VI Encontro do Hotel de Hilbert

Criptografia: o que o Heron tem a ver com isso?

Beatriz C. da Motta Ribeiro* (UFJF)

com a colaboração de Reginaldo Braz (UFJF) e Sandro Mazorche (UFJF)

20 de novembro de 2018

Resumo

Esse texto é um complemento para quem quiser saber mais sobre a palestra. Nosso objetivo é conectar uma pergunta básica de geometria de triângulos com um assunto atual de pesquisa matemática: a criptografia de curvas elípticas. Vamos começar vendo como podemos usar trigonometria e a fórmula de Heron para classificação de famílias de triângulos com mesma área e perímetro, obtendo uma equação especial cujas soluções serão chamadas de curva elíptica. Assim, nosso objetivo é entender como essas curvas que surgem de uma fórmula do século I são utilizadas para a segurança de informações no século XXI. Para isso, na segunda parte da palestra, vamos estudar um pouco de aritmética modular e os princípios básicos da criptografia. Por fim, vamos construir uma aritmética entre pontos de uma curva elíptica e usar essa matemática para entender a criptografia baseada em curvas elípticas.

1 Uma família de triângulos

Essa primeira seção está baseada no artigo [1].

Vamos começar com os triângulos da figura 1. É fácil verificar que ambos têm perímetro igual a 12.

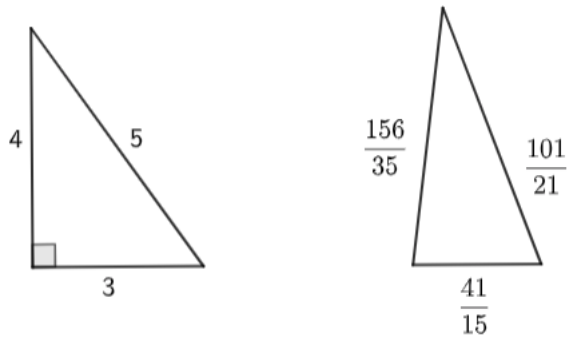


Figura 1: triângulos de mesmo perímetro.

*Endereço eletrônico: beatriz@ice.ufjf.br

Ambos têm também a mesma área. A do triângulo retângulo é claro que é 6, a do outro podemos calcular usando a fórmula de Heron:

$$A = \sqrt{s(s-a)(s-b)(s-c)}\,,$$

onde a, b, c são as medidas dos lados e $s = \frac{1}{2}(a+b+c)$ é o semiperímetro do triângulo.

Olhando para triângulos aparentemente tão diferentes mais com duas propriedades iguais, podemos nos perguntar: *como encontrar triângulos com área e perímetro fixados?* A resposta dessa pergunta tem relação com o fato de que todo triângulo tem um círculo inscrito e, então, a área do triângulo tem relação com o raio desse círculo:

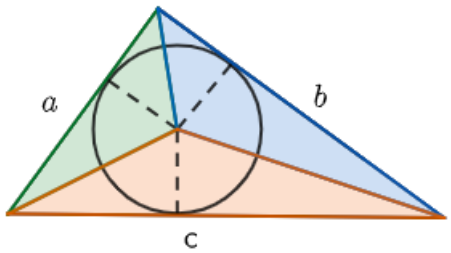


Figura 2: Triângulo de lados a, b, c com círculo de raio r inscrito.

Por exemplo, vejamos o triângulo da figura 2, de lados a, b, c. O círculo inscrito tem raio r. Dividindo esse triângulo em 3 triângulos coloridos, todos de altura igual ao raio r do círculo inscrito, concluimos que a área do triângulo é r vezes o semiperímetro.

$$A = A_{\text{verde}} + A_{\text{azul}} + A_{\text{laranja}} = \frac{ar}{2} + \frac{br}{2} + \frac{cr}{2} = r\frac{a+b+c}{2} = rs \tag{1}$$

Ou seja: todo triângulo de mesma área e mesmo perímetro tem o mesmo círculo inscrito. Você saberia dizer se vale a recíproca, ou seja se dois triângulos têm mesmos círculos inscritos então tem mesma área e perímetro?

Voltanto ao triângulo, vemos que as alturas dos 3 triângulos coloridos dividem o círculo em 3 setores de ângulos α, β, γ, como na figura 3.

