Então, $p_1 \cdots p_r = x^2 + y^2$, para certos números naturais x e y.

   Se a é par, então $2^a = 2^{2c} = (2^c)^2$, pelo que temos:

   $$\begin{aligned} n &= 2^a p_1 \cdots p_r q_1^2 \cdots q_s^2 = (2^c)^2 \left(x^2 + y^2\right) q_1^2 \cdots q_s^2 \\ &= (2^c)^2 q_1^2 \cdots q_s^2 x^2 + (2^c)^2 q_1^2 \cdots q_s^2 y^2 \\ &= (2^c q_1 \cdots q_s x)^2 + (2^c q_1 \cdots q_s y)^2 \end{aligned}$$

   Logo, n é uma soma de dois quadrados não nulos.

   Se a é ímpar, então $n = 2^a = 2^{2c+1} = 2 \times 2^{2c}$. Ora,

   $$\begin{aligned} 2p_1 \cdots p_r &= 2\left(x^2 + y^2\right) = x^2 + 2xy + y^2 + x^2 - 2xy + y^2 \\ &= (x+y)^2 + (x-y)^2 \end{aligned}$$

   Observemos que, como $p_1 \cdots p_r$ é ímpar, se $p_1 \cdots p_r = x^2 + y^2$, podemos supor, sem perda de generalidade, que x é par e y é ímpar, pelo que $x + y$ e $x - y$ são ímpares e, por isso, diferentes de zero.

Então:

$$\begin{aligned} n &= 2^{2c+1}p_1\cdots p_r q_1^2\cdots q_s^2 = 2\times 2^{2c}p_1\cdots p_r q_1^2\cdots q_s^2 = 2^{2c}\times p_1\cdots p_r q_1^2\cdots q_s^2 \\ &= (2^c)^2\left((x+y)^2+(x-y)^2\right) = (2^c(x+y))^2+(2^c(x-y))^2 \end{aligned}$$

Então, n é uma soma de dois quadrados não nulos.

Finalmente, observe-se que, se algum primo congruente com 3, módulo 4, ocorrer em n um número ímpar de vezes, então n não é soma de dois quadrados não nulos.

Está, assim, terminada a demonstração.

Observação

O caso da decomposição de um número natural em três quadrados não nulos é muito mais difícil.

Repare-se que estão bem definidos os números que se decompõem numa soma de três quadrados; só que alguns desses quadrados podem ser zero. Por exemplo, 5 decompõe-se numa soma de três quadrados ($5 = 2^2+1^2+0^2$), mas 5 não pode decompor-se numa soma de três quadrados não nulos. Acresce que o produto de duas somas de três quadrados não nulos não tem que ser uma soma de três quadrados não nulos. Assim, $3 = 1^2+1^2+1^2$ e $29 = 4^2+3^2+2^2$, mas o seu produto (87) não pode decompor-se numa soma de menos de quatro quadrados não nulos.

Saber quais os números naturais que podem decompor-se numa soma de três quadrados é uma questão em aberto (ou, pelo menos, era até há pouco tempo). De qualquer modo, vejamos alguns resultados sobre somas de três quadrados não nulos:

Proposição 206 *Seja q um número primo congruente com 3, módulo 8. Então, para qualquer número natural n, q^n é uma soma de três quadrados não nulos.*

Demonstração

Seja q um número primo congruente com 3, módulo 8. Já vimos que existem números naturais x e y, tais que $q = x^2+2y^2$.

Então, $q = x^2+y^2+y^2$, pelo que q é uma soma de três quadrados não nulos.

Mas, $q^2 = \left(x^2+2y^2\right)^2 = x^4+4x^2y^2+4y^4 = \left(x^2\right)^2+(2xy)^2+\left(2y^2\right)^2$. Então, q^2 pode decompor-se numa soma de três quadrados não nulos.

E, $q^{2n+1} = (q^n)^2\times q = (q^n)^2\left(x^2+y^2+y^2\right) = (q^nx)^2+(q^ny)^2+(q^ny)^2$, pelo que q^{2n+1} pode decompor-se numa soma de três quadrados não nulos.

E, por fim, $q^{2n+2} = (q^n)^2\times q^2 = (q^n)^2\left(\left(x^2\right)^2+(2xy)^2+\left(2y^2\right)^2\right) = \left(q^nx^2\right)^2+(2q^nxy)^2+\left(2q^ny^2\right)^2$, pelo que q^{2n+2} é uma soma de três quadrados não nulos.

Assim, para $q = 11$, temos:

$11 = 3^2+1^2+1^2$

$11^2 = 9^2+6^2+2^2$

$11^3 = 11^2\times\left(3^2+1^2+1^2\right) = 33^2+11^2+11^2$

$11^4 = 11^2\times\left(9^2+6^2+2^2\right) = 99^2+66^2+22^2$

Proposição 207 *Sejam m um número natural e q um número primo congruente com 3, módulo 8. Então, m^2q é uma soma de três quadrados não nulos.*

Demonstração

Trivial.

Proposição 208 *Seja q um número primo congruente com 3, módulo 8. Então, para qualquer número natural n, 2^nq é uma soma de três quadrados não nulos.*

Demonstração

Se q é um número primo congruente com 3, módulo 8, então existem números naturais x e y, tais que $q = x^2 + 2y^2$.

Então, $2^{2m}q = (2^m)^2 \left(x^2 + 2y^2\right) = (2^m x)^2 + (2^m y)^2 + (2^m y)^2$.

E, $2^{2m+1}q = 2^{2m} \times 2 \left(x^2 + 2y^2\right) = (2^m)^2 \left(2x^2 + 4y^2\right) = (2^m x)^2 + (2^m x)^2 + \left(2^{m+1} y\right)^2$.

Então, para qualquer número natural n, $2^n q$ pode decompor-se numa soma de três quadrados não nulos, uma vez que a afirmação vale para os números pares e para os números ímpares.

Observação

Exemplos triviais de somas de três quadrados não nulos:

$3n^2$, $2n^2 + 1$, $2n^2 + 4$, $2n^2 + 9$, $2n^2 + 16$, $n^2 + 2$, $n^2 + 5$, $n^2 + 8$, $n^2 + 10$, $n^2 + 13$, $n^2 + 17$, $n^2 + 18$, $n^2 + 20$, $n^2 + 25$, $n^2 + 26$, $n^2 + 29$, $n^2 + 32$, $n^2 + 34$, etc...

