MATEMÁTICA UNIVERSITÁRIA
nº.22/23 – junho/dezembro 1997 – pp.18-29

Números congruentes e curvas elíticas

Amílcar Pacheco

Introdução

Um número inteiro $n \geq 1$ é dito um *número congruente* se existir um triângulo retângulo cujos lados sejam números racionais e cuja área seja n. A questão de determinar se um dado número é congruente foi inicialmente estudada pelos gregos sendo posteriormente sistematizada pelos árabes [Dic52, Chapter XVI].

A primeira etapa para determinar se um número n é congruente é obter números racionais x, y e z que sejam lados de um triângulo retângulo, ou seja tais que $x^2+y^2 = z^2$. Uma tripla de inteiros positivos (x, y, z) tais que $x^2 + y^2 = z^2$ é chamada uma *tripla pitagórica*. Para encontrar x, y e z tomamos inteiros $a > b > 0$ e traçamos no plano XOY a reta passando por $(-1, 0)$ com coeficiente angular b/a. Esta reta intersecta o círculo $S^1 = \{(X, Y) \in \mathbb{R}^2 ;\ X^2 + Y^2 = 1\}$ no ponto

$$u = \frac{a^2 - b^2}{a^2 + b^2} \quad \text{e} \quad v = \frac{2ab}{a^2 + b^2}$$

gerando a tripla

$$x = a^2 - b^2\,,\ y = 2ab\,,\ z = a^2 + b^2 \tag{1}$$

O problema de achar números congruentes reduz-se então a achar triplas pitagóricas tais que $n = xy/2$.

Euler mostrou que $n = 7$ é um número congruente. Fermat mostrou que $n = 1$ não é um número congruente. Isto é essencialmente equivalente a provar que não existem soluções inteiras a, b, c para $a^4 + b^4 = c^4$

tais que $abc \neq 0$. Posteriormente obteve-se que $n = 2, 3, 4$ não são números congruentes, mas 5 e 6 o são. Entretanto não havia um critério que pudesse determinar a priori se um dado número é congruente. Nos anos 80 descobriu-se a conexão entre números congruentes e a aritmética das curvas elíticas. Um dos resultados mais importantes é o Teorema de Tunnell [Tun83] que fornece uma condição suficiente para um número ser congruente (para uma introdução a esta perspectiva ver [Kob84, Chapter I]). Tal condição também é necessária, mas para isto é preciso uma hipótese adicional. Sua demonstração envolve a L -série de Hasse-Weil de uma curva elítica, a conjectura de Birch e Swinnerton-Dyer e formas modulares de peso $k/2$, onde $k \in \mathbb{Z}$. O objetivo do presente artigo é mostrar como é obtida esta conexão (ver Teorema 2).

1 Números congruentes

Antes de estendermos a noção de números congruentes a números racionais positivos, lembremos que um inteiro positivo n é dito *livre de quadrados*, se n puder ser escrito da forma $n = \prod_{i=1}^{r} p_i$, onde os p_i's são números primos distintos.

Um número racional positivo n é um *número congruente* se existirem $x, y, z \in \mathbb{Q}$ positivos tais que $x^2 + y^2 = z^2$ e $n = \frac{xy}{2}$. Notemos que existe $s \in \mathbb{Q} - \{0\}$ tal que $s^2 n \in \mathbb{Z}$ é livre de quadrados. A área do triângulo retângulo de lados sx, sy e sz é igual a $s^2 n$. Ou seja $s^2 n$ é um número inteiro congruente. Assim podemos sempre supor que n seja um inteiro positivo livre de quadrados. Seja $\mathbb{Q}^2$ o grupo multiplicativo dos números racionais positivos que são quadrados. O argumento acima mostra que o fato de n ser um número congruente depende apenas de sua classe módulo $\mathbb{Q}^2$ e que nesta classe sempre existe um número inteiro $m \geq 1$ livre de quadrados.

