UNIVERSIDADE ESTADUAL DE CAMPINAS
DEPARTAMENTO DE MATEMATICA ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Inteiros que são soma de dois quadrados

Ana Carolina Neves Pinto – 80603
Bruno Alves Pereira – 90531
Lislene Heloisa Alves – 81948
Natália Silvério Baldon – 82373
Luiz Fernando Campos de Oliveira - 82043
Viviane Reis e Silva – 86431

CAMPINAS, NOVEMBRO DE 2011

Inteiros que são soma de dois quadrados

Introdução

O Problema de Waring

Num trabalho publicado em 1770, Waring afirmou que todo número inteiro positivo é a soma de no máximo 4 quadrados, 9 cubos e no máximo 19 quarta potências.

Embora ele não tenha apresentado nenhuma demonstração para estas afirmações, às quais deve ter sido levantado pela observação de muitos exemplos, provavelmente ele suspeitava da existência, para cada inteiro positivo k, de um inteiro positivo g(k), tal que todo inteiro positivo n pudesse ser expresso como a soma de no máximo g(k) k-ésimas positivas potências.

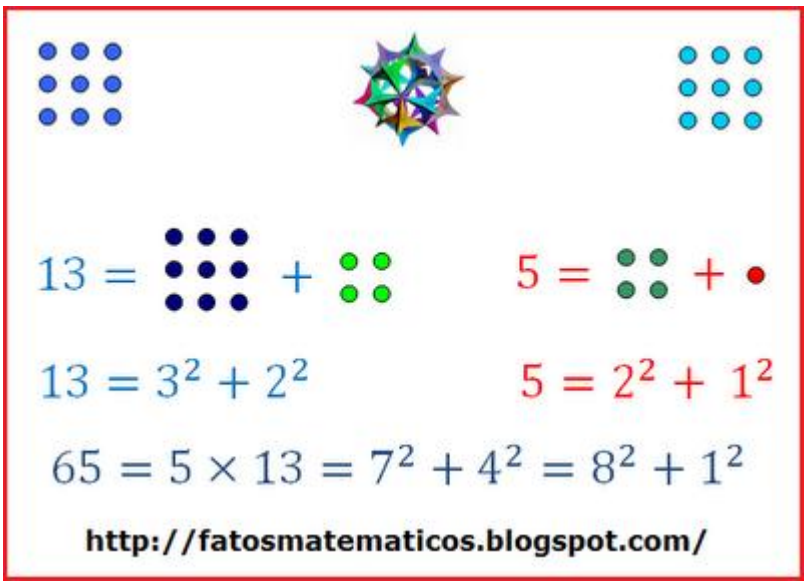
No mesmo ano de 1770, Lagrange demonstrou que todo inteiro é a soma de no máximo quatro quadrados.

Somente em 1859 é que surgiu a demonstração para o fato de que todo inteiro é a soma de no máximo 9 cubos. Em 1909 Hilbert provou a existência, para todo k de um inteiro positivo g(k), independente de *n*, com a propriedade de que todo inteiro *n* pode ser expresso como a soma de no máximo g(k) k-ésimas potências. A demonstração, por ele apresentada, prova apenas a existência de g(k), mas não fornece informações sobre o valor real de g(k).

Hardy e Littlewood desenvolveram métodos analíticos fornecendo limitantes superiores para g(k) para todo k.

Em nossa monografia, caracterizamos os inteiros que possuem representação como soma de dois quadrados e apresentaremos um resultado de Euler que nos diz que certos primos possuem representação única como soma de dois quadrados.

Soma de Dois Quadrados



Quais os números que podem ser escritos como soma de dois quadrados? Ou três quadrados? Existe algum número natural N de modo que possa ser escrito como soma de dois, três, quatro, ..., N quadrados simultaneamente?

Definição 1: Dizemos que um inteiro positivo n pode ser representando como soma de dois quadrados se $x^2 + y^2 = n$ para algum x, y pertencentes a Z positivos.

Observação 1: Por comodidade, incluiremos o zero como uma possibilidade para x ou y. Assim, os quadrados perfeitos estão incluídos nesta lista, pois $m^2 = m^2 + 0^2$.

Na listagem abaixo, temos as possíveis representações dos 15 primeiros números naturais, onde "**nsq**" significa que o *número não é soma de dois quadrados*.