Há outros exemplos de somas de três quadrados não nulos: Um número ímpar n, que não seja da forma $n = 8m + 7$, com $m \in \mathbb{N}$, e que admita um factor primo q, tal que q ocorra em n um número ímpar de vezes, é uma soma de três quadrados não nulos.

Por exemplo, $8085 = 3 \times 5 \times 7^2 \times 11 \equiv 15 \times (-1)^2 \times 3 \equiv -3 \equiv 5 \pmod 8$ tem de ser uma soma de três quadrados não nulos.

Mas, como obter uma decomposição?

Neste caso, felizmente, uma primeira tentativa basta:

$$8085 - 89^2 = 164 = 4 \times 41 = 4 \times 25 + 4 \times 16 = 10^2 + 8^2$$

Logo, $89^2 + 10^2 + 8^2 = 8085$. Mas,

$$8085 - 86^2 = 689 = 13 \times 53 = (9 + 4) \times (49 + 4)$$

Se não nos recordarmos da fórmula (fácil de obter) que dá $\left(a^2 + b^2\right)\left(c^2 + d^2\right)$, podemos usar matrizes e determinantes:

$$\begin{bmatrix} 3 & -2 \\ 2 & 3 \end{bmatrix} \times \begin{bmatrix} 7 & -2 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 17 & -20 \\ 20 & 17 \end{bmatrix}$$

Logo,

$$\left(3^2 + 2^2\right) \times \left(7^2 + 2^2\right) = \begin{vmatrix} 3 & -2 \\ 2 & 3 \end{vmatrix} \times \begin{vmatrix} 7 & -2 \\ 2 & 7 \end{vmatrix} = \begin{vmatrix} 17 & -20 \\ 20 & 17 \end{vmatrix} = 17^2 + 20^2$$

Então, $8085 = 17^2 + 20^2 + 86^2$, tendo-se obtido outra decomposição.

Terminamos com a seguinte proposição que generaliza o que acabámos de ver:

Proposição 209 *Sejam $a, b, c, d \in \mathbb{Z}$. Então, existem $x, y \in \mathbb{Z}$, tais que $\left(a^2 + b^2\right) \times \left(c^2 + d^2\right) = x^2 + y^2$.*

Demonstração

$$\begin{aligned} \left(a^2 + b^2\right) \times \left(c^2 + d^2\right) &= \begin{vmatrix} a & -b \\ b & a \end{vmatrix} \times \begin{vmatrix} c & -d \\ d & c \end{vmatrix} = \begin{vmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{vmatrix} \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

Apêndice A

Decomposição de 169 em somas de quadrados não nulos

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**N^o de qnn**
0	0	0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	1	0	0	0	0	0	0	1	0	2
0	0	1	1	0	0	0	0	0	0	0	1	0	3
0	0	0	3	0	0	0	0	0	0	1	0	0	4
1	1	0	0	0	1	0	2	0	0	0	0	0	5
0	4	1	0	0	0	0	0	0	0	0	1	0	6
0	4	0	2	0	0	0	0	0	0	1	0	0	7
1	6	0	0	0	0	0	0	0	0	0	1	0	8
4	3	1	0	0	0	0	0	0	0	0	1	0	9
4	3	0	2	0	0	0	0	0	0	1	0	0	10
5	5	0	0	0	0	0	0	0	0	0	1	0	11
8	2	1	0	0	0	0	0	0	0	0	1	0	12
1	10	0	0	0	0	0	2	0	0	0	0	0	13
9	4	0	0	0	0	0	0	0	0	0	1	0	14
12	1	1	0	0	0	0	0	0	0	0	1	0	15
5	9	0	0	0	0	0	2	0	0	0	0	0	16
13	3	0	0	0	0	0	0	0	0	0	0	1	17
16	0	1	0	0	0	0	0	0	0	0	1	0	18
2	10	3	0	4	0	0	0	0	0	0	0	0	19
2	10	4	1	3	0	0	0	0	0	0	0	0	20
2	10	5	2	2	0	0	0	0	0	0	0	0	21
6	9	3	0	4	0	0	0	0	0	0	0	0	22
6	9	4	1	3	0	0	0	0	0	0	0	0	23
6	9	5	2	2	0	0	0	0	0	0	0	0	24
10	8	3	0	4	0	0	0	0	0	0	0	0	25
10	8	4	1	3	0	0	0	0	0	0	0	0	26
10	8	5	2	2	0	0	0	0	0	0	0	0	27
1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**N^o de qnn**

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**N^o de qnn**
14	7	3	0	4	0	0	0	0	0	0	0	0	28
14	7	4	1	3	0	0	0	0	0	0	0	0	29
14	7	5	2	2	0	0	0	0	0	0	0	0	30
18	6	3	0	4	0	0	0	0	0	0	0	0	31
18	6	4	1	3	0	0	0	0	0	0	0	0	32
18	6	5	2	2	0	0	0	0	0	0	0	0	33
22	5	3	0	4	0	0	0	0	0	0	0	0	34
22	5	4	1	3	0	0	0	0	0	0	0	0	35
22	5	5	2	2	0	0	0	0	0	0	0	0	36
26	4	3	0	4	0	0	0	0	0	0	0	0	37
26	4	4	1	3	0	0	0	0	0	0	0	0	38
26	4	5	2	2	0	0	0	0	0	0	0	0	39
30	3	3	0	4	0	0	0	0	0	0	0	0	40
0	40	1	0	0	0	0	0	0	0	0	0	0	41
3	37	2	0	0	0	0	0	0	0	0	0	0	42
1	42	0	0	0	0	0	0	0	0	0	0	0	43
4	39	1	0	0	0	0	0	0	0	0	0	0	44
7	36	2	0	0	0	0	0	0	0	0	0	0	45
5	41	0	0	0	0	0	0	0	0	0	0	0	46
8	38	1	0	0	0	0	0	0	0	0	0	0	47
11	35	2	0	0	0	0	0	0	0	0	0	0	48
9	40	0	0	0	0	0	0	0	0	0	0	0	49
12	37	1	0	0	0	0	0	0	0	0	0	0	50