Observemos que 6 é o menor número congruente tal que existe um triângulo retângulo cujos lados têm como comprimento números naturais, a saber, 3, 4 e 5. De fato, o inteiro 5 é o menor número congruente, entretanto 5 é a área do triângulo retângulo de lados $\frac{3}{2}$, $\frac{20}{3}$ e $\frac{41}{6}$.

Uma primeira "receita ingênua" para produzir um número congruente n é utilizar (1) para listar todas as possíveis triplas pitagóricas. Depois para cada tripla calcular a respectiva área e verificar se n ocorre na lista das áreas. É claro que este procedimento está longe de fornecer

um método eficiente. Em geral impomos a restrição $x < y < z$ à tripla pitagórica x, y, z distinguindo-a por exemplo da tripla y, x, z. Dessa forma diminuimos o número de triplas a serem testadas.

Podemos caracterizar de maneira elementar um número congruente da seguinte forma.

Proposição 1 *Seja $n \geq 1$ um número inteiro livre de quadrados. Sejam $x, y, z \in \mathbb{Q}$ tais que $0 < x < y < z$. Então existe uma bijeção entre o conjunto de triângulos retângulos de lados x, y, z e área n e o conjunto de números racionais w tais que*

$$w, w + n, w - n \in \mathbb{Q}^2,$$

dada por

$$(x, y, z) \longmapsto w = \left(\frac{z}{2}\right)^2$$

com inversa

$$w \longmapsto (\sqrt{w+n} - \sqrt{w-n}, \sqrt{w+n} + \sqrt{w-n}, 2\sqrt{w}).$$

Em particular, n é um número congruente se e somente se existir um número racional w tal que

$$w, w + n, w - n \in \mathbb{Q}^2.$$

Prova. Se $x^2 + y^2 = z^2$ e $n = \frac{xy}{2}$, então $(x \pm y)^2 = z^2 \pm 4n$. Logo

$$\left(\frac{x \pm y}{2}\right)^2 = \left(\frac{z}{2}\right)^2 \pm n. \tag{2}$$

Tomando $w = (\frac{z}{2})^2$ temos que $w, w + n, w - n \in \mathbb{Q}^2$.

Reciprocamente, dado w tal que $w, w + n, w - n \in \mathbb{Q}^2$ então $x = \sqrt{w+n} - \sqrt{w-n}$, $y = \sqrt{w+n} + \sqrt{w-n}$ e $z = 2\sqrt{w}$ satisfazem a $0 < x < y < z$, $xy = 2n$ e $x^2 + y^2 = z^2$. □

2 Equações cúbicas

Nesta seção mostramos como associar a um número congruente n uma solução de uma certa equação cúbica.

Seja n um número congruente e $x, y, z \in \mathbb{Q}$ tais que $0 < x < y < z$, $n = \frac{xy}{2}$ e $x^2 + y^2 = z^2$. Por (2) temos que

$$\left(\frac{x^2 - y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^4 - n^2.$$

Em outras palavras, encontramos soluções racionais $u = \frac{z}{2}$ e $v = \frac{x^2-y^2}{4}$ para a equação $u^4 - n^2 = v^2$. Multiplicando ambos os membros desta equação por u^2 obtemos

$$(u^2)^3 - n^2u^2 = (uv)^2.$$

Portanto, $a = u^2$ e $b = uv$ fornece uma solução racional (a, b) para a equação cúbica $\mathcal{Y}^2 = \mathcal{X}^3 - n^2\mathcal{X}$.