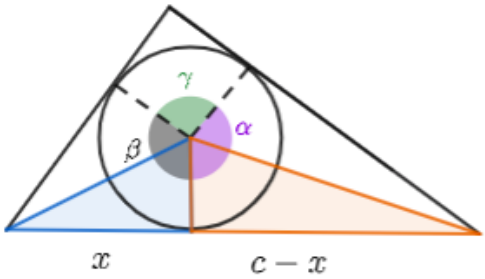


Figura 3: Os ângulos α, β e γ definidos pelas alturas dos triângulos da figura 2.

Vamos nos deter por enquanto no triângulo que aqui está dividido em dois triângulos retângulos azul e laranja. Se a base do triângulo maior mede c, então o triângulo azul tem base x e o laranja tem base $c - x$. Ambos tem altura r. Além disso, os demais lados dos triângulos bissectam os ângulos β e α.

Então, obtemos

$$\operatorname{tg}\left(\frac{\beta}{2}\right) = \frac{x}{r} \qquad \text{e} \qquad \operatorname{tg}\left(\frac{\alpha}{2}\right) = \frac{c-x}{r},$$

ou seja

$$x = r\left(\operatorname{tg}\left(\frac{\alpha}{2}\right) + \operatorname{tg}\left(\frac{\beta}{2}\right)\right)$$

Repetindo o processo nos demais triângulos e somando, obtemos

$$s = r\left(\operatorname{tg}\left(\frac{\alpha}{2}\right) + \operatorname{tg}\left(\frac{\beta}{2}\right) + \operatorname{tg}\left(\frac{\gamma}{2}\right)\right) \tag{2}$$

Juntando as expressões em (1) e (2), obtemos:

$$\frac{s^2}{A} = \operatorname{tg}\left(\frac{\alpha}{2}\right) + \operatorname{tg}\left(\frac{\beta}{2}\right) + \operatorname{tg}\left(\frac{\gamma}{2}\right) \tag{3}$$

Denotando por x, y, z as tangentes de $\frac{\alpha}{2}$, $\frac{\beta}{2}$ e $\frac{\gamma}{2}$, respectivamente, notando que $\gamma = 2\pi - \alpha - \beta$ e usando a fórmula da tangente da soma de ângulos, temos que

$$\begin{aligned} z = \operatorname{tg}\left(\frac{\gamma}{2}\right) &= \operatorname{tg}\left(\pi - \frac{\alpha}{2} - \frac{\beta}{2}\right) \\ &= -\operatorname{tg}\left(\frac{\alpha}{2} + \frac{\beta}{2}\right) = -\left(\frac{\operatorname{tg}\left(\frac{\alpha}{2}\right) + \operatorname{tg}\left(\frac{\beta}{2}\right)}{1 - \operatorname{tg}\left(\frac{\alpha}{2}\right)\operatorname{tg}\left(\frac{\beta}{2}\right)}\right) = -\frac{x+y}{1-xy} \end{aligned}$$

Dessa forma, a expressão em (3) torna-se:

$$\frac{s^2}{A} = x + y - \frac{x+y}{1-xy}$$

que considerando $k = \frac{s^2}{A}$ podemos reescrever como

$$k(1-xy) = (x+y)(1-xy) - (x+y),$$

ou seja

$$x^2y + xy^2 = kxy - k \tag{4}$$

A equação (4) define o que chamamos de curva no plano cartesiano, de forma que todo triângulo com mesma área e mesmo perímetro fixos determina um ponto (x, y) da curva e todo ponto da curva em uma certa região do plano corresponde a um triângulo. Essa região é a que corresponde aos ângulos tais que $\alpha + \beta + \gamma = 2\pi$ e $0 < \alpha, \beta, \gamma < \pi$, isto é a região com $x, y > 0$ e $xy > 1$.

Voltando ao nosso exemplo inicial, temos $A = 6$ e $s = 6$, donde $k = s^2/A = 6$ e a curva que representa a família de triângulos com essas propriedades é

$$x^2y + xy^2 = 6xy - 6$$

representada na figura a seguir:

Todos os pontos na componente do primeiro quadrante correspondem a um triângulo de lados

$$a = x + y, \quad b = y + z, \quad c = z + x$$

Em particular, alguns pontos podem representar o mesmo triângulo: por exemplo, o triângulo pitagórico de lados 3, 4, 5 é representado pelos pontos $(1, 2)$, $(2, 1)$, $(2, 3)$, $(3, 2)$, $(1, 3)$ e $(3, 1)$.

