V Bienal da SBM
Sociedade Brasileira de Matemática
UFPB - Universidade Federal da Paraíba
18 a 22 de outubro de 2010

PROPRIEDADES DO GRUPO DOS TERNOS PITAGÓRICOS

Thais Silva do Nascimento * & Martinho da Costa Araujo †

1 Introdução

Um tema muito antigo, mas que ainda desperta muito interesse são os Ternos Pitagóricos (**TP**). Existem vários modelos de se produzir (**TP**). Em ([**2,3**]) é apresentada uma maneira de associar um (**TP**) a um elemento de um grupo $\mathbb{P}$. Este trabalho tem como objetivo apresentar algumas propriedade do grupo $\mathbb{P}$.

Uma identidade famosa atribuida a Diophantus (325 - 409 A.D.) mostra que dados dois inteiros, que podem ser escritos como a soma de dois quadrados, o seu produto também é soma de dois quadrados, ver([**1**]), ou seja,

$$(a^2+b^2)(x^2+y^2) = (ax-by)^2 + (ay+bx)^2 \tag{1.1}$$

De fato,

$$\begin{aligned}(a^2+b^2)(x^2+y^2) &= a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2\\ (a^2+b^2)(x^2+y^2) &= (a^2x^2 - 2axby + b^2y^2) + (a^2y^2 + 2axby + b^2x^2)\\ (a^2+b^2)(x^2+y^2) &= (ax-by)^2 + (ay+bx)^2.\end{aligned}$$

Fazendo $a^2+b^2=c^2$ e $x^2+y^2=z^2$ com $c, z \in \mathbb{Z}$, esta identidade sugere uma maneira de construir um terno pitagórico (**TP**) a partir de outros dois, ou seja, uma nova tripla onde suas coordenadas satisfazem o Teorema de Pitágoras. Observe que se os ternos (a,b,c) e (x,y,z) são pitagóricos, então

$$(ax-by, ay+bx, cz)$$

também é pitagórico.

Assim, se (a,b,c) é um **TP**, dizemos que ele representa um Triângulo Pitagórico, ou seja, triângulo retângulo com catetos a, b e hipotenusa c. Deste modo, podemos definir uma operação $\oplus$, a qual chamaremos de adição, que associa a dois ternos pitagóricos (a,b,c) e (x,y,z) o novo terno pitagórico $(ax-by,\ ay+bx,\ cz)$.

Um *Terno Pitagórico Pimitivo* (ou *Triângulo Pitagórico Primitivo*) é um **TP** (a,b,c), com $a,b,c \in \mathbb{Z}$ e mdc(a,b,c) = 1. Ao invés de considerar o conjunto de todos os ternos pitagóricos, iremos considerar apenas o conjunto $\mathbb{P} = \{(a,b,c) : a,b,c \in \mathbb{Z}, a^2+b^2=c^2 \quad \text{e} \quad mdc(a,b,c)=1\}$, onde terno (ka,kb,kc) será representado pelo seu primitivo (a,b,c). Assim, vamos definir em $\mathbb{P}$ a operação $\oplus$, chamada de adição de dois ternos pitagóricos por:

$$(a,b,c) \oplus (x,y,z) = (ax-by, ay+bx, cz). \tag{1.2}$$

*Universidade Federal de Mato Grosso , UFMT, MT, Brasil, thaisnascimento.cv@gmail.com
†Universidade Federal de Mato Grosso , Dpto. de Matemática , MT, Brasil, martinho@ufmt.br

Vamos assumir que $ax - by > 0$ e mostraremos que o conjunto $\mathbb{P}$ com esta operação de adição é um grupo. Para facilitar a verificação das propriedades de $\mathbb{P}$ iremos fazer uma identificação de uma tripla em $\mathbb{P}$ com pontos no círculo unitário no plano complexo, ou seja, mostraremos que $\mathbb{P}$ é isomorfo a um subgrupo do círculo unitário $\mathbf{S}^1$, o que nos levará a uma representação geométrica dos elementos de $\mathbb{P}$. Em seguida, verificaremos algumas propriedades deste grupo constatando que o mesmo é um grupo abeliano gerado pelo conjunto de triângulos que tem como hipotenusa um primo da forma $4n + 1$ e que isto nos diz quantos triângulos retângulos tem a mesma hipotenusa, conforme ([**2,3**]).