Reciprocamente, dada uma solução racional (a, b) da equação cúbica $\mathcal{Y}^2 = \mathcal{X}^3 - n^2\mathcal{X}$, perguntamos se (a, b) provém de um triângulo retângulo como acima. Isto nem sempre é verdade. Primeiro é necessário que $a \in \mathbb{Q}^2$. Além disto o denominador de a tem que ser par. De fato, dada uma tripla pitagórica $x < y < z$, seja s o mmc dos denominadores de x, y e z. Logo $x' = sx$, $y' = sy$, $z' = sz$ são números inteiros primos entre si. Neste caso x' e y' têm paridades distintas, digamos que x' seja ímpar e y' seja par. Em particular z' é ímpar. Portanto $a = (\frac{z}{2})^2 = (\frac{z'}{2s})^2$ tem denominador par. Sejam x_1, y_1 e z_1 os denominadores de x, y e z, respectivamente. Denotamos por $2^{x_1'}$, $2^{y_1'}$ e $2^{z_1'}$ as maiores potências de 2 dividindo x_1, y_1 e z_1. Seja 2^{s_1} a maior potência de 2 dividindo s. Como sx e sz são ímpares e sy é par, concluimos que $s_1 = x_1' = z_1'$ e $s_1 < y_1'$. Estas condições nem sempre são satisfeitas. Por exemplo $((\frac{41}{7})^2, \frac{29520}{7^3})$ é uma solução de $\mathcal{Y}^2 = \mathcal{X}^3 - (31)^2\mathcal{X}$ que não provém de nenhum triângulo retângulo.

Proposição 2 *Seja $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ uma solução de $\mathcal{Y}^2 = \mathcal{X}^3 - n^2\mathcal{X}$ tal que*

$$a \in \mathbb{Q}^2 \text{ com denominador par.}$$

Então, existe um triângulo retângulo de área n e lados $\sqrt{a+n} - \sqrt{a-n}$, $\sqrt{a+n} + \sqrt{a-n}$ e $2\sqrt{a}$.

Prova. Seja $u = \sqrt{a} \in \mathbb{Q}$, $u > 0$ e $v = \frac{b}{u}$. Então $v^2 = \frac{b^2}{a} = a^2 - n^2$. Seja t o denominador de u. Logo os denominadores de v^2 e a^2 são iguais a

t^4, em particular,

$$\left(t^2v, t^2n, t^2a\right)$$

é uma tripla pitagórica com t^2n par e mdc $\left(t^2v, t^2n, t^2a\right) = 1$.

Uma tripla pitagórica x, y e z tal que $\text{mdc}(x, y, z) = 1$ é chamada uma *tripla pitagórica primitiva*. Suponhamos que y seja par, logo x e z são ímpares. Sejam $A, B, C > 0$ números inteiros tais que $y = 2C$, $z + x = 2A$ e $z - x = 2B$. Observemos que $\text{mdc}(A, B) = 1$ e $AB = C^2$. Logo existem inteiros positivos α e β tais que $A = \alpha^2$ e $B = \beta^2$. Em particular, $z = A + B = \alpha^2 + \beta^2$, $x = A - B = \alpha^2 - \beta^2$ e $y = z^2 - x^2 = (2\alpha\beta)^2$. Portanto $y = 2\alpha\beta$.

Aplicando este argumento à tripla $\left(t^2v, t^2n, t^2a\right)$ obtemos que existem inteiros positivos α, β tais que

$$t^2v = \alpha^2 - \beta^2 \quad , \quad t^2n = 2\alpha\beta \quad \text{e} \quad t^2a = \alpha^2 + \beta^2.$$

Consequentemente o triângulo retângulo de lados

$$\left(\frac{2\alpha}{t}, \frac{2\beta}{t}, 2u\right)$$

tem área $\frac{2\alpha\beta}{t^2} = n$. Pela Proposição 1 temos que esta tripla corresponde a $(\frac{2u}{2})^2 = u^2 = a$. Logo existe um triângulo retângulo de lados $\sqrt{a+n} - \sqrt{a-n}$, $\sqrt{a+n} + \sqrt{a-n}$ e $2\sqrt{a}$ de área n . □

3 Curvas Elíticas

A equação cúbica obtida no parágrafo anterior é um exemplo de uma curva algébrica chamada uma curva elítica. A aritmética desta *curva elítica* consiste no estudo dos pontos (a, b) satisfazendo a equação cúbica tais que $a, b \in \mathbb{Q}$. O Teorema de Mordell-Weil afirma justamente que a partir de um número finito de "*pontos geradores*" com coordenadas racionais na curva elítica, utilizando-se retas ligando pontos da curva obtém-se todos os demais pontos com coordenadas racionais. O número de "*pontos geradores de ordem infinita*" é chamado o posto da curva elítica. O Teorema 2 mostra que n é um número congruente se e somente se o posto da curva elítica associada à equa ção cúbica acima é positivo. Para demonstrá-lo desenvolvemos algumas ferramentas nas subseções subsequentes deste parágrafo.

