MATEMÁTICA UNIVERSITÁRIA
n$^{\underline{o}}$ 41 – Dezembro/2006 – pp. 1–10

Triângulos retângulos com lados inteiros: Procurando as hipotenusas

José F. Andrade

1 Introdução

O objetivo principal deste artigo é determinar os números inteiros que são hipotenusa de um triângulo retângulo cujos catetos são também números inteiros. Mostraremos que existe um triângulo retângulo com hipotenusa z se e somente se z é divisível por um número primo que deixa resto 1 quando dividido por 4.

Mostraremos também como encontrar todos os tais triângulos retângulos e quantos são eles, em função da decomposição de z em fatores primos.

O estudo dos triângulos retângulos cujos lados são números inteiros — e que de agora em diante passaremos a chamar de triângulos retângulos, salvo nos enunciados dos resultados — desperta um grande interesse. Por exemplo, os artigos listados nas referências tratam de questões relacionados ao tema. No artigo [7] são determinados os chamados ternos pitagóricos, i. e. os ternos $x, y, z \in \mathbb{N}$ tais que $x^2 + y^2 = z^2$, em função de dois parâmetros u, v. No mesmo artigo artigo mostra-se também que se $x \geq 3$, existe um triângulo retângulo com cateto x e como se determinar todos os triângulos retângulos com este valor fixado para um de seus catetos. Porém não encontramos na literatura a determinação dos triângulos retângulos com um valor fixado para sua hipotenusa.

Para $z \leq 25$ é fácil ver que apenas 5, 10, 13, 15, 17, 20 e 25 são hipotenusa de um triângulo retângulo. Com efeito, temos $3^2 + 4^2 = 5^2$, $6^2 + 8^2 = 10^2$, $5^2 + 12^2 = 13^2$, $9^2 + 12^2 = 15^2$, $8^2 + 15^2 = 17^2$, $12^2 + 16^2 = 20^2$, $15^2 + 20^2 = 25^2$, $7^2 + 24^2 = 25^2$ e, para os demais números inteiros menores que 25, testes simples mostram que não é possível encontrar um triângulo retângulo com estes valores para sua hipotenusa. Note que 25 é hipotenusa de dois triângulos retângulos não semelhantes.

Na determinação das soluções de $x^2 + y^2 = z^2$ escrevemos x^2 como produto de dois números inteiros: $x^2 = (z + y)(z - y)$ e a partir desta decomposição é que encontramos todos os triângulos retângulos com um cateto determinado. Para determinarmos os inteiros z que são hipotenusa de um triângulo retângulo, não é possível escrever z^2 como produto de dois números inteiros em função de x e y, mas de modo similar ao da resolução da equação de grau 2 com discriminante negativo, no qual passamos para o conjunto dos números complexos para encontrar suas raízes, é possível e conveniente passar para o conjunto dos números complexos para escrever z^2 como produto de dois fatores que dependam de x e y: $z^2 = x^2 + y^2 = (x + yi)(x - yi)$. Como $x, y \in \mathbb{Z}$, nossos fatores pertencem ao anel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$, conhecido como anel dos inteiros de Gauss, o qual tem propriedades muito boas. No livro [4], são usadas propriedades de $\mathbb{Z}[i]$ para se determinar, em função de dois parâmetros, todos os ternos pitagóricos x, y, z, com x e y primos entre si. Neste trabalho utilizaremos a decomposição de z em fatores irredutíveis de $\mathbb{Z}[i]$ para mostrarmos nossos resultados. No próximo parágrafo apresentaremos, sem demonstrações, as propriedades de $\mathbb{Z}[i]$ que precisamos. O parágrafo 3 será dedicado aos nossos resultados, e o último a três exemplos.

2 Os inteiros de Gauss

Lembramos que num anel comutativo com unidade A, um elemento $u \in A$ é inversível se existe um elemento $u' \in A$ tal que $uu' = 1$. Um elemento não nulo e não inversível r é irredutível se sempre que escrevermos $r = st$ então s é inversível ou t é inversível. Dois elementos irredutíveis r_1 e r_2 são associados se $r_1 = ur_2$ com u inversível. Se $\alpha = a + bi \in \mathbb{Z}[i]$ definimos a norma de α como sendo o número natural $N(\alpha) = |a+bi|^2 = a^2 + b^2$. É claro que $N(\alpha) = N(\overline{\alpha}) = N(\overline{a + bi}) = N(a - bi)$. Segue das propriedades do módulo de um número complexo que se $\alpha, \beta \in \mathbb{Z}[i]$ então $N(\alpha\beta) = N(\alpha)N(\beta)$.

