Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Teorema de Mordell-Weil: Cálculo do posto de $E(\mathbb{Q})$

Jaime Edmundo Apaza Rodriguez[1]
UNESP, Ilha Solteira

Resumo. Um clássico resultado da Teoria das Curvas Elípticas definidas sobre o corpo dos números racionais $\mathbb{Q}$ é o Teorema de Mordell-Weil o qual afirma que se E é uma curva elíptica sobre $\mathbb{Q}$, então o conjunto de pontos racionais $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado. O teorema de estrutura para tais grupos garante que $E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$, onde T é o subgrupo de torsão (finito) e $r \geq 0$ é um inteiro, o posto de $E(\mathbb{Q})$. Neste trabalho apresentamos esse teorema, outros resultados necessários e mostraremos dois exemplos de como determinar o número r.

Palavras-chave. Curva elíptica, subgrupo de torsão, posto de uma curva elíptica, pontos racionais.

1 Introdução

Na teoria das curvas elípticas definidas sobre o corpo dos números racionais $\mathbb{Q}$ existe um clássico resultado referente ao grupo de seus pontos racionais. Este resultado (o Teorema de Mordell-Weil) foi mostrado por Mordell em 1922 para curvas elípticas sobre $\mathbb{Q}$. Em 1928 este resultado foi provado por Weil, não apenas para curvas elípticas sobre corpos de números (que são extensões finitas de $\mathbb{Q}$), senão também para variedades abelianas (análogas das curvas elípticas em dimensões superiores).

O Teorema de Mordell-Weil afirma que se E é uma curva elíptica sobre $\mathbb{Q}$, então $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado. O teorema de estrutura para grupos abelianos finitamente gerados afirma que $E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$, onde T é o subgrupo de torsão (finito) e $r \geq 0$ um inteiro, o posto de $E(\mathbb{Q})$.

Calcular o subgrupo T é relativamente simples. Para isso são usados os teoremas de Lutz-Nagell e de Mazur. Mas a determinação do inteiro r é um pouco mais trabalhoso. Neste trabalho, por meio de dois exemplos, mostraremos como calcular esse número r.

A seguir são apresentado os resutados mais importantes que usaremos no cálculo do posto r do grupo $E(\mathbb{Q})$.

Teorema 1.1. *(Teorema de Lutz-Nagell): Seja a curva elíptica E dada por $y^2 = x^3 + Ax + B$, com $A, B \in \mathbb{Z}$. Seja $P = (x, y) \in E(\mathbb{Q})$ de ordem finito. Então $x, y \in \mathbb{Z}$. Se $y \neq 0$, então $y^2 | 4A^3 + 27B^2$.*

[1]jaime.rodriguez@unesp.br

Observação 1.1. *O número $4A^3 + 27B^2$ é chamado discriminante da curva elíptica E.*

Teorema 1.2. *(Teorema de Mordell-Weil) Seja E uma curva elíptica sobre $\mathbb{Q}$. Então $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado.*

Teorema 1.3. *(Teorema de Estrutura) Todo grupo abeliano finitamente gerado G pode ser escrito na forma*

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s} \oplus \mathbb{Z}^r$$

com $r \geq 0$ e $n_i | n_{i+1}$, onde os inteiros r e n_i são determinados unicamente por G.

Aplicando este resultado ao grupo $E(\mathbb{Q})$ temos que

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$$

onde T é um grupo finito (subgrupo de torsão de $E(\mathbb{Q})$) e $r \geq 0$ inteiro positivo, chamado de posto de $E(\mathbb{Q})$.

Outros resultados a serem usados são

Teorema 1.4. *Seja a curva elíptica E dada pela equação $y^2 = (x - e_1)(x - e_2)(x - e_3)$, com $e_1, e_2, e_3 \in \mathbb{Z}$. A aplicação*

$$\varphi : E(\mathbb{Q}) \longrightarrow (\mathbb{Q}^*/\mathbb{Q}^{*^2}) \oplus (\mathbb{Q}^*/\mathbb{Q}^{*^2}) \oplus (\mathbb{Q}^*/\mathbb{Q}^{*^2})$$

dada por

$$(x, y) \longmapsto (x - e_1,\ x - e_2,\ x - e_3), \quad \textit{quando} \quad y \neq 0$$

$$\infty \longmapsto (1, 1, 1)$$

$$(e_1, 0) \longmapsto ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3)$$

$$(e_2, 0) \longmapsto (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3)$$

$$(e_3, 0) \longmapsto (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2))$$

é um homomorfismo cujo núcleo é $2E(\mathbb{Q})$.