3.1 O Teorema de Mordell-Weil

Uma curva algébrica afim $C \subset \mathbb{C} \times \mathbb{C}$ é definida como o conjunto dos zeros de um polinômio $f(X,Y) \in C[X,Y] - \mathbb{C}$. Seja $d \geq 1$ o grau de f e

$$F(X,Y,Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

O plano projetivo complexo $\mathbb{P}^2_{\mathbb{C}}$ é definido geometricamente como o quociente de $\mathbb{C}^3$ pela relação de equivalência: $(a,b,c) \sim (a',b',c')$ se e somente se existe $\lambda \in \mathbb{C}^*$ tal que $a' = \lambda a$, $b' = \lambda b$ e $c' = \lambda c$. Esta definição se generaliza para um corpo K qualquer. Denotamos por $\mathbb{P}^2_K$ o plano projetivo correspondente.

A curva projetiva definida por F é dada por

$$\mathcal{C}_F = \{(a:b:c) \in \mathbb{P}^2_{\mathbb{C}} : F(a,b,c) = 0\}.$$

Notemos que C é obtida como

$$\{(a,b) \in \mathbb{C} \times \mathbb{C};\ (a:b:1) \in \mathcal{C}_F\}.$$

Dizemos que $\mathcal{C}_F$ é a projetivização de C.

Uma curva algébrica projetiva $\mathcal{C}_F$ é não singular, se

$$\frac{\partial F}{\partial X}(P) \neq 0 \quad \text{ou} \quad \frac{\partial F}{\partial Y}(P) \neq 0 \quad \text{ou} \quad \frac{\partial F}{\partial Z}(P) \neq 0,$$

para todo $P \in \mathcal{C}_F$. O gênero de uma curva não singular é definido por $\frac{(d-1)(d-2)}{2}$. Uma curva elítica é uma curva de gênero 1. Logo ela é definida pelos zeros de um polinômio homogêneo em X, Y e Z de grau 3. Após uma transformação projetiva de coordenadas, podemos supor que a curva elítica $\mathcal{E}$ é dada por $\mathcal{C}_{F_{A,B}}$ onde

$$F_{A,B}(X,Y,Z) = Y^2Z - X^3 - AXZ^2 - BZ^3$$

com $\Delta = -(4A^3 + 27B^2) \neq 0$. O número Δ é chamado o *discriminante da equação*. Seja $\mathcal{O} = (0:1:0) \in \mathcal{E}$.

Um dos fatos mais importantes sobre uma curva elítica é que esta possui uma estrutura de grupo abeliano.

Descrição geométrica. Dados $P, Q \in \mathcal{E}$, seja $l \subset \mathbb{P}^2_{\mathbb{C}}$ a reta passando por P e Q. Uma reta intersecta uma cúbica em 3 pontos, pois pelo

Teorema de Bézout duas curvas algébricas projetivas não singulares de graus m e n intersectam-se em mn pontos contados com as suas respectivas multiplicidades. Denotamos por R o terceiro ponto de $l \cap \mathcal{E}$ e seja $l' \subset \mathbb{P}^2_{\mathbb{C}}$ a reta passando por R e $\mathcal{O}$. Definimos $P \oplus Q$ como o terceiro ponto de $l' \cap \mathcal{E}$. O ponto $\mathcal{O}$ é o elemento neutro desta operação. É fácil verificar que a adição $\oplus$ é associativa e comutativa. A operação $\oplus$ se estende à curva afim E obtida a partir de $\mathcal{E}$ como os zeros em $\mathbb{C} \times \mathbb{C}$ do polinômio $f_{A,B}(X,Y) = Y^2 - X^3 - AX - B$ e será também denotada por $\oplus$. O ponto $(0:1:0)$ fica idenficado com o "*ponto no infinito*" de E.