- $1 = 1^2 + 0^2$
- $2 = 1^2 + 1^2$
- 3 = nsq
- $4 = 2^2 + 0^2$
- $5 = 2^2 + 1^2$
- 6 = nsq
- 7 = nsq
- $8 = 2^2 + 2^2$
- $9 = 3^2 + 0^2$
- $10 = 3^2 + 1^2$
- 11 = nsq
- 12 = nsq
- $13 = 2^2 + 3^2$
- 14 = nsq
- 15 = nsq

Agora matematicamente, vamos caracterizar todos os inteiros *n* para os quais a equação

$$x^2 + y^2 = n \qquad (1.1)$$

possui solução em inteiros. Neste resultado, demonstrado primeiramente por Fermat, utilizamos a seguinte identidade, a qual é verdadeira para quaisquer números reais *a, b, c* e *d.*

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \qquad (1.2)$$

Esse fato elementar nos diz que o produto de números que podem ser representados pela soma de dois quadrados também pode ser representado como soma de dois quadrados. Uma forma simples de se verificar (1.2) é pela consideração de complexos $\alpha = a + bi$ e $\beta = d + ci$ lembrando que $\alpha\bar{\alpha}\beta\bar{\beta} = \alpha\beta\,\overline{\alpha\beta}$.

Iniciamos com um resultado no qual identificamos os primos que possuem representação como soma de dois quadrados.

Teorema 1.1 *Sendo* p *um primo a equação* $x^2 + y^2 = p$ *possui solução inteira se, e somente se,* $p = 2$ *ou* $p \equiv 1 \pmod 4$.

Demonstração: Observamos, inicialmente, que $2 = 1^2 + 1^2$. Sabemos que para todo primo ímpar p temos $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$.
Como, para todo inteiro *a*, $a^2 \equiv 0$ ou $1 \pmod 4$ vemos que se $x^2 + y^2 = p$ então $p \equiv 1 \pmod 4$.

Resta-nos mostrar que todo p satisfazendo $p \equiv 1 \pmod 4$ pode ser expresso como soma de dois quadrados.

Tomamos, pois, um primo $p \equiv 1 \pmod 4$. Pelo Teorema I existe x tal que $x^2 \equiv -1 \pmod p$. Com este x definimos a função $f(u,v) = u + xv$ e tomamos $m = [\sqrt{p}]$. Como $\sqrt{p}$ não é um inteiro temos $m < \sqrt{p} < m+1$. Consideramos os pares (u,v) de inteiros onde $0 \le u \le m$ e $0 \le v \le m$. Desta forma vemos que u pode assumir m+1 valores e v, também, pode assumir m+1 valores. Portanto o número total de pares é $(m+1)^2$. Como $m+1 > \sqrt{p}$ temos que $(m+1)^2 > p$, isto é, o total de pares é superior a p. Como um sistema completo de resíduos módulo p possui exatamente p elementos, concluímos que se considerarmos f(u,v) módulo p teremos mais números do que classes de resíduos para coloca-los. Logo, pelo Princípio da Casa dos Pombos, existem pelo menos dois pares distintos (u_1,v_1) e (u_2,v_2) com coordenadas satisfazendo $0 \le u_i \le m$ e $0 \le v_i \le m (i = 1,2)$ para os quais

$$f(u_1,v_1) \equiv f(u_2,v_2) \pmod p.$$

Isto equivale a $u_1 + xv_1 \equiv u_2 + xv_2 \pmod p$, isto é, $u_1 - u_2 \equiv -x(v_1 - v_2) \pmod p$.

Elevando-se ao quadrado ambos os membros desta última congruência temos:

$$(u_1 - u_2)^2 \equiv x^2 (v_1 - v_2)^2 \equiv -(v_1 - v_2)^2 \pmod{p}$$

uma vez que $x^2 \equiv -1 \pmod{p}$.

Definindo $a = u_1 - u_2$ e $b = v_1 - v_2$ obtemos

$$a^2 + b^2 \equiv 0 \pmod{p}$$

ou seja, $p \mid (a^2 + b^2)$. Como os pares (u_1,v_1) e (u_2,v_2) são distintos, a e b não são ambos nulos, isto é, $a^2 + b^2 > 0$.

Sendo u_1 e u_2 inteiros no intervalo [0,m] temos que $a = u_1 - u_2$ satisfaz $-m \leq a \leq m$. também para $b = v_1 - v_2$ temos $-m \leq b \leq m$ pela mesma razão. Como $m < \sqrt{p}$ concluímos que $|a| < \sqrt{p}$ e $|b| < \sqrt{p}$. Isto nos diz que $a^2 + b^2 < 2p$.