Teorema 1.5. *(Forma fraca do teorema de Mordell-Weil) Seja E um curva elíptica sobre $\mathbb{Q}$. Então $E(\mathbb{Q})/2E(\mathbb{Q})$ é grupo finito.*

Observação 1.2. *As demonstrações destes resultados podem ser encontrados, por exemplo, em [4].*

DOI: 10.5540/03.2020.007.01.0443

2 Aplicações: Cálculo do número r

Exemplo 1: Seja a curva elíptica $E : y^2 = x^3 - 4x = x(x-2)(x+2)$. São encontrados 4 pontos racionais sobre E. Assim temos, pelo teorema 1.5:

$$E(\mathbb{Q})/2E(\mathbb{Q}) = \{\infty, (0,0), (2,0), (-2,0)\}.$$

Fazendo cálculos com o teorema 1.1, temos que o subgrupo de torsão de $E(\mathbb{Q})$ é $T = E[2]$. Logo pelo teorema 1.5 temos que $E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$, de onde segue que

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (T/2T) \oplus \mathbb{Z}_2^r = T \oplus \mathbb{Z}_2^r.$$

Dado que $E(\mathbb{Q})/2E(\mathbb{Q})$ tem ordem 4 então devemos ter $r = 0$. Portanto

$$E(\mathbb{Q}) = E[2] = \{\infty, (0,0), (2,0), (-2,0)\}.$$

Exemplo 2: Seja a curva elíptica $E : y^2 = x^3 - 25x = x(x-5)(x+5)$. Encontramos os pontos

$$(0,0), (5,0), (-5,0), (-4,6).$$

Alguns cálculos, considerando uma reta tangente à curva passando pelo ponto $(-4,6)$, fornecem o ponto

$$2(-4,6) = (\frac{41^2}{12^2}, \frac{-62279}{1728}).$$

Dado que o ponto $2(-4,6)$ não tem coordenadas inteiras, então $(-4,6)$ não pode ser ponto de torsão, pelo teorema 1.1. De fato, os cálculos realizados usando o teorema 1.1 mostram que o subgrupo de torsão é

$$T = \{(\infty, (0,0), (5,0), (-5,0)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Afirmamos que

$$E(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}.$$

Agora, o posto r deve ser, pelo menos 1, pois o ponto $(-4,6)$ é de ordem infinito. Então o problema é mostrar que o posto é exatamente 1.

Para verificar isso consideremos a aplicação

$$\varphi : E(\mathbb{Q}) \longrightarrow (\mathbb{Q}^*/\mathbb{Q}^{*^2}) \oplus (\mathbb{Q}^*/\mathbb{Q}^{*^2}) \oplus (\mathbb{Q}^*/\mathbb{Q}^{*^2})$$

do teorema 1.4, definida por $\varphi(x,y) = (x, x-5, x+5)$ quando $y \neq 0$.

Usando o fato que $-4 \equiv -1 \ (mod\ m^2)$ e $-9 \equiv -1 \ (mod\ n^2)$, para alguns $m, n \in \mathbb{Z}^+$, temos que

$$\varphi(-4,6) = (-1,-1,1).$$

Agora, novamente pelo teorema 1.4 temos que

$$\varphi(\infty) = (1,1,1)$$

$$\varphi(0,0) = (-1,-5,5)$$
$$\varphi(5,0) = (5,2,10)$$
$$\varphi(-5,0) = (-5,-10,2).$$

Como φ é um homomorfismo, observamos que $\varphi(-4,6)$ vezes qualquer uma dessas triplas esta na imagem de φ, de modo que

$$(1,5,5), (-5,-2,10), (5,10,2)$$

correspondem aos pontos dados.

Escrevendo

$$x = au^2, \quad x-5 = bv^2, \quad x+5 = cw^2$$

temos que $\varphi(x,y) = (a,b,c)$. Podemos assumir então que

$$a,b,c \in \{\pm 1, \pm 2, \pm 5, \pm 10\}.$$

Além disso, abc é um quadrado e assim c é determinado por a *e* b. Por tanto ignoraremos c e nos concentraremos nas possiblidades para a *e* b.

Existem 64 possíveis pares $a,\ b$. Até agora temos 8 pares que correspondem aos pontos acima. Estes pares são dados em

$$L = \{(1,1),(1,5),(-1,-1),(-1,-5),(5,2),(5,10),(-5,-2),(-5,-10)\}.$$

Agora resta eliminar as 56 possiblidades restantes.

Observemos que

$$x-5 = bv^2 < x = au^2 < x+5 = cw^2.$$

Se $a < 0$, então $b < 0$. Se $a > 0$, então $c > 0$ e portanto $b > 0$ dado que abc é quadrado. Por isso a *e* b devem ter o mesmo sinal. Isto deixa 32 pares possíveis para a *e* b.

Agora consideramos, e eliminamos, três pares especiais. Pelo fato de φ ser um homomorfismo, basta para eliminar todos, exceto os oito pares correspondentes aos pontos conhecidos.

(a,b) = (2, 1). Temos que

$$x = 2u^2, \quad x-5 = v^2, \quad x+5 = 2w^2.$$

Logo

$$2u^2 - v^2 = 5, \quad 2w^2 - 2u^2 = 5.$$

Se u ou v tivessem denominador par, então o outro também o terá. No entanto, $2u^2$ tem uma potência ímpar de 2 em seu denominador, enquanto v^2 tem uma potência par de 2 em seu denominador. Por isso, $2u^2 - v^2$ não é um número inteiro, o que é contraditório. Segue então que u, v tem denominadores ímpares, de modo que podemos considerar eles módulo potência de 2. Como $v^2 \equiv -5\ (mod\ 2)$, deve-se ter v ímpar. Assim $v^2 \equiv 1\ (mod\ 8)$ e portanto $2u^2 \equiv 6\ (mod\ 8)$.