Os elementos inversíveis de $\mathbb{Z}[i]$ são exatamente 1, -1, i e $-i$. Os demais elementos não nulos de $\mathbb{Z}[i]$ não são inversíveis em $\mathbb{Z}[i]$ porque os seus inversos em $\mathbb{C}$ não pertencem a $\mathbb{Z}[i]$. Enunciaremos agora três teoremas envolvendo os elementos irredutíveis de $\mathbb{Z}[i]$, cujas demonstrações são encontradas em [4].

Teorema 2.1 (Fermat). *Seja $p \in \mathbb{N}$ um número primo. São equivalentes:*

1. $p = 2$ *ou* $p \equiv 1 \pmod 4$.
2. p *não é irredutível em* $\mathbb{Z}[i]$.
3. p *é soma de dois quadrados.*

Teorema 2.2. *Os elementos irredutíveis de $\mathbb{Z}[i]$ são:*

1. $\pm p$, $\pm pi$ *com p primo em $\mathbb{N}$ tal que* $p \equiv 3 \pmod 4$.
2. $a + bi$ *com* $a^2 + b^2 = p$, *p primo em $\mathbb{N}$.*

Teorema 2.3. *Todo elemento não nulo e não inversível de $\mathbb{Z}[i]$ se escreve de maneira única — a menos de elementos inversíveis — como produto de elementos irredutíveis.*

Observações:

1. O último teorema é semelhante ao Teorema Fundamental da Aritmética.
2. A maneira de escrever um número primo como soma de dois quadrados $p = a^2 + b^2$ com $a \geq b > 0$ é única. Veja [4].

3. Como $1+i=-i(1-i)$, $1+i$ e $1-i$ são associados. Usando a última igualdade, temos $2=1^2+1^2=(1+i)(1-i)=-i(1+i)^2$.

4. Quando $p \equiv 1 \pmod 4$, escrevemos $p=a^2+b^2$. Como p é ímpar, então a e b têm paridade distinta e podemos supor $a>b>0$. Neste caso, verificamos que $a+bi$ e $a-bi$ não são associados.

5. Se cada um dos inteiros $r,s \in N$ é soma de dois quadrados, então rs também é. Com efeito, supondo $r=a^2+b^2$ e $s=c^2+d^2$, temos $rs=(a^2+b^2)(c^2+d^2)=N(a+bi)N(c+di)=N((a+bi)(c+di))=N(ac-bd+(ad+bc)i)=(ac-bd)^2+(ad+bc)^2$.

3 A hipotenusa

Começamos com o nosso resultado principal, que estabelece quais os inteiros que são hipotenusa de um triângulo retângulo.

Teorema 3.1. *Seja z um número inteiro positivo. Então existe um triângulo retângulo com hipotenusa z e catetos números inteiros se e somente se z é divisível por um número primo p tal que $p \equiv 1 \pmod 4$, i. e. p deixa resto 1 quando dividido por 4.*

Demonstração: Seja p um número primo tal que $z=pz_1$ com $p \equiv 1 \pmod 4$. Usando o Teorema 2.1, temos que $p=a^2+b^2=N(a+bi)$. Logo $p^2=N(a+bi)^2=N((a+bi)^2)=N(a^2-b^2+2abi)=(a^2-b^2)^2+(2ab)^2$. Pela observação acima, como $a>b>0$, temos $a^2-b^2>0$ e $2ab>0$. Logo $z^2=p^2z_1^2=((a-b)^2+(2ab)^2))z_1^2=((a-b)z_1)^2+(2abz_1)^2$.

Reciprocamente, suponha que z não seja divisível por nenhum primo tal que $p \equiv 1 \pmod 4$ e que $x^2+y^2=z^2$ com $x,y \in \mathbb{N}$, $x,y>0$. Neste caso a decomposição de z em fatores primos é da forma $z=2^v q_1^{s_1} \dots q_l^{s_l}$ com $q_j \equiv 3 \pmod 4$. Como $z^2=(x+yi)(x-yi)$ e $N(x+yi)=N(x-yi)$, então tomando a decomposição de z^2 em elementos irredutíveis de $\mathbb{Z}[i]$ (Teorema 2.3) vemos que $x+yi=u(1+i)^{2v}q_1^{s_1}\dots q_l^{s_l}=u(2i)^v q_1^{s_1}\dots q_l^{s_l}$ com u inversível em $\mathbb{Z}[i]$. Assim, $x+yi$ é um número real ou um número imaginário puro, acarretando respectivamente, $y=0$ ou $x=0$, uma contradição. $\square$

É fácil ver que, como p é primo, a e b são primos entre si, e consequentemente $a^2 - b^2$ e $2ab$ são também primos entre si. Este é um caso particular do lema a seguir.