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**N^o de qnn**
15	34	2	0	0	0	0	0	0	0	0	0	0	51
13	39	0	0	0	0	0	0	0	0	0	0	0	52
16	36	1	0	0	0	0	0	0	0	0	0	0	53
19	33	2	0	0	0	0	0	0	0	0	0	0	54
17	38	0	0	0	0	0	0	0	0	0	0	0	55
20	35	1	0	0	0	0	0	0	0	0	0	0	56
23	32	2	0	0	0	0	0	0	0	0	0	0	57
21	37	0	0	0	0	0	0	0	0	0	0	0	58
24	34	1	0	0	0	0	0	0	0	0	0	0	59
27	31	2	0	0	0	0	0	0	0	0	0	0	60
25	36	0	0	0	0	0	0	0	0	0	0	0	61
28	33	1	0	0	0	0	0	0	0	0	0	0	62
31	30	2	0	0	0	0	0	0	0	0	0	0	63
29	35	0	0	0	0	0	0	0	0	0	0	0	64
32	32	1	0	0	0	0	0	0	0	0	0	0	65
35	29	2	0	0	0	0	0	0	0	0	0	0	66
33	34	0	0	0	0	0	0	0	0	0	0	0	67
36	31	1	0	0	0	0	0	0	0	0	0	0	68
39	28	2	0	0	0	0	0	0	0	0	0	0	69
37	33	0	0	0	0	0	0	0	0	0	0	0	70
40	30	1	0	0	0	0	0	0	0	0	0	0	71
43	27	2	0	0	0	0	0	0	0	0	0	0	72

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**N^o de qnn**
41	32	0	0	0	0	0	0	0	0	0	0	0	73
44	29	1	0	0	0	0	0	0	0	0	0	0	74
47	26	2	0	0	0	0	0	0	0	0	0	0	75
45	31	0	0	0	0	0	0	0	0	0	0	0	76
48	28	1	0	0	0	0	0	0	0	0	0	0	77
51	25	2	0	0	0	0	0	0	0	0	0	0	78
49	30	0	0	0	0	0	0	0	0	0	0	0	79
52	27	1	0	0	0	0	0	0	0	0	0	0	80
55	24	2	0	0	0	0	0	0	0	0	0	0	81
53	29	0	0	0	0	0	0	0	0	0	0	0	82
56	26	1	0	0	0	0	0	0	0	0	0	0	83
59	23	2	0	0	0	0	0	0	0	0	0	0	84
57	28	0	0	0	0	0	0	0	0	0	0	0	85
60	25	1	0	0	0	0	0	0	0	0	0	0	86
63	22	2	0	0	0	0	0	0	0	0	0	0	87
61	27	0	0	0	0	0	0	0	0	0	0	0	88
64	24	1	0	0	0	0	0	0	0	0	0	0	89
67	21	2	0	0	0	0	0	0	0	0	0	0	90
65	26	0	0	0	0	0	0	0	0	0	0	0	91
68	23	1	0	0	0	0	0	0	0	0	0	0	92
71	20	2	0	0	0	0	0	0	0	0	0	0	93
69	25	0	0	0	0	0	0	0	0	0	0	0	94
72	22	1	0	0	0	0	0	0	0	0	0	0	95
75	19	2	0	0	0	0	0	0	0	0	0	0	96
73	24	0	0	0	0	0	0	0	0	0	0	0	97
76	21	1	0	0	0	0	0	0	0	0	0	0	98
79	18	2	0	0	0	0	0	0	0	0	0	0	99
77	23	0	0	0	0	0	0	0	0	0	0	0	100
80	20	1	0	0	0	0	0	0	0	0	0	0	101
83	17	2	0	0	0	0	0	0	0	0	0	0	102
81	22	0	0	0	0	0	0	0	0	0	0	0	103
84	19	1	0	0	0	0	0	0	0	0	0	0	104
87	16	2	0	0	0	0	0	0	0	0	0	0	105
85	21	0	0	0	0	0	0	0	0	0	0	0	106
88	18	1	0	0	0	0	0	0	0	0	0	0	107
91	15	2	0	0	0	0	0	0	0	0	0	0	108
89	20	0	0	0	0	0	0	0	0	0	0	0	109
92	17	1	0	0	0	0	0	0	0	0	0	0	110
95	14	2	0	0	0	0	0	0	0	0	0	0	111
93	19	0	0	0	0	0	0	0	0	0	0	0	112
96	16	1	0	0	0	0	0	0	0	0	0	0	113
99	13	2	0	0	0	0	0	0	0	0	0	0	114
97	18	0	0	0	0	0	0	0	0	0	0	0	115
100	15	1	0	0	0	0	0	0	0	0	0	0	116
103	12	2	0	0	0	0	0	0	0	0	0	0	117

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**N^o de qnn**
101	17	0	0	0	0	0	0	0	0	0	0	0	118
104	14	1	0	0	0	0	0	0	0	0	0	0	119
107	11	2	0	0	0	0	0	0	0	0	0	0	120
105	16	0	0	0	0	0	0	0	0	0	0	0	121
108	13	1	0	0	0	0	0	0	0	0	0	0	122
111	10	2	0	0	0	0	0	0	0	0	0	0	123
109	15	0	0	0	0	0	0	0	0	0	0	0	124
112	12	1	0	0	0	0	0	0	0	0	0	0	125
115	9	2	0	0	0	0	0	0	0	0	0	0	126
113	14	0	0	0	0	0	0	0	0	0	0	0	127
116	11	1	0	0	0	0	0	0	0	0	0	0	128
119	8	2	0	0	0	0	0	0	0	0	0	0	129
117	13	0	0	0	0	0	0	0	0	0	0	0	130
120	10	1	0	0	0	0	0	0	0	0	0	0	131
123	7	2	0	0	0	0	0	0	0	0	0	0	132
121	12	0	0	0	0	0	0	0	0	0	0	0	133
124	9	1	0	0	0	0	0	0	0	0	0	0	134
127	6	2	0	0	0	0	0	0	0	0	0	0	135
125	11	0	0	0	0	0	0	0	0	0	0	0	136
128	8	1	0	0	0	0	0	0	0	0	0	0	137
131	5	2	0	0	0	0	0	0	0	0	0	0	138
129	10	0	0	0	0	0	0	0	0	0	0	0	139
132	7	1	0	0	0	0	0	0	0	0	0	0	140