Logo $a^2 + b^2$ é um inteiro divisível por p e satisfazendo $0 < a^2 + b^2 < 2p$. Como o único inteiro múltiplo de p neste intervalo é p, concluímos que $a^2 + b^2 = p$.

□

Este resultado nos permite, agora, identificar todos os inteiros que possuem representação como soma de dois quadrados.

Teorema 1.2: *Um inteiro* n *pode ser representado como a soma de dois quadrados se, e somente se, tiver fatoração da forma*

$$n = 2^{\alpha} p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_r^{\alpha r} q_1^{\beta 1} q_2^{\beta 2} \ldots q_s^{\beta s}$$

onde $p_i \equiv 1 \pmod 4$ e $q_i \equiv 3 \pmod 4$, i = 1, 2, ..., r j = 1, 2, ..., s *e todos os expoentes* β_j *são pares.*

Demonstração: Sabemos que $2 = 1^2 + 1^2$ e que pelo Teorema 1.1 todos os p_i's podem ser representados pela soma de dois quadrados. Logo se β_j's forem pares cada um pode ser escrito como $\beta_i = 2\beta_i'$ o que nos diz que $q_j^{\beta j} = (q_j^2)^{\beta j'}$. Mas $q_j^2 = q_j^2 + 0^2$, ou seja, q_j^2 é a soma de dois quadrados.

Disto concluímos, usando a equação (1.2), que se todos os β_j's forem pares, n terá representação como soma de dois quadrados.

Suponhamos, agora, que n possa ser representado como soma de dois quadrados e que algum β_j seja ímpar. Sem perda de generalidade podemos considerar β_1 ímpar. Seja d = (a,b) onde a e b são inteiros tais que $a^2 + b^2 = n$.

Como $d \mid a$ e $d \mid b$ temos $a = k_1 d$ e $b = k_2 d$. Sabemos, pelo corolário da Preposição II, que $(a/d , b/d) = 1$, isto é, $(k_1, k_2) = 1$. Como $d^2 \mid n$, temos $n = kd^2$. Portanto,

Teoremas adicionais

Teorema I: *Para* p *primo, a congruência* $x^2 \equiv -1 \pmod p$ *tem solução se, e somente se,* $p = 2$ *ou* $p \equiv 1 \pmod 4$.

Demonstração: É claro que x = 1 nos fornece uma solução se p = 2. Vamos construir uma solução para o caso $p \equiv 1 \pmod 4$.

Para p um primo ímpar podemos escrever o Teorema de Wilson da seguinte forma:

$$(1 \cdot 2 \cdot 3 \ldots j \ldots (\tfrac{p-1}{2})) ((\tfrac{p+1}{2}) \ldots (p - j) \ldots (p - 2) (p - 1)) \equiv -1 \pmod p$$

Observamos que o produto (p - 1)! está dividido em duas partes, cada uma com o mesmo número de fatores. Podemos reescrever este produto formando pares, uma vez que para cada fator j na primeira parte temos o fator (p - j) na segunda. Logo, pelo Teorema de Wilson pode escrito como:

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

Como $j(p - j) \equiv -j^2 \pmod p$ temos:

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

Mas sendo $p \equiv 1 \pmod 4$, sendo (p - 1)/2 é par e, portanto,

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

é solução de $x^2 \equiv -1 \pmod p$.

Suponhamos, agora, que a congruência $x^2 \equiv -1 \pmod p$ tenha solução e que p > 2. Elevando ambos os membros à potencia (p - 1)/2 obtemos:

$$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod p$$

Como $(x^2)^{(p-1)/2} \equiv x^{(p-1)} \pmod p$, pelo Teorema IV (observe que p não divide x pois $x^2 \equiv -1 \pmod p$) temos que

$$(-1)^{(p-1)/2} \equiv 1 \pmod p$$

Logo $(p-1)/2$ é par, ou seja $p \equiv 1 \pmod 4$. □

Preposição II: *Se* c > 0 *e* a *e* b *são divisíveis por* c, então

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$$

Demonstração: Como a e b são divisíveis por c, temos que a/c e b/c são inteiros. Basta, então, substituir na Preposição V "a" por "a/c" e "b" por "b/c" tomando t = c.