Lema 3.1. *Sejam $p_1, \ldots, p_k$ números primos distintos tais que $p_j \equiv 1 \pmod 4$. Suponha que $p_j = a_j^2 + b_j^2$ com $a_j, b_j \in \mathbb{Z}$ e seja $\alpha = x + yi = (a_1 + b_1 i)^{n_1}(a_2 + b_2 i)^{n_2} \ldots (a_k + b_k i)^{n_k}$. Então x e y são primos entre si (em $\mathbb{Z}$).*

Demonstração: Primeiro observamos que, pelo Teorema 2.1, podemos escrever $p_j = a_j^2 + b_j^2$. Decorre dos Teoremas 2.2 e 2.3 que $(a_1 + b_1 i)^{n_1}(a_2 + b_2 i)^{n_2} \ldots (a_k + b_k i)^{n_k}$ é a decomposição (única) de α em elementos irredutíveis de $\mathbb{Z}[i]$. Então x e y não podem ser ambos divisíveis por 2 ou por um primo q tal que $q \equiv 3 \pmod 4$ porque $1 + i$ e q não aparecem na decomposição de α e x e y não podem ser ambos divisíveis por um primo p tal que $p \equiv 1 \pmod 4$ porque para cada $a + bi$ que aparece na decomposição de α, o seu conjugado complexo não aparece nesta decomposição. Concluímos então que x e y são primos entre si. $\square$

Vamos agora ver como encontrar todos os triângulos retângulos com hipotenusa z.

Seja $z = z_1 z_2$, onde todos os primos p_j que dividem z_1 são tais que $p_j \equiv 1 \pmod 4$ e todos aqueles q_j que dividem z_2 são tais que $q_j = 2$ ou $q_j \equiv 3 \pmod 4$. Vimos na demonstração do Teorema 3.1, que como consequência dos Teoremas 2.2 e 2.3, x e y têm que ser múltiplos de z_2. Portanto, o que realmente importa na determinação dos triângulos retângulos com hipotenusa z são os primos p_j que dividem z_1. Seja pois d um divisor de z_1, $z = dz_3$. Vamos obter x_1, y_1 primos entre si tais que $x_1^2 + y_1^2 = d^2$ e tomando $x = x_1 z_3$ e $y = y_1 z_3$ teremos $x^2 + y^2 = z^2$. Podemos então supor que $z = p_1^{t_1} p_2^{t_2} \ldots p_k^{t_k}$ com $p_j \equiv 1 \pmod 4$ e vamos encontrar x e y primos entre si tais que $x^2 + y^2 = z^2$.

Para facilitar a compreensão, vamos tratar inicialmente do caso caso particular $k = 1$. Suponha então que $z = p^t$ com $p = a^2 + b^2 = (a + bi)(a - bi)$. Então $z^2 = N(p^t) = N((a + bi)^t)N((a - bi)^t) = N((a + bi)^t)N((a + bi)^t) = N((a + bi)^{2t})$. Assim, se $(a + bi)^{2t} = x + yi$ então

$x^2+y^2=z^2$ e, pelo Lema 3.1, x e y são primos entre si. No caso de x ou y ser negativo, trocamos o sinal para obter o valor da cateto. Podemos escolher $z^2 = N(p^t) = N((a+bi)^t)N((a-bi)^t) = N((a-bi)^t)N((a-bi)^t) = N((a-bi)^{2t})$. Mas, por propriedade da conjugação complexa $(a-bi)^{2t} = x - yi$, e portanto obtemos o mesmo triângulo retângulo. Porém, não podemos trocar alguns dos fatores $a+bi$ por $a-bi$ sem trocar todos eles, porque neste caso os inteiros x e y são ambos divisíveis por p. Ainda mais, devido à decomposição única dos elementos de $\mathbb{Z}[i]$ em produto de elementos irredutíveis, não é possível encontrar outro triângulo retângulo não semelhante a este com os catetos primos entre si. Consequentemente, neste caso temos apenas um triângulo retângulo com hipotenusa z e catetos x e y primos entre si.