DOI: 10.5540/03.2020.007.01.0443

Isto implica que $u^2 \equiv 3 \ (mod\ 4)$, o que é impossível, o que implica na eliminação do par $(a, b) = (2, 1)$.

(a,b) = (5, 1). Temos que

$$x = 5u^2, \quad x - 5 = v^2, \quad x + 5 = 5w^2.$$

Logo

$$5u^2 - v^2 = 5, \quad 5w^2 - 5u^2 = 5.$$

Se o denominador de u ou v é divisível por 5, então assim o será o outro. Mas então $5u^2$ tem uma potência ímpar de 5 no seu denominador, enquanto que v^2 tem uma potência par de 5 no seu denominador. Mas isto é impossível, e assim os denominadores de u e v são ambos não divisíveis por 5. Como $w^2 - u^2 = 1$, o mesmo vale para w. Portanto, podemos considerar u, v, w módulo 5. Temos então $v \equiv 0 \ (mod\ 5)$, e assim podemos escrever $v = 5v_1$. Portanto

$$u^2 - 5v_1^2 = 1$$

e assim $u^2 \equiv 1 \ (mod\ 5)$. Portanto $w^2 = 1 + u^2 \equiv 2 \ (mod\ 5)$. Mas isto é impossível, o que implica na eliminação do par $(a, b) = (5, 1)$.

(a,b) = (10, 1). Temos que

$$x = 10u^2, \quad x - 5 = v^2, \quad x + 5 = 10w^2.$$

Logo

$$10u^2 - v^2 = 5, \quad 10w^2 - 10u^2 = 5.$$

Como no caso anterior, os denominadores de u, v, w não são divisíveis por 5. Consideremos $v = 5v_1$. Então $2u^2 - 5v_1^2 = 1$ e assim $2u^2 \equiv 1 \ (mod\ 5)$. Mas isto é impossível, o que implica na eliminação do par **(a,b) = (10, 1)**.

Os pares da forma $(a, 1)$, com $a < 0$ também são eliminados pois a, b devem ter o mesmo sinal. Por isso $(1, 1) = \varphi(\infty)$ é o único par da forma $(a, 1)$ correspondente a esse ponto.

Agora seja (a, b) qualquer par. Existe um ponto P com $\varphi(P) = (a', b)$ no conjunto

$$L = \{(1, 1), (1, 5), (-1, -1), (-1, -5), (5, 2), (5, 10), (-5, -2), (-5, -10)\},$$

para algum a'. Se existir um ponto Q com $\varphi(Q) = (a, b)$, então

$$\varphi(P - Q) = (a', b)(a, b)^{-1} = (a'', 1)$$

para algum a''. Mostramos que $(a'', 1)$ não está na imagem de φ quando $a'' \neq 1$. Por isso $a'' = 1$ e assim $a = a'$ e $(a, b) = (a', b) = \varphi(P)$. Consequentemente os únicos pares na imagem de φ são aqueles que estão no conjunto L.

Como mencionado anteriormente, o subgrupo de torsão de $E(\mathbb{Q})$ é $E[2]$ e assim

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2^r$$

para algum r.

DOI: 10.5540/03.2020.007.01.0443

Como a imagem de φ tem ordem 8 e o núcleo de φ é $2E(\mathbb{Q})$, então a ordem de $E(\mathbb{Q})/2E(\mathbb{Q})$ é 8 e portanto $r = 1$. Isto implica que

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}.$$

Observar que também foi provado que $E[2]$ e $(-4, 6)$ geram um subgrupo de $E(\mathbb{Q})$ de índice ímpar. Pode ser mostrado que eles realmente geram o grupo todo.

3 Conclusões

Como foi observado, o cálculo do posto r (o número de pontos de ordem infinita) do grupo $E(\mathbb{Q})$ é uma tarefa mais complexa que o cálculo do subgrupo de torsão, ou seja, que o cálculo dos pontos de ordem finita.

Os exemplos exibidos são casos específicos e simples do cálculo do número r, usando alguns resultados apresentados na primeira seção. Existem casos em que o cálculo do número r é realmente difícil como o caso do grupo não trivial de Shafarevich-Tate (veja-se [4]), onde tem que se usar a chamada Cohomologia de Galois.

Referências

[1] D. M. G. Dias, J. E. A. Rodriguez. *Um clássico resultado: O Teorema de Mordell.* CNMAC, Campinas, 2018.

[2] W. Fulton. *Algebraic Curves*, Addison-Wesley Publishing Company, 1989.

[3] N. Koblitz. *Introduction to Elliptic Curves and modular forms.*, Vol. 97 of graduate texts in Mathematics, Springer-Verlag, 1993.

[4] L. Washington. *Elliptic Curves, Number Theory and Cryptography*, CRC Press, 2008.

DOI: 10.5540/03.2020.007.01.0443