Teorema III: *Sejam* a, b *e* m *inteiros tais que* m > 0 *e* (a,m) = d. *no caso em que* d *não divide* b *a congruência* $ax \equiv b \pmod m$ *não possui nenhuma solução e quando* d *divide* b, *possui exatamente* d *soluções incongruentes módulo* m.

Demonstração: Sabemos que o inteiro x é solução de $ax \equiv b \pmod m$ se, e somente se, existe um inteiro y tal que ax = b + my, ou, o que é equivalente, ax – my = b. Sabemos que esta equação não possui nenhuma solução caso d não divide b, e que se d divide b ela possui infinitas soluções dadas por $x = x_0 - (m/d)k$ e $y = y_0 - (a/d)k$ onde (x_0, y_o) é uma solução particular de ax – my = b. Logo a congruência $ax \equiv b \pmod m$possui infinitas soluções dadas por $x = x_0 - (m/d)k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob que condições $x_1 = x_0 - (m/d)k_1$ e $x_2 = x_0 - (m/d)k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes então $x_0 - (m/d)k_1 \equiv x_0 - (m/d)k_2 \pmod m$, e como $(m/d) \mid m$, temos $(m/d\ ,\ m) = m/d$, o que nos permite o cancelamento de m/d, resultando $k_1 \equiv k_2 \pmod d$. observe que m foi substituído por d = m/(m/d). Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. □

Teorema IV: (Pequeno Teorema de Fermat) *Seja* p *primo. Se* p *não divide* a *então* $a^{(p-1)} \equiv 1 \pmod p$.

Demonstração: Sabemos que o conjunto formado pelos p números 0, 1, 2, ..., p-1 constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser

colocado em correspondência biunívoca com um subconjunto de {0, 1, 2, ..., p - 1}. Vamos, agora, considerar os números a, 2a, 3a, ..., (p - 1)a. Como (a,p) = 1, nenhum destes números ia, $1 \leq i \leq p - 1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dos dois deles são incongruentes módulo p, pois $aj \equiv ak \pmod{p}$ implica $j \equiv k \pmod{p}$ e isto só é possível se j = k, uma vez que ambos j e k são positivos menores do que p. temos, portanto, um conjunto de p – 1 elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos 1, 2, 3. ..., p – 1. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a\,(2a)\,(3a) \ldots (p-1)\,a \equiv 1.2.3 \ldots (p-1) \pmod{p}$$

ou seja $a^{(p-1)}(p-1)! \equiv (p-1)! \pmod{p}$. Mas, como ((p - 1)! , p) = 1, podemos cancelar o fator (p - 1)! em ambos os lados, obtendo

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

o que conclui a demonstração. □

Preposição V: *Para todo inteiro positivo* t*,* (ta,tb) = t(a,b).

Demonstração: Temos que (ta,tb) é o menor valor positivo de mta + ntb (m e n inteiros), que é igual a t vezes o menor valor positivo de ma + nb = t . (a,b).

Um Teorema de Unicidade de Euler

Com a finalidade de provarmos que certos primos possuem representação única como soma de dois quadrados, vamos necessitar de algumas proposições.

Proposição 1.3: *Se um primo* $p = c^2 + d^2$ *e se existir* $q > 1$ *tal que* $pq = a^2 + b^2$, $(a,b) = 1$, *então* q *é a soma dos quadrados de dois inteiros relativamente primos.*

Demonstração: É claro que se $p = c^2 + d^2$, p primo, então $(c,d) = 1$. Sendo $pq = a^2 + b^2$ temos

$$c^2(a^2 + b^2) - a^2(c^2 + d^2) = c^2pq - a^2p = kp$$

onde $k = c^2q - a^2$. Logo,

$$\begin{aligned} kp &= c^2(a^2 + b^2) - a^2(c^2 + d^2) \\ &= b^2c^2 - a^2d^2 = (bc - ad)(bc + ad) \end{aligned}$$

O que nos diz que p divide pelo menos um dos fatores (bc - ad) e (bc + ad). Temos $bc – ad \neq 0$ pois bc = ad implica que a = c e b = d (lembre-se que (a,b) = (c,d) = 1), o que implicaria p e pq iguais.

