Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

O Problema dos Números Congruentes: Três versões equivalentes

Jaime Edmundo Apaza Rodriguez[1]
Departamento de Matemática, UNESP, Ilha Solteira, SP
Nair Rodrigues de Souza[2]
Instituto Federal de Mato Grosso do Sul, IFMS, Três Lagoas, MS

Resumo. A procura dos números inteiros n que representem áreas de triângulos retângulos e cujos lados sejam números racionais é conhecido como o Problema dos Números Congruentes. Este problema apareceu pela primeira vez nos manuscritos arabes, por volta de 900 A.C. Em 1983, J. B. Tunnell deu uma resposta conjectural a este problema, provando que se existe um triângulo com área n (seja este par ou ímpar), então o número de soluções pares é igual ao número de soluções ímpares (para certas equações Diofantinas). Recentemente o Problema dos Números Congruentes veio a tona de novo com a descoberta da sua forte conexão com a Aritmética da Curvas Elípticas, um assunto muito discutido nas últimas décadas. Neste trabalho apresentamos três versões equivalentes do Problema dos Números Congruentes: A versão original, a versão triangular e a versão com Curvas Elípticas.

Palavras-chave. Números Congruentes, Curvas Elípticas, Equações Diofantinas.

1 Introdução

O problema dos Números Congruentes foi declarado pelo matemático persa Al-Karaji $(953 - 1029)$. Sua versão não considerava triângulos, mas a expressava em termos de números quadrados, números que são quadrados de números inteiros: $1, 4, 9, 16, 25, 36, \cdots$, os quadrados de números racionais: $25/9, 49/100, 144/25$, etc. A questão indagada por ele era: Se para qualquer número inteiro n existe um quadrado a^2, então $a^2 - n$ *e* $a^2 + n$ são também quadrados? Quando isto for verdade, n é dito número congruente. O nome vem do fato de que existem três quadrados que são congruentes módulo n. Al-Karaji foi fortemente influenciado pela tradução árabe das obras do matemático grego Diofanto $(210 - 290)$, o qual já estudava e elaborava problemas similares.

Houve um certo progresso nos mil anos seguintes. Em 1225, Fibonacci demonstrou que os números 5 e 7 são congruentes e conjecturou que o número 1 não é congruente. A prova foi fornecida por Fermat em 1659. Em 1915, os números congruentes menores do que 100 já foram determinados e, em 1952, Kurt Heegner, introduziu profundas técnicas matemáticas sobre este assunto e mostrou que todos os números primos, na sequência

[1]jaime@mat.feis.unesp.br
[2]nair.souza@ifms.edu.br

$5, 13, 21, 29, \cdots$, são congruentes. No entanto, até 1980 haviam ainda alguns casos, de números menores do que 1000, que não foram resolvidos.

Em 1982, J. B. Tunnell, da Universidade Rutgers, fez progressos significativos via a conexão (Heegner foi o primeiro em usar) entre os números congruentes e as curvas elípticas. Ele encontrou uma simples fórmula para determinar se um número n é ou não congruente. Isto permitiu que os primeiros mil casos fossem rapidamente resolvidos. A questão é que a total validade da sua fórmula depende da veracidade de um caso particular, que é um dos problemas pendentes na matemática, conhecido como a Conjectura de Birch e Swinnerton-Dyer. Esta conjectura é um dos Sete Problemas do Milênio, apresentados pelo Instituto Clay de Matemática, com um prêmio de um milhão de dólares.

2 As duas primeiras versões do problema

Segundo um manuscrito árabe do século X, o principal objetivo dos triângulos retângulos racionais é a seguinte questão:

Problema dos Números Congruentes: Versão I: Dado um número inteiro positivo n, encontrar um racional quadrado a^2 ($a \in \mathbb{Q}^*$) tal que $a^2 \pm n$ sejam ambos racionais quadrados.

Definição 2.1. *Um inteiro n é um número congruente se existir um racional quadrado a^2 tal que $a^2 \pm n$ sejam ambos racionais quadrados.*

Exemplo 1:

(1) 5 é um número congruente pois existe $a = \dfrac{41}{12}$ tal que

$$\left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2, \ \left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2.$$

(2) 6 é um número congruente pois existe $a = \dfrac{5}{2}$ tal que

$$\left(\frac{5}{2}\right)^2 - 6 = \left(\frac{1}{2}\right)^2, \ \left(\frac{5}{2}\right)^2 + 6 = \left(\frac{7}{2}\right)^2.$$

(3) 7 é um número congruente pois existe $a = \dfrac{337}{120}$ tal que

$$\left(\frac{337}{120}\right)^2 - 7 = \left(\frac{113}{120}\right)^2, \ \left(\frac{337}{120}\right)^2 + 7 = \left(\frac{463}{120}\right)^2.$$

Definição 2.2. *Um triângulo retângulo é dito racional se seus lados e hipotenusa são todos números racionais.*

DOI: 10.5540/03.2017.005.01.0229

Problema dos Números Congruentes: Versão II: Dado um número inteiro positivo n, encontrar um triângulo retângulo tal que seus lados sejam números racionais e sua área igual a n.