Descrição algébrica. [SilTat92, Chapter 1, Section 4] Seja $P \in E$, $\ominus P$ seu inverso e $[2]P = P \oplus P$. Denotamos $P = (x_P, y_P), Q = (x_Q, y_Q) \in E$ com $P \neq Q, \ominus Q$, e $P \oplus Q = (x_{P\oplus Q}, y_{P\oplus Q})$. Valem as seguintes fórmulas

$$x_{P\oplus Q} = \mu^2 - x_P - x_Q \quad \text{e} \quad y_{P\oplus Q} = -\mu x_{P\oplus Q} - \nu, \tag{3}$$

onde

$$\mu = \frac{y_Q - y_P}{x_Q - x_P} \quad e \quad \nu = \frac{x_P y_Q - x_Q y_P}{x_Q - x_P}.$$

Em particular, se $x_P, y_P, x_Q, y_Q \in \mathbb{Q}$, então $x_{P\oplus Q}, y_{P\oplus Q} \in \mathbb{Q}$. Seja $[2]P = (x_{[2]P}, y_{[2]P})$. Temos que

$$x_{[2]P} = \frac{x_P^4 - 2Ax_P^2 - 8Bx_P + A^2}{4x_P^3 + 4Ax_P + 4B}. \tag{4}$$

Seja $\mathcal{E}(\mathbb{Q}) = \{(a:b:c) \in \mathcal{E}\,;\ a,b,c \in \mathbb{Q}\}$.

Teorema de Mordell-Weil [SilTat92, Chapter III, Section 5] $\mathcal{E}(\mathbb{Q})$ *é um grupo abeliano finitamente gerado.*

Observação. Seja $\mathcal{E}(\mathbb{Q})_{\text{tor}}$ o subgrupo de $\mathcal{E}(\mathbb{Q})$ dos elementos de ordem finita. Pelo Teoremas de Mordell-Weil e da Decomposição de Grupos Abelianos Finitamente Gerados [GarLeq88, Teorema VI.7] segue que existe um isomorfismo de grupos

$$\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r.$$

Dizemos que r é o *posto algébrico* de $\mathcal{E}$.

3.2 Pontos de ordem 2

Seja $P = (a : b : 1), Q = (a : -b : 1) \in \mathcal{E}$ e $l \subset \mathbb{P}^2_{\mathbb{C}}$ a reta passando por P e Q. Observermos que, neste caso, $\mathcal{O}$ é o terceiro ponto de $l \cap \mathcal{E}$. Consideremos a reta

$$\mathcal{L} = \{(a' : b' : c') \, ; \, c' = 0\}.$$

Esta é a reta tangente a $\mathcal{E}$ em $\mathcal{O}$. Pela descrição geométrica da adição $\oplus$, concluimos que $Q = \ominus P$.

Um ponto P é de ordem 2 se e somente se $P = \ominus P$. Isto significa que $b = 0$. Se γ_1, γ_2 e γ_3 são as 3 raízes distintas de $X^3 + AX + B$, então os pontos de ordem 2 de E são

$$(\gamma_1 : 0 : 1) \quad , \quad (\gamma_2 : 0 : 1) \quad \text{e} \quad (\gamma_3 : 0 : 1).$$

3.3 Reduzindo módulo p

Seja p um número primo, $\mathbb{F}_p$ o corpo finito de p elementos, $\mathbb{P}^2_{\mathbb{F}_p}$ e $\mathbb{P}^2_{\mathbb{Q}}$ os planos projetivos definidos sobre $\mathbb{F}_p$ e $\mathbb{Q}$, respectivamente. Dado $(a : b : c) \in \mathbb{P}^2_{\mathbb{Q}}$ podemos sempre escolher representantes $a_0, b_0, c_0 \in \mathbb{Z}$. Para isto basta multiplicar a, b, c pelo menor múltiplo comum dos denominadores, por exemplo. Além disto podemos fazer esta escolha de tal forma que $\text{mdc}(a_0, b_0, c_0) = 1$. Assim, definimos a aplicação

$$\begin{aligned} \Phi : \mathbb{P}^2_{\mathbb{Q}} &\longrightarrow \mathbb{P}^2_{\mathbb{F}_p} \\ P = (a_0 : b_0 : c_0) &\longmapsto \widetilde{P} = (\widetilde{a}_0 : \widetilde{b}_0 : \widetilde{c}_0). \end{aligned}$$