Se $p \mid (bc - ad)$ temos $bc – ad = tp$. Sejam

$$\begin{aligned} r &= b – tc \\ s &= a + td \end{aligned} \qquad (1.3)$$

Multiplicando-se a primeira das igualdades em (1.3) por “c” e a segunda por “d” temos

$$\begin{aligned} cr &= bc – tc^2 \\ ds &= ad + td^2 \end{aligned}$$

Subtraindo, membro a membro, obtemos

$$cr – ds = (bc - ad) – t(c^2 + d^2) = tp – tp = 0$$

isto é, cr = ds, ou seja, r = d s/c e, como (c,d) = 1, n= s/c é inteiro.

Sendo s = c a/c temos que

$$r = nd \qquad e \qquad s = nc \tag{1.4}$$

Neste caso de (1.3) temos

$$pq = a^2 + b^2 = (nc - td)^2 + (tc + nd)^2$$
$$= (t^2 + n^2)(c^2 + d^2) = p(t^2 + n^2),$$

e, portanto, $q = (t^2 + n^2)$. O fato de (t,n) = 1 segue de (1.3) juntamente com (1.4) uma vez que (a,b) = 1.

O caso $p \mid (bc + ad)$ é semelhante, isto é, se bc + ad = kp definimos

$$r = b – kc$$
$$s = a - kd \tag{1.5}$$

Logo,

$$cr = bc – kc^2$$
$$ds = ad - kd^2$$

e, portanto, $cr + ds = (bc + ad) – k(c^2 + d^2) = kp – kp = 0$. Disto concluímos que cr = ds, r = dn e s = -cn, onde n = -s/c.

Levando-se estes valores em (1.5) obtemos

$$pq = a^2 + b^2 = (nc - td)^2 + (tc + nd)^2$$
$$= (t^2 + n^2)(c^2 + d^2) = p(t^2 + n^2),$$

segue pela substituição de r = dn e s = -cn em (1.5) mais o fato de (a,b) = 1.

A proposição seguinte é consequência imediata da anterior.

Preposição 1.4: *Se* pq *é a soma dos quadrados de dois inteiros relativamente primos e* q *não é a soma de dois quadrados de inteiros relativamente primos, então* p *possui um fator primo que não é a soma de dois quadrados.*

Demosntração: Se $p = p_1 p_2 ... p_n$ onde cada primo p_i (i = q, 2, ..., n) é a soma de dois quadrados. Como

p_1 (p_2 p_3... p_n q) = pq é a soma de dois quadrados inteiros primos entre si, a proposição anterior nos diz que p_2 p_3 ... p_n é a soma de dois quadrados inteiros relativamente primos. Repetindo este procedimento concluímos que q é a soma de dois quadrados inteiros relativamente primos, o que é uma contradição. Disto concluímos que se q não pode ser expresso como soma de dois quadrados inteiros relativamente primos e pq pode, então p, necessariamente, deve possuir um fator primo que não é soma de dois quadrados inteiros primos entre si.

Preposição 1.5: *Se um primo* p *divide* $a^2 + b^2$ *com* (a,b) = 1, *então* p *é a soma de dois quadrados.*

Demosntração: A prova que apresentamos é por contradição utilizando a Proposição 1.4. Suponhamos que p não seja a soma de dois quadrados e que $p \mid (a^2 + b^2)$ com (a,b) = 1.

Como p não divide a e p não divide b temos, que existem q_1, q_2, r_1 e r_2 satisfazendo

$$a = q_1p \pm r_1 \quad 0 < r_1 \leq p/2$$
$$b = q_2p \pm r_2 \quad 0 < r_2 \leq p/2$$

Logo, $r_1^2 + r_2^2 = a^2 + b^2 + mp = Mp \leq p^2/2$.

Como r_1 e r_2 são menores do que p, qualquer divisor comum de r_1 e r_2 deve dividir M. Fazendo, se necessário, estas simplificações, obtemos

$$a_1^2 + b_1^2 = np, \qquad \text{com } (a_1, b_1) = 1$$

A proposição 1.4 nos garante que n possui um fator primo p_1 no qual não é a soma de dois quadrados e satisfaz $p_1 \leq p/2$.

Se repetirmos exatamente o processo descrito acima com p_1 no lugar de p iremos obter um primo p_2 , $p_2 < p_1$, o qual não é soma de dois quadrados. Mas esta afirmação contradiz o fato de que os fatores primos de todas as somas de dois números relativamente primos pequenos são expressos como soma de dois quadrados. ($3^2 + 4^2 = 5^2$, $3^2 + 2^2 = 13$, $3^2 + 1^2 = 10$, $2^2 + 1^2 = 5$, $1^2 + 1^2 = 2$).