2 Algumas propriedades de $\mathbb{P}$

Cada terno pitagórico primitivo (a,b,c) determina um número complexo $z = a+ib$, com módulo $|z| = \sqrt{a^2 + b^2} = c$. Para $z = a+ib$ e $w = x+iy$, podemos escrever (1.1) na forma $|z|\,|w| = |zw|$. O segmento da origem a z intercepta o círculo unitário $\mathbf{S}^1$, no plano complexo, num ponto $e^{i\alpha} = \dfrac{a}{c} + i\dfrac{b}{c}$.

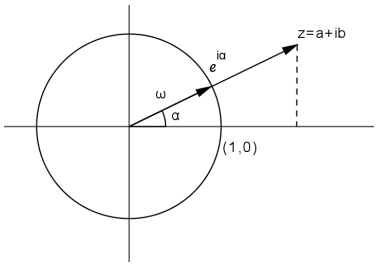

Figura 1: Círculo Unitário $\mathbf{S}^1$ no Plano Complexo

De fato, seja $w = \cos\alpha + i\sin\alpha$ o ponto de interseção entre o círculo unitário e $z = a + ib$. Temos que $w = kz$ e $|w| = 1$, $k \in \mathbb{R}$. Segue daí que $k = \dfrac{1}{c}$, logo $w = e^{i\alpha} = \dfrac{a}{c} + i\dfrac{b}{c}$.

Lema 2.1. *Seja $\mathbf{S}^1$ o círculo unitário no plano complexo, então a função $\phi : \mathbb{P} \to \mathbf{S}^1$ definida por $\phi((a,b,c)) = e^{i\alpha} = \dfrac{a}{c} + i\dfrac{b}{c}$ é um homomorfismo injetor.*

Prova: Sejam (a,b,c) e $(x,y,z) \in \mathbb{P}$, considere $\phi((a,b,c)) = e^{i\alpha} = \dfrac{a}{c} + i\dfrac{b}{c}$ e $\phi((x,y,z)) = e^{i\beta} = \dfrac{x}{z} + i\dfrac{y}{z}$. Então

$$\begin{aligned}
\phi((a,b,c) \oplus (x,y,z)) &= \phi((ax - by, ay + bx, cz)) = \frac{ax - by}{cz} + i\frac{ay + bx}{cz} \\
\phi((a,b,c) \oplus (x,y,z)) &= \left(\frac{a + ib}{c}\right)\left(\frac{x + iy}{z}\right) = e^{i\alpha}e^{i\beta} = \phi((a,b,c))\phi((x,y,z)).
\end{aligned}$$

Logo ϕ é um homomorfismo. Além disso, se $e^{i\alpha} = e^{i\beta}$ então $\dfrac{a}{c} = \dfrac{x}{z}$ e $\dfrac{b}{c} = \dfrac{y}{z} \Rightarrow ay = bx$. Como $mdc(x,y,z) = 1$, existem $r, s \in \mathbb{Z}$ tais que $xr + ys = 1$. Segue daí que $a = x(ar + bs), b = y(ar + bs)$ e $c = z(ar + bs)$. Mas $mdc(a,b,c) = 1$, logo $(a,b,c) = (x,y,z)$. Portanto ϕ é um homomorfismo injetor. $\square$

Deste modo, a soma de ternos pitagóricos em $\mathbb{P}$ corresponde ao produto de números complexos. Visualizando no círculo unitário, temos que a nossa adição em $\mathbb{P}$ corresponde a adição de ângulos em $\mathbf{S}^1$. Segue, diretamente desta correspondência, que a adição definida em (1.2) tem as seguintes propriedades:

- associativa: $[(a,b,c) \oplus (x,y,z)] \oplus (u,v,w) = (e^{i\alpha}e^{i\beta})e^{i\gamma} = e^{i\alpha}(e^{i\beta}e^{i\gamma}) = (a,b,c) \oplus [(x,y,z) \oplus (u,v,w)]$