2 Uma família de curvas

As curvas do tipo $x^2y + xy^2 = kxy - k$ fazem parte de uma família maior: as curvas elípticas. Em geral, fazendo mudanças de variáveis, as curvas dessas família podem ser escritas como

$$y^2 = x^3 + ax + b\,,$$

onde $4a^3 + 27b^2 \neq 0$.

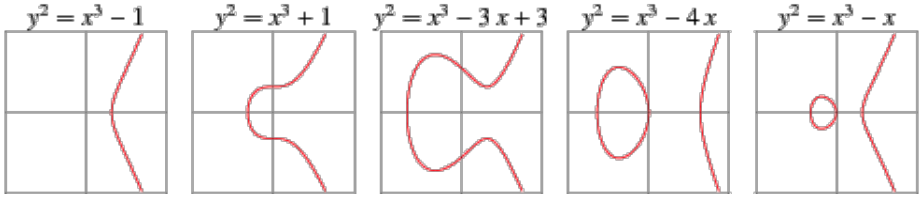


Figura 4: Exemplos de curvas elípticas.

As curvas não tem esse nome por serem elipses, mas sim por aparecerem no estudo de certas funções chamadas elípticas. Essas curvas são o centro de muitas pesquisas em Teoria dos Números, Teoria dos Códigos e Criptografia, além de serem elemento chave na demonstração do famoso Último Teorema de Fermat (aquele que ficou aberto por 350 anos e afirma que não existem soluções inteiras não triviais para $x^n + y^n = z^n$ se $n \geq 3$).

2.1 Obtendo pontos em uma curva

Um dos pontos de grande interesse nessas curvas é o que vamos descrever a seguir. dados dois pontos P e Q na curva, traçando a reta secante à curva definida por $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, encontramos mais um ponto R na curva. Encontrar as coordenadas (x, y) de S depende das coordenadas de P e Q segundo o sistema:

$$\begin{cases} y^2 = x^3 + ax + b & \text{equação da curva} \\ (x_1 - x_2)(x - x_2) = (y_1 - y_2)(y - y_2) & \text{equação da reta por } P \text{ e } Q \end{cases}$$

Ou seja, acabamos por resolver uma equação cúbica em x das quais já conhecemos duas raízes x_1 e x_2.

Por exemplo, voltando à curva $x^2y + xy^2 = 6xy - 6$, escolhendo os pontos $P = (1, 2)$ e $Q = (2, 3)$ devemos resolver:

$$\begin{cases} x^2y + xy^2 = 6xy - 6 \\ y = x + 1 \end{cases}$$

ou seja, devemos encontrar as raízes de $2x^3 - 3x^2 - 5x + 6 = 0$ sabendo que $x = 1$ e $x = 2$ são raízes. Fazendo isso dividindo

$$2x^3 - 3x^2 - 5x + 6$$

por

$$(x - 1)(x - 2) = x^2 - 3x + 2\,,$$

obtendo $2x + 3$. Assim $x = -3/2$, que nos dá $y = -1/2$, ou seja, o ponto $R = (-3/2, -1/2)$.

Podemos repetir esse método, obtendo novos pontos da curva elíptica. É possível provar que existem infinitos pontos com coordenadas racionais nessas curvas. Além disso, esse método nos permite definir uma operação entre pontos da curva que obedece todas as propriedades esperadas de uma boa operação: comutatividade, associatividade, existência de elemento neutro e existência de elemento inverso. Vamos definir essa operação a seguir.

2.2 Uma operação entre pontos de uma curva elíptica

A definição de uma operação entre pontos de uma curva elíptica é dada geometricamente. Como vimos, dados dois pontos P e Q, em geral encontramos um terceiro ponto $R = (x, y)$ na curva elíptica fixada. Refletindo esse ponto em relação ao eixo x, isto é, tomando o ponto que chamaremos de $-R = (x, -y)$, veja a figura 5. Vamos definir

$$P \oplus Q = -R$$

Como a definição depende apenas da reta secante por P e Q, claro que $P \oplus Q = Q \oplus R$, ou seja, a operação é comutativa.