Com este resultado podemos, agora, apresentar uma das demonstrações dadas por Euler para a unicidade da representação de certos primos como a soma de quadrados.

Teorema 1.3: *Todo primo da forma* 4n + 1 *possui representação única como soma de dois quadrados.*

Demonstração: Pelo Teorema I sabemos que -1 é um resíduo quadrático para todo primo $p \equiv 1 \pmod 4$, isto é, que existe um inteiro "a" tal que $a^2 \equiv -1 \pmod p$ para p primo, p = 4n +1.

Logo como $p \mid a^2 + 1$ concluímos pela Proposição 1.4, que p é soma de dois quadrados. Suponhamos a existência de duas representações distintas para p, isto é, $p = a^2 + b^2 = c^2 + d^2$. Sendo p ímpar um dos números a e b é um ímpar enquanto o outro é par. É claro que o mesmo se verifica para os números c e d.

Como $a^2 + b^2 = c^2 + d^2$ temos $a^2 - c^2 = d^2 - b^2$ e, portanto, (a - c)(a + c) = (d - b)(d + b). Seja r = (a – c , d - b), logo a – c = mr e d – b = nr onde (n,m) = 1. Portanto, m(a + c) = n(d + b). Sendo (m,n) = 1, se tomarmos s = (a + c , d + b), concluímos que a + c = ns e d + b = ms. Se a e c são ambos pares ou ambos ímpares temos que r e s são ambos ímpares. Neste caso m e n são ímpares.

É fácil ver que

$$\begin{aligned}(r^2 + s^2)(m^2 + n^2) &= m^2r^2 + m^2s^2 + n^2r^2 + n^2s^2 \\ &= (a - c)^2 + (d + b)^2 + (d - b)^2 + (a + c)^2 \\ &= 2(a^2 + b^2) + 2(c^2 + d^2)\end{aligned}$$

Dividindo, membro a membro, por 4 obtemos:

$$[(r^2 + s^2)(m^2 + n^2)]/4 = [(a^2 + b^2)]/2 + [(c^2 + d^2)]/2 = p$$

Esta última igualdade nos diz que r e s são pares então p é o produto dos inteiros $(m^2 + n^2)/2$ e $(r^2 + s^2)/2$ os quais são maiores do que 1. Se r e s são ímpares eles não podem ser ambos iguais a 1 pois teríamos, neste caso, a = d e b = c. a hipótese de m = n = 1 também nos daria a = d e b = c. portanto, quando r e s são ímpares, p é o produto de $(r^2 + s^2)/2$ e $(m^2 + n^2)/2$ os quais são, ambos, diferentes de 1. Como as duas fatorações acima são impossíveis, uma vez que p é primo, a representação de $p(p \equiv 1 (\mathrm{mod}\, 4))$ como a soma de quadrados é única. □

Grupos

Definição 2: Um conjunto S de números não negativos é um semigrupo multiplicativo se, e somente se, ele tem o produto de cada par de seus elementos, como elemento de S, isto é,

$$\begin{cases} x \in S \\ y \in S \end{cases} \Rightarrow xy \in S$$

Por exemplo, o conjunto N^+ é um semigrupo multiplicativo. O conjunto Z_+ também é de todos os inteiros não negativos é um semigrupo multiplicativo. O conjunto P de todos os pares positivos e de todos os ímpares positivos são também exemplos de semigrupos multiplicativos.

Proposição 1: Se S é um semigrupo multiplicativo de inteiros não negativos, e todos os primos pertencem a S, então os inteiros maiores que 1 pertencem a S.

Demonstração: Isto é apenas outro modo de enunciar o Teorema Fundamental da Aritmética que afirma que todos os naturais maiores que 1 é produto de números primos.

A conexão entre semigrupos e a soma de dois quadrados é dado pelo seguinte Teorema:

Proposição 2: O conjunto $S_2 = \{m^2 + n^2 : m, n \in Z_+\}$ da soma de dois quadrados é um semigrupo multiplicativo.