- comutativa: $(a,b,c) \oplus (x,y,z) = e^{i\alpha}e^{i\beta} = e^{i\beta}e^{i\alpha} = (x,y,z) \oplus (a,b,c)$
- O triângulo degenerado (1,0,1) é o elemento identidade, pois $(a,b,c) \oplus (1,0,1) = e^{i\alpha}e^{i0} = e^{i\alpha} = (a,b,c)$
- Para garantir que $\mathbb{P}$ é fechado para esta soma, precisamos analisar o caso ignorado até agora $ax - by \leq 0$, ou seja, $\gamma = \alpha + \beta \geq \frac{\pi}{2}$. Considere $\gamma = \theta + \frac{\pi}{2}$, com $0 \leq \theta < \frac{\pi}{2}$, então o triângulo $(\cos\gamma, \sin\gamma, 1)$ é congruente ao triângulo $(\cos\theta, \sin\theta, 1)$, que é obtido por uma rotação de $-\frac{\pi}{2}$ em relação a origem.
- Para garantir o inverso em $\mathbb{P}$, sempre que $\gamma = \alpha + \beta \geq \frac{\pi}{2}$ reduziremos o ângulo soma módulo $\frac{\pi}{2}$. Por exemplo, reduzimos o ângulo $\gamma = \frac{\pi}{2}$ módulo $\frac{\pi}{2}$ para 0, que corresponde ao elemento (1,0,1). Segue daí que (a,b,c) e (b,a,c) são inversos um do outro, pois $\gamma = \alpha + \beta = \frac{\pi}{2}$ então $(a,b,c) \oplus (b,a,c) = (1,0,1)$. Note que embora os triângulos (a,b,c) e (b,a,c) sejam congruentes, estamos considerando-os como elementos diferentes em $\mathbb{P}$.

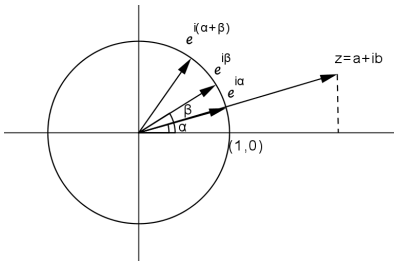

Figura 2: Representação de um complexo sobre $\mathbf{S}^1$

Em resumo, o conjunto $\mathbb{P}$ dos ternos pitagóricos primitivos é um grupo abeliano com a operação de adição definida por :

$$(a,b,c) \oplus (x,y,z) = \begin{cases} (ax - by, ay + bx, cz), & \text{se} \quad ax - by > 0 \\ (ay + bx, ax - by, cz), & \text{se} \quad ax - bt \leq 0. \end{cases}$$

O elemento identidade de $\mathbb{P}$ é o triângulo degenerado (1,0,1) e o inverso aditivo de (a,b,c) é (b,a,c). E o núcleo $\ker(\phi) = \{(a,b,c) : \phi(a,b,c) = 1\} = \{(1,0,1)\}$ o que é equivalente a dizer que ϕ é injetiva.

A construção geométrica do produto de dois complexos dá uma interpretação alternativa da operação do grupo $\mathbb{P}$. Dados $(a,b,c), (x,y,z) \in \mathbb{P}$ podemos multiplicar $v = a + ib$ e $w = x + iy$ geométricamente, para o caso em que $\alpha + \beta \leq \frac{\pi}{2}$, obtendo a soma $(a,b,c) \oplus (x,y,z)$.

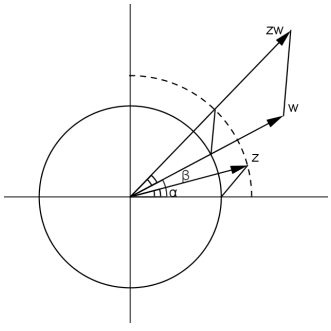

Figura 3: Representação Geométrica da soma de TPP

3 $\mathbb{P}$ é um grupo livre

Para cada (a,b,c) em $\mathbb{P}$, o conjunto $\langle(a,b,c)\rangle = \{n(a,b,c) : n \in \mathbb{Z}\}$, onde

$$n(a,b,c) = \begin{cases} (1,0,1), & \text{se} \quad n = 0 \\ \underbrace{(a,b,c) \oplus \cdots \oplus (a,b,c)}_{n-vezes}, & \text{se} \quad n \in \mathbb{N} = \{1,2,3,....\}. \end{cases}$$

Lembramos que $-n(a,b,c)$ é o inverso de $n(a,b,c)$, e que $\langle(a,b,c)\rangle$ é um subgrupo de $\mathbb{P}$, chamado de subgrupo cíclico gerado por (a,b,c). Vamos mostrar que $\mathbb{P}$ é soma direta de grupos cíclicos infinitos, ou seja, se $\{g_i\}$ é o conjunto de geradores de subgrupos de $\mathbb{P}$, então cada $g \in \mathbb{P}$ é uma combinação linear da forma $n_1 g_{i_1} \oplus \cdots \oplus n_k g_{i_k}$, com g_{i_k} distintos, os coeficientes $n_i \in \mathbb{Z}$ inteiros não nulos e $k \in \mathbb{N}$.