Suponha agora que $k > 1$, $p_j = a_j^2 + b_j^2 = (a_j + b_j i)(a_j - b_j i)$ e $\alpha_j = a_j + b_j i$. Seja $\alpha = x + yi$ um dos números complexos $\beta_1\beta_2\ldots\beta_k$ onde $\beta_j = \alpha_j^{2t_j}$ ou $\beta_j = \overline{\alpha_j}^{2t_j}$. Temos que $N(\alpha) = z^2$ i. e. $x^2+y^2=z^2$ e pelo Lema 3.1, x e y são primos entre si. Vamos agora contar quantos são os tais triângulos. Existem 2^k possibilidades para a escolha de α, mas dois a dois, um é o conjugado complexo do outro, gerando o mesmo um triângulo retângulo. Obtivemos portanto, $\dfrac{2^k}{2} = 2^{k-1}$ triângulos retângulos não semelhantes com catetos x e y primos entre si e tais que $x^2+y^2=z^2$. Como no caso $k=1$, não é possível encontrar um outro triângulo retângulo não semelhante a estes já obtidos com os catetos primos entre si.

Seja $z = p_1^{t_1}p_2^{t_2}\ldots p_k^{t_k}$ com $p_j \equiv 1 \pmod 4$ e vamos contar quantos são os triângulos retângulos com hipotenusa z.

Tomemos um divisor $d = p_{j_1}^{s_{j_1}}p_{j_2}^{s_{j_2}}\ldots p_{j_m}^{s_{j_m}}$ de z com expoentes positivos, $z = dz_1$. Para este divisor obtemos 2^{m-1} triângulos retângulos com catetos primos entre si e hipotenusa d. Multiplicando os catetos e a hipotenusa por z_1, obtemos 2^{m-1} triângulos retângulos com hipotenusa z. Com estes primos $p_{j_1}, p_{j_2}, \ldots, p_{j_m}$ são exatamente $t_{j_1}t_{j_2}\ldots t_{j_m}$ divisores. Variando $j_1, j_2, \ldots, j_m$ com $1 \leq j_1 < j_2 < \ldots < j_m \leq k$, vemos que z possui

$$\sum_{1\leq j_1<j_2<\ldots<j_m\leq k} t_{j_1}t_{j_2}\ldots t_{j_m}$$

divisores com exatamente m primos distintos. Finalmente fazendo m variar de 1 a k, acabamos de demonstrar o seguinte teorema:

Teorema 3.2. *Seja $z = p_1^{t_1}p_2^{t_2}\ldots p_k^{t_k}w$. Suponha que os números primos p_j são distintos, que $p_j \equiv 1 \pmod 4$ e que w não é divisível por nenhum primo p tal que $p \equiv 1 \pmod 4$. Então existem*

$$\sum_{m=1}^{k} 2^{m-1}(\sum_{1\leq j_1<j_2<\ldots<j_m\leq k} t_{j_1}t_{j_2}\ldots t_{j_m})$$

triângulos retângulos não semelhantes com hipotenusa z e catetos números inteiros.

No caso particular em que $z = p_1p_2\ldots p_kw$, a soma do Teorema 3.2 adquire uma forma interessante.

Corolário 3.1. *Suponha que $z = p_1p_2\ldots p_kw$ e que as demais condições do Teorema 3.2 são satisfeitas. Então existem*

$$\sum_{m=1}^{k} 2^{m-1}\begin{pmatrix} k \\ m \end{pmatrix}$$

triângulos retângulos não semelhantes com hipotenusa z e catetos números inteiros.

4 Exemplos

Exemplo 4.1. $z = 325 = 5^2 \times 13$

Primeiro observamos que 5 e 13 deixam resto 1 quando divididos por 4.

São 2 divisores com os primos 5 e 13 e para cada um deles temos $2^{2-1} = 2$ triângulos retângulos. São 2 divisores com o primo 5 e um com o primo 13 e para cada um deles temos $2^{1-1} = 1$ triângulo retângulo.

No total são 7 triângulos retângulos não semelhantes com hipotenusa 325. Vamos determiná-los:

Como $5 = 2^2 + 1^2 = (2+1)(2-i)$ e $13 = 3^2 + 2^2 = (3+2i)(3-2i)$, sejam

$$\begin{array}{rcccl}
\alpha_1 = & (2+i)^4(3+2i)^2 & = (-7+24i)(5+12i) & = & -323+36i, \\
\alpha_2 = & (2+i)^4(3-2i)^2 & = (-7+24i)(5-12i) & = & 253+204i, \\
\alpha_3 = & 5(2+i)^2(3+2i)^2 & = 5(3+4i)(5+12i) & = & -165+280i, \\
\alpha_4 = & 5(2+i)^2(3-2i)^2 & = 5(3+4i)(5-12i) & = & 315+80i, \\
\alpha_5 = & 13(2+i)^4 & = 13(-7+24i) & = & -91+312i, \\
\alpha_6 = & 25(3+2i)^2 & = 25(5+12i) & = & 125+300i, \\
\alpha_7 = & 65(2+i)^2 & = 65(3+4i) & = & 195+260i.
\end{array}$$