Demonstração: Usaremos números complexos. Seja z = a + bi

$$z \cdot \bar{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2$$

Agora sejam x_1, y_1, x_2 e y_2 inteiros não negativos. Queremos mostrar que

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

é a soma de dois inteiros ao quadrados, isto é, possui a forma $x_3^2 + y_3^2$ para algum x_3, y_3 Є Z. Fazendo $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$, $x_3 = \text{Re}(z_1 z_2)$ e $y_3 = \text{Im}(z_1 z_2)$, segue que

$$\begin{aligned}(x_1^2 + y_1^2)(x_2^2 + y_2^2) &= |z_1|^2 |z_2|^2 = z_1 \bar{z_1} z_2 \bar{z_2} \\ &= z_1 z_2 (\bar{z_1} \bar{z_2}) = (z_1 z_2)(\bar{z_1} \bar{z_2}) = |z_1 z_2|^2 \\ &= \text{Re}(z_1 z_2)^2 + \text{Im}(z_1 z_2)^2 = x_3^2 + y_3^2\end{aligned}$$

Exemplo

1. Mostre que 65 é soma de dois quadrados e ache os naturais a e b tal que $65 = a^2 + b^2$.

Resolução: Sendo 65 = 13 x 5 e pela listagem anterior $5 = 1^2 + 2^2$ e $13 = 2^2 + 3^2$, Segue da Preposição 1, que 65 é soma de dois quadrados. Para achar a e b, considere os números complexos z_1 e z_2 formado pelas parcelas dos números 5 e 13, isto é

$$z_1 = 1 + 2i \text{ e } z_2 = 2 + 3i$$

Como

$$z_1 z_2 = (1 + 2i)(2 + 3i) = -4 + 7i$$

Segue que a = 4 e b = 7, de modo que $65 = 4^2 + 7^2$.

Curiosidade

Vamos demonstrar a fórmula da soma dos quadrados dos *"n"* primeiros números naturais não nulos (não se preocupe isso não é cobrado no vestibular da UFRGS):

$$\{1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + ... + n^2\}$$

Para entender esta demonstração, devemos saber algumas coisas antes. Quanto vale $\boldsymbol{(a+b)^3}$?

Vamos ver:

$(a + b)^3 = (a + b) \cdot (a + b) \cdot (a + b)$
$(a + b)^3 = (a + b)^2 \cdot (a + b)$
$(a + b)^3 = (a^2 + 2ab + b^2) \cdot (a + b)$
$(a + b)^3 = a^3 + a^2b + 2a^2b + 2ab^2 + ab^2 + b^3$

$\boldsymbol{(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3}$

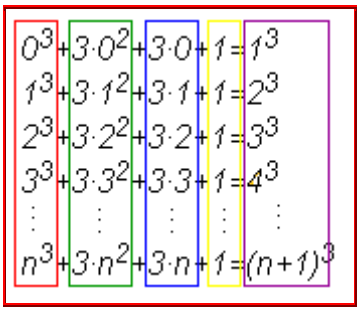
Sabendo esta fórmula, vamos aplica-la em $\boldsymbol{(p + 1)^3}$.

$(p + 1)^3 = p^3 + 3p^2 \cdot 1 + 3p \cdot 1^2 + 1^3$
$\mathbf{(p + 1)^3 = p^3 + 3 \cdot p^2 + 3 \cdot p + 1}$

Agora vamos substituir nesta fórmula o valor de *"p"* pelos números naturais, a partir de 0 até um valor *"n"*.

$p=0 \Rightarrow (0+1)^3 = 0^3+3\cdot 0^2+3\cdot 0+1 = 1^3$
$p=1 \Rightarrow (1+1)^3 = 1^3+3\cdot 1^2+3\cdot 1+1 = 2^3$
$p=2 \Rightarrow (2+1)^3 = 2^3+3\cdot 2^2+3\cdot 2+1 = 3^3$
$p=3 \Rightarrow (3+1)^3 = 3^3+3\cdot 3^2+3\cdot 3+1 = 4^3$
... ...
$p=n \Rightarrow (n+1)^3 = n^3+3\cdot n^2+3\cdot n+1=(n+1)^3$

Agora vamos trabalhar em cima da coluna destacada. Veja o gráfico abaixo:



Veja que separamos cada grupo de parcelas semelhantes das equações com blocos de cores diferentes. Vamos somar todas as equações. Como a soma é comutativa, ou seja, não importa a ordem das parcelas que a soma é a mesma, vamos somar primeiro os termos semelhantes do grupo vermelho, depois do verde e assim sucessivamente:

$0^3+1^3+2^3+3^3+...+n^3$ O *zero* ao cubo é *zero*, portanto não conta
$\mathbf{1^3+2^3+3^3+...+n^3}$

$3\cdot 0^2+3\cdot 1^2+3\cdot 2^2+3\cdot 3^2+...+3\cdot n^2$ Colocando o *3* em evidência e tirando o *zero* (pois *zero* não conta)
$\mathbf{3\cdot(1^2+2^2+3^2+...+n^2)}$ Olha a soma aí

$3\cdot 0+3\cdot 1+3\cdot 2+...+3\cdot n$ Colocando o *3* em evidência e tirando o *zero*
$\mathbf{3\cdot(1+2+3+...+n)}$

$1+1+1+...+1$ O algarismo *1* aparece *(n+1)* vezes, portanto esta soma vale:
$\mathbf{(n+1)}$

$\mathbf{1^3+2^3+3^3+...+n^3+(n+1)^3}$

Agora que sabemos quanto vale cada bloco, vamos colocá-los na mesma ordem de onde tiramos. A ordem é esta:

Portanto, substituindo as cores pelos seus valores, temos:

$$1^3+2^3+...+n^3 \;+\; 3\cdot(1^2+2^2+...+n^2) \;+\; 3\cdot(1+2+...+n) \;+\; (n+1) \;=\; 1^3+...+n^3+(n+1)^3$$

O que estamos procurando é a soma dos quadrados (e ela já esta na equação acima, no bloco verde) portanto, vamos chamá-la de "*S*" (para economizar tempo).

$$1^3+2^3+...+n^3 \;+\; 3\cdot S \;+\; 3\cdot(1+2+...+n) \;+\; (n+1) \;=\; 1^3+2^3+...+n^3+(n+1)^3$$

Todos os termos ao cubo do bloco vermelho irão se cancelar com os termos ao cubo do bloco roxo (pois um está de um lado da equação e outro do outro lado), no momento temos:

$$0 \;+\; 3\cdot S \;+\; 3\cdot(1+2+...+n) \;+\; (n+1) \;=\; (n+1)^3$$

O bloco vermelho pode ser retirado.

No bloco azul temos dentro do parênteses a soma dos "*n*" primeiros número naturais, que seguem como uma PA de razão ***r=1*** , primeiro termo $a_1=1$ e último termo $a_n=n$ e o número de termos é o próprio ***"n"***. Utilizando a fórmula da soma "*n*" primeiros termos de uma PA, temos:

$$Sn = \frac{(a_1 + a_n)n}{2} \qquad Sn = \frac{(1+n)n}{2}$$

Agora podemos substituir no bloco azul o valor de dentro do parênteses pelo valor que achamos:

$$3\cdot S \;+\; 3\cdot(1+n)\cdot n/2 \;+\; (n+1) \;=\; (n+1)^3$$

Não precisamos mais dos blocos:

$$3S + \frac{3(1+n)n}{2} + (n+1) = (n+1)^3$$

Vamos multiplicar os dois lados da equação por 2 (para tirar a fração que está enchendo o saco):

$$6S+3(1+n)n+2(n+1)=2(n+1)^3$$

Como é o *"S"* que queremos, vamos isolá-lo:

$$6S=-3(n+1)n-2(n+1)+2(n+1)^3$$

Podemos colocar o *(n+1)* em evidência no lado direito da equação

$$6S=(n+1)\cdot[-3n-2+2(n+1)^2]$$

Vamos desenvolver o quadrado do lado direito e efetuar alguns cálculos:

$$6S=(n+1)\cdot[-3n-2+2(n^2+2n+1)]$$
$$6S=(n+1)\cdot(-3n-2+2n^2+4n+2)$$
$$6S=(n+1)\cdot(2n^2+n)$$
$$6S=(n+1)\cdot n(2n+1)$$

Agora podemos "passar" o *6* para o outro lado e isolar nosso *"S"* .

$$S = \frac{(n+1)n(2n+1)}{6}$$

Esta é a fórmula da soma dos quadrados dos "n" primeiros números naturais não nulos

REFERÊNCIAS BIBLIOGRÁFICAS

Plinio, José. Introdução à Teoria dos números. Campinas – SP, 1998.

Sites:

http://www.matematica.tv/estudo_matematica_online/curiosidades_matematica

http://fatosmatematicos.blogspot.com/2011/02