Lema 3.1. *Se $a,b,r,k,s \in \mathbb{Z}$ e p é primo tal que $rsab \not\equiv p^2k \pmod{p^2}$ e $a^2+b^2 \equiv r^2+s^2 \equiv 0 \pmod{p^2}$, então exatamente uma das afirmações é verdadeira:*

$$ra + sb \equiv rb - sa \equiv 0 \pmod{p^2} \quad ou \quad ra - sb \equiv rb + sa \equiv 0 \pmod{p^2}.$$

Prova: Temos que $(ra-sb)(ra+sb) = r^2(a^2+b^2) - b^2(r^2+s^2)$. Mas $a^2+b^2 \equiv r^2+s^2 \equiv 0 \pmod{p^2}$, então $(ra+sb)(ra-sb) \equiv 0 \pmod{p^2}$.

- Se $p|(ra+sb)$ e $p|(ra-sb)$, então $p|2sb$ e $p|2ra$, o que implica que $p^2|2rasb$, contrariando a hipótese de que $rsab \not\equiv p^2k \pmod{p^2}$. Logo $ra+sb \equiv 0 \pmod{p^2}$ ou $ra-sb \equiv 0 \pmod{p^2}$.
- Se $ra+sb \equiv 0 \pmod{p^2}$, então $(ra+sb)^2 \equiv 0 \pmod{p^4}$. Por hipótese $(a^2+b^2)(r^2+s^2) \equiv 0 \pmod{p^4}$ e como $(rb-sa)^2 + (ra+sb)^2 = (a^2+b^2)(r^2+s^2) \equiv 0 \pmod{p^4}$, temos que $(rb-sa)^2 \equiv 0 \pmod{p^4}$, ou seja, $(rb-sa) \equiv 0 \pmod{p^2}$. Portanto, $ra+sb \equiv rb-sa \equiv 0 \pmod{p^2}$. Analogamente, se $ra-sb \equiv 0 \pmod{p^2}$, então $ra-sb \equiv rb+sa \equiv 0 \pmod{p^2}$. □

Proposição 3.1. *O grupo $\mathbb{P}$ dos ternos pitagóricos primitivos é um grupo cíclico infinito, gerado pelo conjunto dos ternos (a,b,p), com p primo, $p \equiv 1 \pmod 4$ e $a > b$.*

Prova: Tome $(r,s,d) \in \mathbb{P}$, $(r,s,d) \neq (1,0,1)$ e consideremos a decomposição em fatores primos de d, ou seja, $d = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$. Nosso objetivo é mostrar que podemos escrever $(r,s,d) = e_1 n_1(a_1,b_1,p_1) \oplus \cdots \oplus e_k n_k(a_k,b_k,p_k)$, onde $a_j > b_j$, $e_j = \pm 1$, $p_j \equiv 1 \pmod 4, 1 \leq j \leq k$. Para isso consideremos as seguintes afirmações, ver([**4**]).

I.) Um terno pitagórico (r,s,d) é unicamente determinado por um par de inteiros positivos relativamente primos (m,n) com $m > n$ e de paridade opostas tal que $r = m^2 - n^2$, $s = 2mn$ e $d = m^2 + n^2$.

II.) Um inteiro positivo primo d e ímpar se escreve como a soma de dois quadrados se, e somente se, $d \equiv 1 \pmod 4$.

Portanto, podemos afirmar que o primo p será a hipotenusa de um triângulo pitgórico primitivivo se, e somente se, $p \equiv 1 \pmod 4$. E esta hipotenusa terá representação única como soma de dois quadrados: $p = m^2 + n^2$. Para $a = m^2 - n^2$, $b = 2mn$, temos que $p^2 = a^2 + b^2$. Assim, se $d = p$, temos duas possibilidades $(r,s,d) = (a,b,p)$ ou $(r,s,d) = (b,a,p) = -(a,b,p)$.