Como $N(\alpha_j) = 325^2$, temos então que

$$\begin{array}{rcrcl}
323^2 & + & 36^2 & = & 325^2, \\
253^2 & + & 204^2 & = & 325^2, \\
165^2 & + & 280^2 & = & 325^2, \\
315^2 & + & 80^2 & = & 325^2, \\
91^2 & + & 312^2 & = & 325^2, \\
125^2 & + & 300^2 & = & 325^2, \\
195^2 & + & 260^2 & = & 325^2,
\end{array}$$

e encontramos os 7 triângulos retângulos cujos lados são números inteiros e com hipotenusa 325.

Exemplo 4.2. $z = 359.125 = 5^3 \times 13^2 \times 17$

Com a ajuda de um *software* matemático, o leitor disciplinado encontrará os $1 \times (3+2+1) + 2 \times (3 \times 2 + 3 \times 1 + 2 \times 1) + 4 \times (3 \times 2 \times 1) = 52$ triângulos retângulos não semelhantes com hipotenusa 359.125.

Exemplo 4.3. $z = 32.045 = 5 \times 13 \times 17 \times 29$

São 8 triângulos retângulos com catetos x e y primos entre si. Com efeito, sejam

$$
\begin{array}{lclcrcl}
\alpha_1 & = & (2+i)^2(3+2i)^2(4+i)^2(5+2i)^2 & = & -31323 & - & 6764i, \\
\alpha_2 & = & (2+i)^2(3+2i)^2(4+i)^2(5-2i)^2 & = & -8283 & + & 30956i, \\
\alpha_3 & = & (2+i)^2(3+2i)^2(4-i)^2(5+2i)^2 & = & -23067 & + & 22244i, \\
\alpha_4 & = & (2+i)^2(3+2i)^2(4-i)^2(5-2i)^2 & = & 21093 & + & 24124i, \\
\alpha_5 & = & (2+i)^2(3-2i)^2(4+i)^2(5+2i)^2 & = & 17253 & + & 27004i, \\
\alpha_6 & = & (2+i)^2(3-2i)^2(4+i)^2(5-2i)^2 & = & 27813 & - & 15916i, \\
\alpha_7 & = & (2+i)^2(3-2i)^2(4-i)^2(5+2i)^2 & = & 32037 & + & 716i, \\
\alpha_8 & = & (2+i)^2(3-2i)^2(4-i)^2(5-2i)^2 & = & 2277 & - & 31964i.
\end{array}
$$

Como $N(\alpha_j) = 32045^2$, temos então que

$$
\begin{array}{rcccl}
31323^2 & + & 6764^2 & = & 32045^2, \\
8283^2 & + & 30956^2 & = & 32045^2, \\
23067^2 & + & 22244^2 & = & 32045^2, \\
21093^2 & + & 24124^2 & = & 32045^2, \\
17253^2 & + & 27004^2 & = & 32045^2, \\
27813^2 & + & 15916^2 & = & 32045^2, \\
32037^2 & + & 716^2 & = & 32045^2, \\
2277^2 & + & 31964^2 & = & 32045^2.
\end{array}
$$

Referências Bibliográficas

[1] Alperin, Roger, The modular tree of Pythagoras, Amer. Math. Monthly **112** (2005) 807–816.

[2] Cross, James, Primitive Pythagorean triples of Gaussian integers, Math. Mag. **59** (1986) 106–110.

[3] Frink, Orrin, Almost Pythagorean triples, Math. Mag. **60** (1987) 234–236.

[4] Garcia, Arnaldo e Lequain, Yves, elementos de álgebra, Projeto Euclides, IMPA, 2002.

[5] Markov, Lubomir, Pythagorean triples and the problem $A = mP$ for triangles, Math. Mag. **79** (2006) 114–121.

[6] McCullough, Darryl, Height and excess of Pythagorean triples, Math. Mag. **78** (2005) 26–44.

[7] Rothbart, Andrea e Paulsell, Bruce, Números Pitagóricos: uma fórmula de fácil dedução e algumas aplicações geométricas, Revista do Professor de Matemática **7** (1985) 49–51.

[8] Scheffold, Egon, Pythagorean triples of polygonal numbers, Amer. Math. Monthly **108** (2001) 257–258.

José Fernandes Silva Andrade

Instituto de Matemática – UFBa

Av. Ademar de Barros s/n

40.170-110 Salvador-Bahia

`e-mail: jandrade@ufba.br`