Proposição 3 *Seja $i \in \{1, 2\}$ e $P_i = (x_i : y_i : z_i) \in \mathbb{P}^2_{\mathbb{Q}}$. A igualdade $\Phi(P_1) = \Phi(P_2)$ ocorre se e somente se p dividir simultaneamente os números $(y_1 z_2 - y_2 z_1)$, $(x_2 z_1 - x_1 z_2)$ e $(x_1 y_2 - x_2 y_1)$.*

Prova. Observemos que $\Phi(P_1) = \Phi(P_2)$ ocorre se e somente se os vetores $(\widetilde{x}_1, \widetilde{y}_1, \widetilde{z}_1)$ e $(\widetilde{x}_2, \widetilde{y}_2, \widetilde{z}_2)$ são $\mathbb{F}_p$-linearmente dependentes, o que equivale à condição acima. □

Seja $n \geq 1$ um número inteiro,

$$F_n(X, Y, Z) = Y^2 Z - X^3 + n^2 X Z^2 \in \mathbb{Z}[X, Y, Z]$$

e $\mathcal{E}_n$ a curva elítica dada por C_{F_n}. Seu discriminante Δ_n é igual a $4n^6$. Seja $p > 2$ um número primo e

$$\widetilde{F}_n(X, Y, Z) = Y^2Z - X^3 + \widetilde{n}^2 X Z^2 \in \mathbb{F}_p[X, Y, Z].$$

a redução de F_n módulo p. Para que $C_{\widetilde{F}_n}$ defina uma curva elítica $\widetilde{\mathcal{E}}_n$ sobre $\mathbb{F}_p$ é necessário e suficiente que $4\widetilde{n}^6 \neq \widetilde{0}$ em $\mathbb{F}_p$. Isto é satisfeito se p não divide n e $p > 2$ (o que estamos supondo). Seja

$$\widetilde{\mathcal{E}}_n(\mathbb{F}_p) = \{(\widetilde{a}_0 : \widetilde{b}_0 : \widetilde{c}_0) \in \mathbb{P}^2_{\mathbb{F}_p} \,;\, (a_0 : b_0 : c_0) \in \mathcal{E}(Q)\}.$$

Neste caso, Φ induz uma aplicação

$$\Phi_n : \mathcal{E}_n(Q) \longrightarrow \widetilde{\mathcal{E}}_n(\mathbb{F}_p).$$

Como já foi observado, as fórmulas (3) e (4) garantem que a adição em $\mathcal{E}_n$ preserva $\mathcal{E}_n(Q)$. A partir destas fórmulas definimos a adiç ão em $\widetilde{\mathcal{E}}_n$. Novamente esta adição preserva $\widetilde{\mathcal{E}}_n(\mathbb{F}_p)$. Além disto, como $p > 2$ então Φ_n é um homomorfismo de grupos.

3.4 Curvas elíticas sobre corpos finitos

Seja $F_{A,B}(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3 \in \mathbb{F}_p[X, Y, Z]$ e $\mathcal{E} = C_{F_{A,B}}$ a curva elítica definida por $F_{A,B}$. O plano projetivo $\mathbb{P}^2_{\mathbb{F}_p}$ é decomposto em dois subconjunto disjuntos:

$$S_1 = \{(a' : b' : c') \in \mathbb{P}^2_{\mathbb{F}_p} \,;\, c' \neq 0\}$$

e

$$S_2 = \{(a' : b' : 0) \in \mathbb{P}^2_{\mathbb{F}_p}\}$$

de cardinalidades p^2 e $p + 1$, respectivamente. Assim, o conjunto

$$\mathcal{E}(\mathbb{F}_p) = \{P = (a' : b' : c') \in \mathbb{P}^2_{\mathbb{F}_p} \,;\, P \in \mathcal{E}\}$$

tem no máximo $p^2 + p + 1$ elementos. O Teorema de Hasse [SilTat92, Chapter IV, Section 1] dá uma cota mais precisa.