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**N^o de qnn**
135	4	2	0	0	0	0	0	0	0	0	0	0	141
133	9	0	0	0	0	0	0	0	0	0	0	0	142
136	6	1	0	0	0	0	0	0	0	0	0	0	143
139	3	2	0	0	0	0	0	0	0	0	0	0	144
137	8	0	0	0	0	0	0	0	0	0	0	0	145
140	5	1	0	0	0	0	0	0	0	0	0	0	146
143	2	2	0	0	0	0	0	0	0	0	0	0	147
141	7	0	0	0	0	0	0	0	0	0	0	0	148
144	4	1	0	0	0	0	0	0	0	0	0	0	149
147	1	2	0	0	0	0	0	0	0	0	0	0	150
145	6	0	0	0	0	0	0	0	0	0	0	0	151
148	3	1	0	0	0	0	0	0	0	0	0	0	152
151	0	2	0	0	0	0	0	0	0	0	0	0	153
149	5	0	0	0	0	0	0	0	0	0	0	0	154
152	2	1	0	0	0	0	0	0	0	0	0	0	155
153	4	0	0	0	0	0	0	0	0	0	0	0	157
156	1	1	0	0	0	0	0	0	0	0	0	0	158
157	3	0	0	0	0	0	0	0	0	0	0	0	160
160	0	1	0	0	0	0	0	0	0	0	0	0	161
161	2	0	0	0	0	0	0	0	0	0	0	0	163
165	1	0	0	0	0	0	0	0	0	0	0	0	166
169	0	0	0	0	0	0	0	0	0	0	0	0	169

Apêndice B

Decomposição dos números até 169 em somas de 5 quadrados não nulos

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**
5	0	0	0	0	0	0	0	0	0	0	0	0	5
4	1	0	0	0	0	0	0	0	0	0	0	0	8
3	2	0	0	0	0	0	0	0	0	0	0	0	11
4	0	1	0	0	0	0	0	0	0	0	0	0	13
2	3	0	0	0	0	0	0	0	0	0	0	0	14
3	1	1	0	0	0	0	0	0	0	0	0	0	16
1	4	0	0	0	0	0	0	0	0	0	0	0	17
2	2	1	0	0	0	0	0	0	0	0	0	0	19
0	5	0	0	0	0	0	0	0	0	0	0	0	20
3	0	2	0	0	0	0	0	0	0	0	0	0	21
1	3	1	0	0	0	0	0	0	0	0	0	0	22
3	1	0	1	0	0	0	0	0	0	0	0	0	23
2	1	2	0	0	0	0	0	0	0	0	0	0	24
2	2	0	1	0	0	0	0	0	0	0	0	0	26
1	2	2	0	0	0	0	0	0	0	0	0	0	27
3	0	1	1	0	0	0	0	0	0	0	0	0	28
1	3	0	1	0	0	0	0	0	0	0	0	0	29
0	3	2	0	0	0	0	0	0	0	0	0	0	30
2	1	1	1	0	0	0	0	0	0	0	0	0	31
0	4	0	1	0	0	0	0	0	0	0	0	0	32
1	2	1	1	0	0	0	0	0	0	0	0	0	34
2	2	0	0	1	0	0	0	0	0	0	0	0	35
2	0	2	1	0	0	0	0	0	0	0	0	0	36
0	3	1	1	0	0	0	0	0	0	0	0	0	37
1	3	0	0	1	0	0	0	0	0	0	0	0	38
1	1	2	1	0	0	0	0	0	0	0	0	0	39
4	0	0	0	0	1	0	0	0	0	0	0	0	40
0	4	0	0	1	0	0	0	0	0	0	0	0	41
0	2	2	1	0	0	0	0	0	0	0	0	0	42
2	0	1	2	0	0	0	0	0	0	0	0	0	43
1	0	3	1	0	0	0	0	0	0	0	0	0	44