Considere um triângulo (r,s,d), onde $d = pq$, com p,q primos e $p \equiv 1 \pmod 4$. Então existe um único par de inteiros (a,b) com $a > b$ tal que $p^2 = a^2 + b^2$, de modo que as equações

$$(r,s,pq) = (a,b,p) \oplus (x,y,z) \quad \text{e} \quad (r,s,pq) = (-(a,b,p)) \oplus (x,y,z),$$

tem as seguintes soluções

$(x,y,z) = (r,s,pq) \oplus (-(a,b,p)) = (rb - sa, ra + sb, p^2q)$ e $(x,y,z) = (r,s,pq) \oplus (a,b,p) = (ra - sb, rb + sa, p^2q)$.

Desde que $rsab \not\equiv p^2k \bmod p^2$ e $a^2 + b^2 \equiv r^2 + s^2 \equiv 0 \bmod p^2$. Pelo lema, apenas uma das soluções (x,y,z) acontece. Além disso, p^2 é fator comum a todas as coordenadas da tripla (x,y,z). Cancelando p^2 da solução, concluimos que $(x,y,z) = (u,v,q)$, onde $u = \dfrac{rb-sa}{p^2}$, $v = \dfrac{ra+sb}{p^2}$ ou $u = \dfrac{ra-sb}{p^2}$, $v = \dfrac{rb+sa}{p^2}$ são inteiros. Logo

$$(r,s,pq) = (u,v,q) \oplus (a,b,p) \quad \text{ou} \quad (r,s,pq) = (u,v,q) \oplus (-(a,b,p)). \tag{1.3}$$

Agora, basta analizar os seguintes casos:

Caso 1.) Se $p = q$ então $(r,s,p^2) = 2(a,b,p)$ ou $(r,s,p^2) = (1,0,1)$ e $(r,s,p^2) = (1,0,1)$ ou $(r,s,p^2) = -2(a,b,p)$, obtemos dois triângulos.

Caso 2.) Se $p \neq q$ e como q é a hipotenusa do triângulo pitagórico (u,v,q), então existe um único par de inteiros (f,g) com $f > g$ tal que $q^2 = f^2 + g^2$, ou seja, $(u,v,q) = (f,g,q)$ ou $(u,v,q) = (g,f,q) = -(f,g,q)$. Substituindo em (**1.3**), obtemos quatro triângulos

$$(r,s,d) = \begin{cases} (f,g,q) \oplus (a,b,p) \quad \text{ou} \quad (f,g,q) \oplus (-(a,b,p)) \\ (-(f,g,q) \oplus (a,b,p) \quad \text{ou} \quad (-(f,g,q)) \oplus (-(a,b,p)). \end{cases}$$

Para $d = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$, temos um número finito de primos e prosseguindo com este raciocínio, temos que $(r,s,d) = e_1n_1(a_1,b_1,p_1) \oplus \cdots \oplus e_kn_k(a_k,b_k,p_k)$, onde $a_j > b_j$, $e_j = \pm 1$, $p_j \equiv 1 \pmod 4, 1 \leq j \leq k$. Portanto, temos que $\mathbb{P} = \langle (a_k,b_k,p_k) \rangle$, $a_k > b_k$, $p_k \equiv 1 \pmod 4$, p_k um fator primo de d e $k \in \mathbb{N}$. □

Este resultado nos permite concluir que existem 2^k triângulos pitagóricos primitivos com a mesma hipotenusa $d = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$.

Referências

[1] STILLWELL, I. N. - *Elements of Number Theory*, 1nd ed, New York: Springer-Verlag, 2003.

[2] MCCULLOUGH, DARRYL - *Height and Excess of Pythagorean Triples*, Mathematics Magazine, vol 57, 1, January, 1984.

[3] ECKERT, ERNEST J. - *The Group of Primitive Pythagorean Triangles*, Mathematics Magazine, vol 78, 1, Frebuary, 2005.

[4] CHOWDHURY, K. C. - *A First Course In Number Theory*, 1nd ed, Daya Ganj, New-Delhi: Asian Books Pvt. Ltda, 2004.

[5] GARCIA, ARNALDO e LEQUAIN, YVES - *Elementos de Algebra*, 4 ed, Rio de Janeiro: IMPA, 2006.

[6] MAOR, ELI - *Trigonometrics Delights*, Princeton University Press, 2002.

[7] - *divulgamat.ehu.es/weborriak/TestuakOnLine/03-04-lcandres.pdf*, acessado em 19 de maio 2010.

[8] - *http://www2-fs.informatik.uni-tuebingen.de/ borchert/ArithmeticalCircuits/Grosswald.pdf*, acessado em 19 de maio 2010.