Teorema de Hasse $|\#\mathcal{E}(\mathbb{F}_p) - 1 - p| \leq 2p^{1/2}$.

Proposição 4 *Se* $p \equiv 3 \, mod 4$ *então* $\#\widetilde{\mathcal{E}}_n(\mathbb{F}_p) = p + 1$.

Prova. Notemos que $(0:0:1)$, $(\widetilde{n}:0:1)$, $(-\widetilde{n}:0:1)$ e $\mathcal{O}$ são pontos distintos em $\widetilde{\mathcal{E}}_n(\mathbb{F}_p)$. Resta-nos agora contar o número de pares $(x,y) \in \widetilde{E}_n(\mathbb{F}_p)$ tais que $x \neq 0, \pm\widetilde{n}$. Agrupemos estes elementos em $\frac{p-3}{2}$ pares $\{x,-x\}$. Como $p \equiv 3 \bmod 4$ e $f(X) = X^3 - n^2X$ é uma funç ão ímpar, então exatamente um dos dois elementos $f(x)$ e $f(-x) = -f(x)$ é um quadrado módulo p. Em qualquer dos dois casos cada par fornece dois pontos em $\widetilde{E}_n(\mathbb{F}_p)$ dados por $(x, \pm f(x)^{1/2})$ ou $(-x, \pm f(-x)^{1/2})$. Portanto temos $\#\widetilde{\mathcal{E}}_n(\mathbb{F}_p) = 2\frac{p-3}{2} + 4 = p+1$. □

3.5 Pontos de ordem finita

Teorema 1 $\#\mathcal{E}_n\mathbb{Q}_{tor} = 4$.

Prova. O conjunto $\mathcal{E}_n\mathbb{Q}_{\text{tor}}$ possui pelo menos 4 elementos, o elemento neutro $\mathcal{O}$ e os 3 pontos de ordem exatamente 2, $(0:0:1)$, $(n:0:1)$ e $(-n:0:1)$. Suponhamos que $\#\mathcal{E}_n\mathbb{Q}_{\text{tor}} > 4$. Logo existe $Q \in \mathcal{E}_n(Q)$ de ordem $N > 2$. Ou seja N é ímpar ou existe $P \in \mathcal{E}_n(Q)$ de ordem exatamente 4. No primeiro caso seja S o subgrupo de $\mathcal{E}_n(Q)$ gerado por Q. No segundo caso como temos 3 pontos de ordem 2 pelo menos um destes pontos não pertence ao subgrupo gerado por P. Denotemos este ponto por R. Nesta última situação seja S o produto dos subgrupos de $\mathcal{E}_n(Q)$ gerados por P e R. Logo $S \cong (\mathbb{Z}/2Z) \times (\mathbb{Z}/4\mathbb{Z})$. Seja $m = N$ ou 8 e $S = \{P_1, \ldots, P_m\}$.

Para cada $i, j \in \{1, \ldots, m\}$, seja $P_i = (x_i : y_i : z_i)$ tal que $x_i, y_i, z_i \in \mathbb{Z}$ e

$$P_i \times P_j = (y_iz_j - y_jz_i, x_jz_i - x_iz_j, x_iy_j - x_jy_i) \in \mathbb{R}^3.$$

Se $P_i \neq P_j$ então $P_i \times P_j \neq 0$. Seja M_{ij} o máximo divisor comum das coordenadas de $P_i \times P_j$. Pela Proposição 3, $\widetilde{P}_i = \widetilde{P}_j$ se e somente se p divide M_{ij}.