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**
0	0	5	0	0	0	0	0	0	0	0	0	0	45
1	1	1	2	0	0	0	0	0	0	0	0	0	46
2	1	0	1	1	0	0	0	0	0	0	0	0	47
1	1	2	0	1	0	0	0	0	0	0	0	0	48
0	2	1	2	0	0	0	0	0	0	0	0	0	49
2	0	0	3	0	0	0	0	0	0	0	0	0	50
1	0	2	2	0	0	0	0	0	0	0	0	0	51
2	0	1	1	1	0	0	0	0	0	0	0	0	52
1	0	3	0	1	0	0	0	0	0	0	0	0	53
0	1	2	2	0	0	0	0	0	0	0	0	0	54
1	1	1	1	1	0	0	0	0	0	0	0	0	55
2	1	0	0	2	0	0	0	0	0	0	0	0	56
0	3	1	0	0	1	0	0	0	0	0	0	0	57
0	2	1	1	1	0	0	0	0	0	0	0	0	58
1	2	0	0	2	0	0	0	0	0	0	0	0	59
1	0	2	1	1	0	0	0	0	0	0	0	0	60
2	0	1	0	2	0	0	0	0	0	0	0	0	61
0	3	0	0	2	0	0	0	0	0	0	0	0	62
2	0	1	1	0	1	0	0	0	0	0	0	0	63
1	1	1	0	2	0	0	0	0	0	0	0	0	64
1	0	0	4	0	0	0	0	0	0	0	0	0	65
1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**
0	0	2	3	0	0	0	0	0	0	0	0	0	66
1	0	1	2	1	0	0	0	0	0	0	0	0	67
2	0	0	1	2	0	0	0	0	0	0	0	0	68
2	0	2	0	0	0	1	0	0	0	0	0	0	69
0	1	1	2	1	0	0	0	0	0	0	0	0	70
1	1	0	1	2	0	0	0	0	0	0	0	0	71
0	1	2	0	2	0	0	0	0	0	0	0	0	72
0	0	1	4	0	0	0	0	0	0	0	0	0	73
1	0	0	3	1	0	0	0	0	0	0	0	0	74
0	0	2	2	1	0	0	0	0	0	0	0	0	75
1	0	1	1	2	0	0	0	0	0	0	0	0	76
2	0	0	0	3	0	0	0	0	0	0	0	0	77
1	0	1	2	0	1	0	0	0	0	0	0	0	78
0	1	1	1	2	0	0	0	0	0	0	0	0	79
0	0	0	5	0	0	0	0	0	0	0	0	0	80
1	2	0	0	0	2	0	0	0	0	0	0	0	81
1	1	0	1	1	1	0	0	0	0	0	0	0	82
1	0	0	2	2	0	0	0	0	0	0	0	0	83
0	3	0	0	0	2	0	0	0	0	0	0	0	84
1	0	1	0	3	0	0	0	0	0	0	0	0	85
0	3	0	0	1	0	1	0	0	0	0	0	0	86
1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**
1	1	2	0	0	0	0	1	0	0	0	0	0	87
1	1	1	0	1	0	1	0	0	0	0	0	0	88
1	2	0	1	0	0	0	1	0	0	0	0	0	89
2	0	0	1	0	2	0	0	0	0	0	0	0	90
1	0	1	2	0	0	1	0	0	0	0	0	0	91
1	0	0	1	3	0	0	0	0	0	0	0	0	92
1	0	2	0	1	0	1	0	0	0	0	0	0	93
1	2	0	0	0	1	1	0	0	0	0	0	0	94
2	1	0	0	1	0	0	1	0	0	0	0	0	95
2	1	1	0	0	0	0	0	1	0	0	0	0	96
0	3	0	0	0	1	1	0	0	0	0	0	0	97
1	0	1	1	0	2	0	0	0	0	0	0	0	98
1	1	1	0	0	1	1	0	0	0	0	0	0	99
2	0	1	0	1	0	0	1	0	0	0	0	0	100
2	0	0	0	2	0	1	0	0	0	0	0	0	101
1	1	0	0	1	2	0	0	0	0	0	0	0	102
2	0	0	1	0	1	1	0	0	0	0	0	0	103
1	1	2	0	0	0	0	0	1	0	0	0	0	104
1	0	0	2	0	2	0	0	0	0	0	0	0	105
1	2	0	1	0	0	0	0	1	0	0	0	0	106
2	0	0	1	1	0	0	1	0	0	0	0	0	107
1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**
1	0	2	0	1	0	0	1	0	0	0	0	0	108
1	2	0	0	0	1	0	1	0	0	0	0	0	109
2	0	0	0	0	3	0	0	0	0	0	0	0	110
1	1	1	1	0	0	0	0	1	0	0	0	0	111
2	0	0	0	1	1	1	0	0	0	0	0	0	112
1	3	0	0	0	0	0	0	0	1	0	0	0	113
1	1	1	0	0	1	0	1	0	0	0	0	0	114
1	2	0	0	1	0	0	0	1	0	0	0	0	115
2	0	0	0	2	0	0	1	0	0	0	0	0	116
1	0	2	0	0	0	2	0	0	0	0	0	0	117
1	2	1	0	0	0	0	0	0	1	0	0	0	118
1	1	0	1	0	0	2	0	0	0	0	0	0	119
1	0	1	0	1	1	1	0	0	0	0	0	0	120
0	3	1	0	0	0	0	0	0	1	0	0	0	121
1	0	0	2	1	0	0	1	0	0	0	0	0	122
1	0	0	0	2	2	0	0	0	0	0	0	0	123
1	0	1	0	2	0	0	1	0	0	0	0	0	124
0	0	0	0	5	0	0	0	0	0	0	0	0	125
1	0	1	1	0	1	0	1	0	0	0	0	0	126
1	0	0	1	1	1	1	0	0	0	0	0	0	127
1	1	0	0	1	0	2	0	0	0	0	0	0	128
1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**
0	3	0	0	0	1	0	0	1	0	0	0	0	129
1	0	0	3	0	0	0	0	1	0	0	0	0	130
1	1	1	0	0	1	0	0	1	0	0	0	0	131
1	0	2	0	0	0	1	1	0	0	0	0	0	132
1	0	1	0	1	0	2	0	0	0	0	0	0	133
1	0	0	0	1	3	0	0	0	0	0	0	0	134
1	0	2	1	0	0	0	0	0	1	0	0	0	135
1	0	0	0	2	1	1	0	0	0	0	0	0	136
0	4	0	0	0	0	0	0	0	0	1	0	0	137
1	0	0	1	0	2	1	0	0	0	0	0	0	138
1	1	0	0	0	1	2	0	0	0	0	0	0	139
1	0	0	0	3	0	0	1	0	0	0	0	0	140
1	1	0	0	0	2	0	1	0	0	0	0	0	141
1	0	1	2	0	0	0	0	0	1	0	0	0	142
1	1	0	0	1	0	1	1	0	0	0	0	0	143
1	0	2	0	1	0	0	0	0	1	0	0	0	144
1	2	0	0	0	1	0	0	0	1	0	0	0	145
1	2	0	1	0	0	0	0	0	0	1	0	0	146
1	1	0	0	1	1	0	0	1	0	0	0	0	147
4	0	0	0	0	0	0	0	0	0	0	1	0	148
1	0	3	0	0	0	0	0	0	0	1	0	0	149
1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**