As versões I e II do Problema dos Números Congruentes são equivalentes, como se mostra a seguir.

Versão I $\Longrightarrow$ *Versão II:* Seja n número inteiro positivo e suponha que $\alpha^2, \beta^2, \gamma^2$ são números racionais quadrados cuja diferença comum é n. Então verifica-se que o triângulo retângulo com lados e hipotenusa

$$a = \gamma - \alpha,\ b = \gamma + \alpha,\quad c = 2\beta$$

tem área n.

Versão II $\Longrightarrow$ *Versão I:* Reciprocamente, suponha que temos um triângulo retângulo racional $[a, b, c]$ com área n. Então os números

$$\left(\frac{a-b}{2}\right)^2,\ \left(\frac{c}{2}\right)^2,\ \left(\frac{a+b}{2}\right)^2$$

formam uma progressão aritmética de 3 números racionais, cuja diferença comum é n.

Exemplo 2:

(1) 5 é a área de um triângulo retângulo racional $[\frac{20}{3}, \frac{3}{2}, \frac{41}{6}]$.

(2) 6 é a área de um triângulo retângulo racional $[3, 4, 5]$.

(3) 7 é a área de um triângulo retângulo racional $[\frac{24}{5}, \frac{35}{12}, \frac{337}{60}]$.

Observação 2.1. *Assumimos que n é um inteiro positivo livre de quadrados (não múltiplo de nenhum quadrado), já que se $[a, b, c]$ é um triângulo retângulo com área n, então $[ak, bk, ck]$ é também um triângulo retângulo com área nk^2, onde k é qualquer número racional.*

Teorema 2.1. *(Fermat) Os números $1, 2, 3$ não são congruentes.*

Demonstração: Sejam (a, b, c) números inteiros positivos, dois a dois coprimos, tal que $a^2 + b^2 = c^2$. Então existe um par de inteiros positivos coprimos (p, q), com $p + q$ ímpar, tal que

$$a = 2pq,\quad b = p^2 - q^2,\quad c = p^2 + q^2.$$

Obtemos assim um número congruente gerado pela fórmula:

$$n = \frac{pq(p+q)(p-q)}{m^2}.$$

Agora suponha que 1 seja um número congruente. Então existe um triângulo retângulo com lados inteiros $[a, b, c]$ com área mínima $m^2 = pq(p + q)(p - q)$.

DOI: 10.5540/03.2017.005.01.0229

Como os 4 fatores de m^2 são coprimos, então

$$p = x^2,\ q = y^2,\ p+q = u^2,\ p-q = v^2.$$

Assim obtemos a equação

$$(u+v)^2 + (u-v)^2 = (2x)^2.$$

Logo a terna $(u+v, u-v, 2x)$ forma um triângulo retângulo com menor área y^2, o que é uma contradição pois tínhamos um triângulo retângulo, $[a, b, c]$, cuja área mínima era $m^2 = pq(p+q)(p-q)$. Portanto 1 não é um número congruente. Analogamente se mostra que 2 *e* 3 não são números congruentes e assim está mostrado o resultado.

Corolário 2.1. *(O triângulo retângulo de Fermat) Se n é um quadrado, então n não é um número congruente.*

Observação 2.2. *Embora se tenha a fórmula*

$$n = \frac{pq(p+q)(p-q)}{m^2},$$

para gerar números congruentes, ela é pouco eficiente. Por exemplo, $n = 157$ *é a área de um triângulo retângulo racional cujos catetos e hipotenusa são [Yan]*

$$a = \frac{411340519227716149383203}{21666555693714761309610},$$

$$b = \frac{6803298487826435051217540}{411340519227716149383203},$$

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Estes resultados se devem ao matemático americano D. B. Zagier. Este fato coloca em evidência, mais uma vez, que matemáticos não podem ser substituídos por computadores.

3 Curvas Elípticas: Terceira versão

Definição 3.1. *Uma curva elíptica é uma curva algébrica (plana) definida por uma equação cúbica da forma*

$$E : y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{Z})$$

com $\triangle = 4a^3 + 27b^2 \neq 0$.