Seja $p > 2$ um número primo que não divide n e tal que $p > M_{ij}$. Logo $\widetilde{P}_i \neq \widetilde{P}_j$. Em particular, S é isomorfo via Φ_n a um subgrupo de $\widetilde{\mathcal{E}}_n(F_p)$. Portanto para quase todo número primo p temos que $\#\widetilde{\mathcal{E}}_n(\mathbb{F}_p)$ é divisível por m. A fortiori isto permanece verdade para quase todo número primo p tal que $p \equiv 3 \bmod 4$. Pela Proposição 4, $\#\widetilde{\mathcal{E}}_n(\mathbb{F}_p) = p+1$, se $p \equiv 3 \bmod 4$. Assim $p \equiv -1 \bmod m$ para quase todo número primo p.

O Teorema das Progressões Aritméticas de Dirichlet afirma que dados dois números inteiros $r, s \neq 0$ tais que $\text{mdc}(r,s) = 1$, existem infinitos números primos da forma $rd + s$ com $d \geq 1$ inteiro. Os casos

$r = 4, s = 3$ e $r = 6, s = 5$ podem ser provados da mesma forma que na demonstração do Teorema de Euclides sobre a infinitude do número de números primos. A demonstração do caso geral utiliza técnicas mais elaboradas da Teoria Analítica dos Números. Para uma demonstração completa ver [Apo76, Chapter 7].

Retornando à demonstração do Teorema, obtemos uma contradição com o Teorema das Progressões Aritméticas de Dirichlet tomando $r = 8$ e $s = 3$ se $m = 8$, $r = 4m$ e $s = 3$ se m é ímpar e 3 não divide m, finalmente $r = 12$ e $s = 7$ se m é ímpar e 3 divide m. □

4 O resultado principal

Teorema 2 *Um número n é congruente se e somente se o posto algébrico de $\mathcal{E}_n$ é positivo.*

Prova. Suponhamos que n seja um número congruente e seja $(a, b) \in E_n(\mathbb{Q})$ a solução da equação cúbica obtida pelo argumento que precede à Proposição 2. Neste caso temos que $a \in \mathbb{Q}^2$ com denominador par. Se (a, b) tiver ordem finita então pelo Teorema 1 temos que (a, b) é necessariamente um ponto de ordem 2. Logo sua primeira coordenada só pode ser 0, n ou $-n$. Claro que $0, -n \notin \mathbb{Q}^2$. Além disto para determinar se um inteiro positivo n é um número congruente, basta considerar sua classe módulo $\mathbb{Q}^2$. Logo supomos sempre que n é livre de quadrados. Portanto $n \notin \mathbb{Q}^2$. Pelo Teorema de Mordell-Weil concluimos que (a, b) tem que ser um ponto de ordem infinita de $\mathcal{E}_n(\mathbb{Q})$. Em particular o posto algébrico de $\mathcal{E}_n$ é positivo.

Reciprocamente dado um ponto $P \in \mathcal{E}_n(\mathbb{Q})$ de ordem infinita então por (4)

$$x_{[2]P} = \frac{x_P^4 + 2n^2x_P^2 + n^4}{(2y_P)^2}$$

satisfaz às condições da Proposição 2. Portanto n é um número congruente. □

Referências

[Apo76] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag 1976.

[Dic52] L. E. Dickson, *History of the Theory of Numbers* , Chelsea, 1952.

[GarLeq88] A. Garcia, Y. Lequain, *Álgebra: um Curso de Introdução*, Projeto Euclides **19**, 1988 (IMPA).

[Kob84] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.

[SilTat92] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, UTM, Springer-Verlag, 1992.

[Tun83] J. Tunnell, *A classical diophantine problem and modular forms of integral weight 3/2*, Invent. Math. 73 (1983), 323-334.

Universidade Federal do Rio de Janeiro
Endereço Postal: Rua Guaiaquil 83, Cachambi, 20785-050 Rio de Janeiro, RJ, Brasil
E-mail: amilcar@impa.br