1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**
1	1	1	0	0	1	0	0	0	1	0	0	0	150
3	1	0	0	0	0	0	0	0	0	0	1	0	151
1	0	1	0	1	1	0	0	1	0	0	0	0	152
1	0	0	1	0	2	0	1	0	0	0	0	0	153
1	1	0	0	0	1	1	1	0	0	0	0	0	154
1	2	0	0	1	0	0	0	0	0	1	0	0	155
3	0	1	0	0	0	0	0	0	0	0	1	0	156
1	1	0	1	0	1	0	0	0	1	0	0	0	157
1	1	0	0	0	2	0	0	1	0	0	0	0	158
1	1	1	0	0	0	0	1	1	0	0	0	0	159
2	0	1	0	0	0	1	0	0	1	0	0	0	160
1	0	0	2	0	0	0	2	0	0	0	0	0	161
1	2	1	0	0	0	0	0	0	0	0	1	0	162
1	0	1	0	1	0	0	2	0	0	0	0	0	163
1	0	0	1	0	0	3	0	0	0	0	0	0	164
1	0	1	0	1	0	1	0	1	0	0	0	0	165
1	2	0	0	0	1	0	0	0	0	1	0	0	166
1	0	0	1	2	0	0	0	0	1	0	0	0	167
1	0	0	0	2	1	0	0	1	0	0	0	0	168
1	1	0	0	0	1	0	2	0	0	0	0	0	169
1	**4**	**9**	**16**	**25**	**36**	**49**	**64**	**81**	**100**	**121**	**144**	**169**	**Soma**

Apêndice C

Decomposição dos números até 676 em somas de 4 quadrados não nulos

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	1	1	4
1	1	1	4	7
1	1	4	4	10
1	1	1	9	12
1	4	4	4	13
1	1	4	9	15
4	4	4	4	16
1	4	4	9	18
1	1	1	16	19
1	1	9	9	20
4	4	4	9	21
1	1	4	16	22
1	4	9	9	23
1	4	4	16	25
4	4	9	9	26
1	1	9	16	27
1	1	1	25	28
1	4	9	16	30
1	1	4	25	31
4	4	9	16	33
1	1	16	16	34
1	9	9	16	35
1	1	9	25	36
1	4	16	16	37

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
4	9	9	16	38
1	1	1	36	39
4	4	16	16	40
1	1	4	36	42
1	1	16	25	43
1	9	9	25	44
1	4	4	36	45
1	4	16	25	46
1	1	9	36	47
4	4	4	36	48
1	16	16	16	49
1	4	9	36	50
1	9	16	25	51
1	1	1	49	52
4	4	9	36	53
1	1	16	36	54
1	1	4	49	55
1	4	16	36	57
1	4	4	49	58
9	9	16	25	59
1	1	9	49	60
4	4	4	49	61
1	9	16	36	62
1	1	25	36	63

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
16	16	16	16	64
4	9	16	36	65
1	4	25	36	66
1	1	1	64	67
1	9	9	49	68
1	16	16	36	69
1	1	4	64	70
1	9	25	36	71
4	16	16	36	72
1	4	4	64	73
1	1	36	36	74
1	1	9	64	75
1	1	25	49	76
1	4	36	36	77
1	4	9	64	78
1	4	25	49	79
4	4	36	36	80
4	4	9	64	81
1	1	16	64	82
1	9	9	64	83
1	1	1	81	84
1	4	16	64	85
4	9	9	64	86
1	1	4	81	87

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
4	4	16	64	88
1	16	36	36	89
1	4	4	81	90
1	1	25	64	91
1	1	9	81	92
4	4	4	81	93
1	4	25	64	94
1	4	9	81	95
1	16	16	64	97
1	25	36	36	98
1	1	16	81	99
1	1	49	49	100
4	25	36	36	101
1	1	36	64	102
1	1	1	100	103
16	16	36	36	104
1	4	36	64	105
1	1	4	100	106
1	9	16	81	107
1	1	25	81	108
1	4	4	100	109
1	9	36	64	110
1	1	9	100	111
4	4	4	100	112
4	9	36	64	113
1	4	9	100	114
1	1	49	64	115
1	9	25	81	116
1	16	36	64	117
1	1	16	100	118
1	1	36	81	119
4	16	36	64	120

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	4	16	100	121
1	4	36	81	122
1	9	49	64	123
1	1	1	121	124
4	4	36	81	125
1	9	16	100	126
1	1	4	121	127
4	9	16	100	129
1	1	64	64	130
9	9	49	64	131
1	1	9	121	132
1	4	64	64	133
1	16	36	81	134
1	4	9	121	135
4	4	64	64	136
1	36	36	64	137
1	1	36	100	138
1	1	16	121	139
1	9	9	121	140
1	4	36	100	141
1	4	16	121	142
1	25	36	81	143
4	4	36	100	144
1	16	64	64	145
1	9	36	100	146
1	1	1	144	147
1	1	25	121	148
4	9	36	100	149
1	1	4	144	150
1	1	49	100	151
16	36	36	64	152
1	4	4	144	153

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	4	49	100	154
1	1	9	144	155
1	9	25	121	156
4	4	49	100	157
1	4	9	144	158
1	1	36	121	159
16	16	64	64	160
4	4	9	144	161
1	1	16	144	162
1	9	9	144	163
1	1	81	81	164
1	4	16	144	165
1	1	64	100	166
1	4	81	81	167
4	4	16	144	168
1	4	64	100	169
1	9	16	144	170
1	1	25	144	171
1	1	1	169	172
1	36	36	100	173
1	4	4	100	174
1	1	4	169	175
4	36	36	100	176
1	16	16	144	177
1	4	4	169	178
1	9	25	144	179
1	1	9	169	180
1	16	64	100	181
1	1	36	144	182
1	1	81	100	183
4	16	64	100	184
1	4	36	144	185

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	4	81	100	186
1	1	16	169	187
1	9	9	169	188
4	4	81	100	189
1	4	16	169	190
1	9	81	100	191
16	16	16	144	192
1	64	64	64	193

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	36	36	121	194
1	1	49	144	195
1	1	25	169	196
1	16	36	144	197
1	4	94	144	198
1	1	1	196	199
4	16	36	144	200
1	36	64	100	201

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	36	36	121	194
1	1	49	144	195
1	1	25	169	196
1	16	36	144	197
1	4	94	144	198
1	1	1	196	199
4	16	36	144	200
1	36	64	100	201

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	64	144	210
1	16	25	169	211
1	9	81	121	212
1	4	64	144	213
1	1	16	196	214
1	9	9	196	215
4	4	64	144	216
1	4	16	196	217
1	9	64	144	218
1	16	81	121	219
1	1	49	169	220
4	9	64	144	221
1	9	16	196	222
1	1	25	196	223
1	16	64	144	225
1	4	25	196	226
1	1	81	144	227
1	1	1	225	228
1	16	16	196	229
1	4	81	144	230
1	1	4	225	231
4	16	16	196	232
4	4	81	144	233
1	1	36	196	234
1	1	64	169	235
1	1	9	225	236
1	4	36	196	237
1	4	64	169	238
1	4	9	225	239
4	4	36	196	240
4	4	64	169	241
1	9	36	196	242