O número $\triangle$ é o discriminante do polinômio cúbico $f(x) = x^3 + ax + b$ e a condição $\triangle \neq 0$ equivale a dizer que $f(x)$ não tem raízes repetidas em $\mathbb{C}$. Este polinômio tem 3 raízes reais ou apenas uma (pois as raízes complexas aparecem em pares).

Seja $E(\mathbb{Q})$ o conjunto de pontos racionais da curva elíptica E, ou seja, o conjunto de pontos $(x, y) \in \mathbb{Q}^2$ que satisfazem a equação acima, junto com o ponto O no infinito. Este ponto hipotético O deve ser considerado como um ponto que se encontra em ambas as

DOI: 10.5540/03.2017.005.01.0229

"pontas" de cada reta vertical. Uma forma precisa de explicar o ponto O é através do mergulho da curva afim no seu "completamento", que é uma curva projetiva.

Os seguintes dois fatos a respeito das curvas elípticas são destacáveis:

1. Uma curva elíptica pode ou não ter um número infinito de pontos racionais. O fato de curvas elípticas terem um número finito de pontos racionais é ainda uma questão em aberto.

2. O conjunto $E(\mathbb{Q})$ tem uma estrutura de grupo abeliano. Denota-se a operação no grupo por $\oplus$ (não confundir com a operação de adição em $\mathbb{R}^2$). Esta é dada pelo método da corda e tangente. A soma de dois pontos pode ser explicitamente calculada como segue (algebricamente isto não faz diferença, mas vamos ilustrar apenas no caso em que $x^3 + ax + b$ tem uma única raiz real).

Para somar dois pontos $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ de $E(\mathbb{Q})$ intersetamos a reta (corda) L, passando por P_1 *e* P_2 (esta será tangente a E em P se $P_1 = P_2 = P$) com E. A reta corta a cúbica em 3 pontos (onde conta-se o ponto O como ponto de E e, no caso da reta tangente a E, conta-se o ponto de tangência como 2 pontos). Seja $P_3 = (x_3, y_3)$ o ponto de interseção de E com L. Então $P_1 + P_2 = (x_3, -y_3)$. O ponto no infinito O atua como identidade já que quasquier 2 pontos de $E(\mathbb{Q})$ que pertençam à reta vertical serão colineares com O. Verifica-se então que $P_1 \oplus P_2 \in E(\mathbb{Q})$.

Deixando de lado os casos triviais quando $P_1 = -P_2$ ou quando pelo menos um deles é igual a O, podemos calcular as coordenadas de $P_1 + P_2$. Para um ponto $P = (x, y)$, seja $x = x(P)$ a x-coordenada de P (similarmente para $y(P)$) e seja L a reta que surge da definição de adição, tendo por equação $y = mx + l$. Então $m = \dfrac{y_1 - y_2}{x_1 - x_2} \in \mathbb{Q}$.

Substituindo na equação da cúbica temos

$$x^3 - m^2x^2 + (a - 2ml)x + b - l^2 = 0.$$

Como x_1, x_2 *e* x_3 são as três soluções da igualdade acima, isto equivale a escrever
$(x - x_1)(x - x_2)(x - x_3) = 0$ ou na forma expandida

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3 = 0.$$

Comparando o coeficientes obtemos

$$x(P_1 + P_2) = x_3 = m^2 - (x_1 + x_2) = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - (x_1 + x_2).$$

Finalmente

$$y(P_1 + P_2) = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)\left[\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - (x_1 + x_2)\right] + l.$$

Como l é claramente racional, isto mostra que $P_1 \oplus P_2$ tem coordenadas racionais.

Um caso especial de curva elíptica é dada por $y^2 = x^3 - n^2x$, com $n \in \mathbb{N},\ n > 1$. A conexão entre números congruentes e curvas elípticas está dada no seguinte resultado.

Teorema 3.1. *Um número inteiro positivos n, livre de quadrados, é número congruente se e somente se a curva elíptica E, definida por*

$$y^2 = x^3 - n^2 x,$$

tem um número infinito de pontos racionais.

Teorema 3.2. *Para $n > 0$, existe uma correspondência $1-1$ entre os seguintes conjuntos:*

$$\{(a,b,c) : a^2 + b^2 = c^2,\ \frac{1}{2}ab = n\}, \quad \{(x,y) : y^2 = x^3 - n^2 x, y \neq 0\}.$$

As correspondências mutuamente inversas entre os dois conjuntos são dadas por:

$$(a,b,c) \longmapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \quad (x,y) \longmapsto \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right).$$

Demonstração: Fixemos o número $n > 0$. As soluções reais (a,b,c) para cada uma das seguintes equações

$$a^2 + b^2 = c^2, \quad \frac{1}{2}ab = n,$$

descrevem uma superfície em $\mathbb{R}^3$. Por isso é natural esperar que essas duas superfícies se cortem em uma curva. Queremos descrever a tal curva $y^2 = x^3 - n^2 x$ sob a escolha certa de coordenadas.