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	16	225	243
1	1	121	121	244
1	36	64	144	245
1	1	100	144	246
1	1	49	196	247
4	36	64	144	248
1	4	100	144	249
1	4	49	196	250
1	9	16	225	251
1	1	25	225	252
4	4	49	196	253
1	9	100	144	254
1	4	25	225	255
64	64	64	64	256
4	9	100	144	257
1	16	16	225	258
1	1	1	256	259
1	9	25	225	260
1	16	100	144	261
1	1	4	256	262
1	1	36	225	263
4	16	100	144	264
1	4	4	256	265
1	4	36	225	266
1	1	9	256	267
1	25	121	121	268
1	36	36	196	269
1	4	9	256	270
1	1	100	169	271
4	36	36	196	272
1	64	64	144	273
1	1	16	256	274

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	9	9	256	275
1	1	49	225	276
1	4	16	256	277
1	16	36	225	278
1	1	81	196	279
4	4	16	256	280
1	36	100	144	281
1	4	81	196	282
1	1	25	256	283
1	9	49	225	284
4	4	81	196	285
1	4	25	256	286
1	9	81	196	287
16	64	64	144	288
1	16	16	256	289
1	1	144	144	290
1	1	64	225	291
1	1	1	289	292
1	4	144	144	293
1	1	36	256	294
1	1	4	289	295
4	4	144	144	296
1	4	36	256	297
1	1	100	196	298
1	9	64	225	299
1	1	9	289	300
1	4	100	196	301
1	9	36	256	302
1	4	9	289	303
4	4	100	196	304
1	16	144	144	305
1	9	100	196	306

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	16	289	307
1	1	81	225	308
1	16	36	256	309
1	4	16	289	310
1	4	81	225	311
4	16	36	256	312
1	16	100	196	313
1	25	144	144	314

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	144	169	315
1	1	25	289	316
4	25	144	144	317
1	4	144	169	318
1	1	121	196	319
16	16	144	144	320
4	4	144	169	321
1	1	64	256	322

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	9	144	169	323
1	9	25	289	324
1	4	64	256	325
1	36	64	225	326
1	1	1	324	327
4	4	64	256	328
1	36	36	256	329
1	1	4	324	330

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	16	25	289	331
1	25	81	225	332
1	4	4	324	333
1	16	121	196	334
1	1	9	324	335
4	4	4	324	336
1	16	64	256	337
1	4	9	324	338
1	1	81	256	339
1	1	49	289	340
4	4	9	324	341
1	1	16	324	342
1	4	49	289	343
16	36	36	256	344
1	4	16	324	345
1	25	64	256	346
1	9	81	256	347
1	1	121	225	348
4	25	64	256	349
1	9	16	324	350
1	1	25	324	351
16	16	64	256	352
1	64	144	144	353
1	4	25	324	354
1	1	64	289	355
1	9	121	225	356
1	16	16	324	357
1	1	100	256	358
1	9	25	324	359
4	16	16	324	360
1	4	100	256	361
1	1	36	324	362

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	9	64	289	363
1	1	1	361	364
1	4	36	324	365
1	9	100	256	366
1	1	4	361	367
4	4	36	324	368
4	9	100	256	369
1	4	4	361	370
1	1	144	225	371
1	1	9	361	372
1	16	100	256	373
1	4	144	225	374
1	1	49	324	375
4	16	100	256	376
1	16	36	324	377
1	4	49	324	378
1	1	16	361	379
1	9	9	361	380
4	4	49	324	381
1	4	16	361	382
1	9	49	324	383
1	64	64	256	385
1	16	144	225	386
1	9	16	361	387
1	1	25	361	388
1	100	144	144	389
1	1	64	324	390
1	1	100	289	391
4	100	144	144	392
1	4	64	324	393
1	1	196	196	394
1	25	144	225	395

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	169	225	396
1	4	196	196	397
1	9	64	324	398
1	1	36	361	399
4	4	196	196	400
4	9	64	324	401
1	1	144	256	402
1	1	1	400	403
1	9	169	225	404
1	4	144	256	405
1	1	4	400	406
1	1	81	324	407
4	4	144	256	408
1	4	4	400	409
1	4	81	324	410
1	1	9	400	411
1	1	49	361	412
4	4	81	324	413
1	4	9	400	414
1	4	49	361	415
64	64	144	144	416
1	16	144	256	417
1	1	16	400	418
1	9	9	400	419
1	9	49	361	420
1	4	16	400	421
1	16	81	324	422
1	1	196	225	423
4	4	16	400	424
1	36	64	324	425
1	1	100	324	426
1	1	25	400	427

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	81	121	225	428
1	4	100	324	429
1	4	25	400	430
1	9	196	225	431
4	4	100	324	432
1	16	16	400	433
1	9	100	324	434
1	1	144	289	435

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	25	49	361	436
1	36	144	256	437
1	1	36	400	438
1	49	100	289	439
4	36	144	256	440
1	4	36	400	441
1	16	25	400	442
1	9	144	289	443

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	1	441	444
4	16	25	400	445
1	9	36	400	446
1	1	4	441	447
16	16	16	400	448
4	9	36	400	449
1	4	4	441	450
1	1	49	400	451

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	9	441	452
1	16	36	400	453
1	1	196	256	454
1	4	9	441	455
4	16	36	400	456
1	4	196	256	457
1	36	196	225	458
1	1	16	441	459
1	1	169	289	460
1	36	100	324	461
1	4	16	441	462
1	1	100	361	463
4	36	100	324	464
1	64	144	256	465
1	1	64	400	466
1	9	16	441	467
1	1	25	441	468
1	4	64	400	469
1	1	144	324	470
1	4	25	441	471
4	4	64	400	472
1	4	144	324	473
1	9	64	400	474
1	16	169	289	475
1	9	25	441	476
4	9	64	400	477
1	9	144	324	478
1	1	36	441	479
16	64	144	256	480
1	16	64	400	481
1	4	36	441	482
1	1	81	400	483

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	1	121	361	484
1	16	144	324	485
1	4	81	400	486
1	1	1	484	487
4	16	144	324	488
1	36	196	256	489
1	1	4	484	490
1	9	81	400	491
1	1	49	441	492
1	4	4	484	493
1	16	36	441	494
1	1	9	484	495
4	4	4	484	496
4	16	36	441	497
1	4	9	484	498
1	16	121	361	499
1	9	49	441	500
1	36	64	400	501
1	1	16	484	502
1	9	9	484	503
4	36	64	400	504
1	4	16	484	505
1	81	100	324	506
1	1	64	441	507
1	25	121	361	508
4	81	100	324	509
1	4	64	441	510
1	1	25	484	511
4	4	64	441	513
1	1	256	256	514
1	9	64	441	515
1	1	225	289	516

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	4	256	256	517
1	36	81	400	518
1	4	225	289	519
4	4	256	256	520
4	36	81	400	521
1	1	36	484	522
1	1	121	400	523
1	1	81	441	524
1	4	36	484	525
1	4	121	400	526
1	4	81	441	527
4	4	36	484	528
1	16	256	256	529
1	9	36	484	530
1	9	121	400	531
1	1	1	529	532
1	64	144	324	533
1	81	196	256	534
1	1	4	529	535
4	64	144	324	536
1	16	36	484	537
1	4	4	529	538
1	16	81	441	539
1	1	9	529	540
4	4	4	529	541
1	36	64	441	542
1	1	100	441	543
16	16	256	256	544
1	144	144	256	545
1	1	144	400	546
1	1	16	529	547
1	9	9	529	548

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	4	144	400	549
1	1	64	484	550
1	1	225	324	551
4	4	144	400	552
1	4	64	484	553
1	4	225	324	554
1	9	16	529	555
1	1	25	529	556

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	36	36	484	557
1	9	64	484	558
1	1	196	361	559
4	36	36	484	560
1	16	144	400	561
1	4	196	361	562
1	81	81	400	563
1	1	121	441	564

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
1	16	64	484	565
1	16	225	324	566
1	1	36	529	567
4	16	64	484	568
1	100	144	324	569
1	4	36	529	570
1	1	169	400	571
1	9	121	441	572

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
4	4	36	529	573
1	4	169	400	574
1	9	36	529	575
16	16	144	400	576
1	64	256	256	577
1	36	100	441	578
1	1	1	576	579
1	1	49	529	580
1	36	144	400	581
1	1	4	576	582
1	4	49	529	583
4	36	144	400	584
1	4	4	576	585
1	1	100	484	586
1	1	9	576	587
1	2	225	361	588
1	4	100	484	589
1	4	9	576	590
1	4	225	361	591
4	4	100	484	592
4	4	9	576	593
1	1	16	576	594
1	1	64	529	595
1	9	225	361	596
1	4	16	576	597
1	1	196	400	598
1	36	121	441	599
4	4	16	576	600
1	4	196	400	601
1	9	16	576	602
1	1	25	576	603
1	25	49	529	604

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
4	9	16	576	605
1	4	25	576	606
1	1	121	484	607
64	144	144	256	608
1	16	16	576	609
1	4	121	484	610
1	9	25	576	611
1	1	81	529	612
1	16	196	400	613
1	1	36	576	614
1	1	289	324	615
4	16	196	400	616
1	4	36	576	617
1	4	289	324	618
1	1	256	361	619
1	9	81	529	620
1	36	100	484	621
1	4	256	361	622
1	9	289	324	623
4	36	100	484	624
4	4	256	361	625
1	81	144	400	626
1	1	49	576	627
1	1	1	625	628
1	16	36	576	629
1	1	144	484	630
1	1	4	625	631
4	16	36	576	632
1	4	144	484	633
1	4	4	625	634
1	9	49	576	635
1	1	9	625	636

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
4	4	4	625	637
1	9	144	484	638
1	1	196	441	639
64	64	256	256	640
4	9	144	484	641
1	1	64	576	642
1	1	16	625	643
1	9	9	625	644
1	4	64	576	645
1	4	16	625	646
1	9	196	441	647
4	4	64	576	648
1	36	36	576	649
1	1	324	324	650
1	9	16	625	651
1	1	25	625	652
1	4	324	324	653
1	16	196	441	654
1	1	169	484	655
4	4	324	324	656
1	16	64	576	657
1	1	256	400	658
1	1	81	576	659
1	9	25	625	660
1	4	256	400	661
1	4	81	576	662
1	1	36	625	663
4	4	256	400	664
1	16	324	324	665
1	4	36	625	666
1	9	81	576	667
1	1	225	441	668

Q_1	Q_2	Q_3	Q_4	$\sum_{i=1}^{4} Q_i$
4	4	36	625	669
1	16	169	484	670
1	4	225	441	671
16	16	64	576	672
1	16	256	400	673
1	16	81	576	674
1	1	144	529	675
1	1	49	625	676

Afterword

The back matter often includes one or more of an index, an afterword, acknowledgements, a bibliography, a colophon, or any other similar item. In the back matter, chapters do not produce a chapter number, but they are entered in the table of contents. If you are not using anything in the back matter, you can delete the back matter TeX field and everything that follows it.

Bibliografia

[1] BRISON, O. J., Grupos e Representações (1999), Lisboa, Faculdade de Ciências de Lisboa

[2] BRISON, O. J., Teoria de Galois (1998), 2^a edição, Lisboa, Faculdade de Ciências de Lisboa

[3] GROSSWALD, E., Representation of Integers as Sums of Squares (1985), New York, Springer-Verlag

[4] LEVEQUE, W. J., Fundamentals of Number Theory (1996), New York, Dover

[5] ANDREWS E. G., Number Theory (1994), New York, Dover

[6] HARDY, G. H. & WRIGHT, E. M., An Introduction to the Number Theory (1960), 4th edition, London, Oxford at Clarendon Press

[7] SWETZ, F. J., From Five Fingers to Infinity (1994), Chicago, Open Court

[8] STARK, H. M., An Introduction to Number Theory (1978), Cambridge, The MIT Press