Seja $c = t + a$. Substituindo em $a^2 + b^2 = c^2$, obtemos $b^2 = t^2 + 2at$, ou equivalentemente $2at = b^2 - t^2$. Como $ab = 2n \neq 0$, então nem a nem b são nulos e assim podemos escrever $a = \frac{2n}{b}$ e substituir em $2at = b^2 - t^2$, para obter $\frac{4nt}{b} = b^2 - t^2$, ou $4nt = b^3 - bt^2$.

Observemos que $t \neq 0$ pois caso contrário teríamos $a = c$ e então $b = 0$. Mas lembre-se que $ab = 2n \neq 0$. Assim, dividindo por t^3, obtemos

$$\frac{4n}{t^2} = \left(\frac{b}{t}\right)^3 - \frac{b}{t}.$$

Multiplicando ambos os lados por n^3 conseguimos

$$\left(\frac{2n^2}{t}\right)^2 = \left(\frac{bn}{t}\right)^3 - n^2\left(\frac{bn}{t}\right).$$

Finalmente, fazendo $x = \dfrac{bn}{t} = \dfrac{bn}{c-a}$ *e* $y = \dfrac{2n^2}{t} = \dfrac{2n^2}{c-a} \neq 0$, obtemos a equação da curva elíptica $y^2 = x^3 - n^2 x$.

Observação 3.1.

(1) A equação $y^2 = x^3 - n^2 x$ tem três soluções racionais triviais para $y = 0$:

$$(0,0), (n,0), (-n,0).$$

DOI: 10.5540/03.2017.005.01.0229

(2) A correspondência estabelecida no teorema 3.2 preserva positividade.

Problema dos Números Congruentes: Versão III: Para um número positivo n, encontrar um ponto racional, com $y \neq 0$, sobre a curva elíptica $E_n : y^2 = x^3 - n^2x$.

O teorema 3.2 estabelece a equivalência entre as versões II e III do Problema dos Números Congruentes. Portanto as versões I, II e III são equivalentes.

Observação 3.2. *O ponto de vista da equação $y^2 = x^3 - n^2x$ permite fazer algo marcante: produzir um novo triângulo retângulo racional com área n a partir de dois triângulos conhecidos (pela lei de grupo de pontos sobre curvas elípticas).*

4 Conclusões

O problema estudado, enunciado há mais de mil anos, refere-se as áreas dos triângulos retângulos. O problema é surprendentemente difícil na hora de determinar quais são os números inteiros que representem a área de triângulos retângulos, cujos lados sejam números inteiros ou racionais. Segundo Brian Conrey, Diretor do Instituto Americano de Matemática, "estes velhos problemas podem parecer escuros, mas geram uma grande quantidade de pesquisas úteis e interessantes, assim como novos desenvolvimentos".

Neste trabalho observamos que existem até três formas diferentes (equivalentes entre si) de se estudar o problema dos Números Congruentes. As duas primeiras são relativamente mais fáceis de estudar e analisar. A terceira forma, que requer o estudo de uma classe de curvas cúbicas (curvas elípticas), é muito mais sofisticada. Seu uso requer um estudo mais profundo de tópicos da Aritmética das Curvas Elípticas, uma grande área de estudo da Geometria Algébrica.

Referências

[1] M. A. Bennett. Lucas's Square Pyramid Problem Revisted, *Acta Arithmetica-Warszawa*, p. 341-347, 2002.

[2] J. S. Chahal. Congruent Numbers and Elliptic Curves, *The Mathematical Association of America*. Vol. 113, No. 4, Apr., 2006.

[3] J. B. Tunnell. A Classic Diophantine Problem and Modular Forms of Weight 3/2. *Invent. Math.*, 72(2), p. 323-334, 1983.

[4] L. C. Washington. Elliptic Curves, Number Theory and Cryptography. *CRC Press, Taylor and Francis Group*, Second Edition, 2008.

[5] P. Yan. Congruent Numbers and Elliptic Curves. *math.okstate.edu*, 2014.

[6] A trillion triangles, New computer methods reveal secrets of ancient math problem. *American Institute of Mathematics*, 2009.