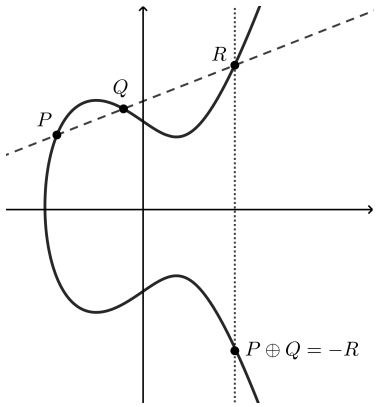


Figura 5: A definição da soma $P \oplus Q$.

A situação descrita na figura anterior é bem ilustrativa, mas deixa escapar alguns problemas. Por exemplo, quando os pontos P e Q estão em uma reta paralela ao eixo y, ou seja, quando queremos somar P e $Q = -P$, quem seria o 3° ponto na curva?

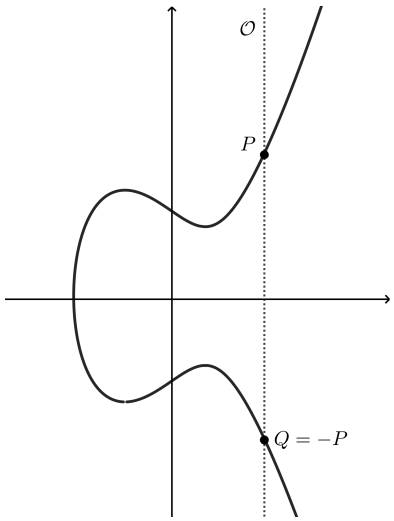


Figura 6: A definição da soma $-P \oplus P$.

Para que nossa operação fique bem definida, vamos chamar esse "ponto" definido por $-P \oplus P$ "no infinito" de $\mathcal{O}$. Esse ponto é ainda mais importante porque será o elemento neutro da operação exatamente pela forma como é definido. Outro caso importante é quando queremos somar um ponto P com ele mesmo.

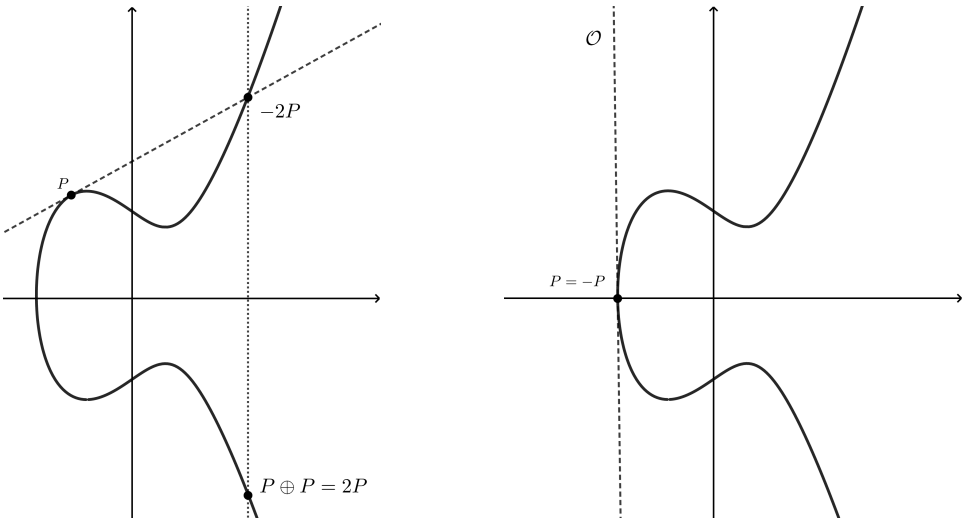


Figura 7: A definição da soma $2P$.

Nesse caso, a reta por P e P é a reta tangente à curva em P, que deve encontrar um "terceiro" ponto na curva ou o ponto $\mathcal{O}$ no caso ilustrado na figura 7 à direita. A figura 8 dá uma ideia da soma de P com ele mesmo diversas vezes.

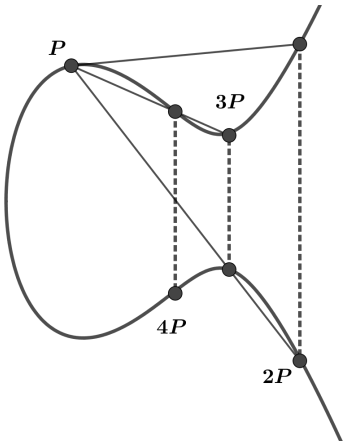


Figura 8: Somando P algumas vezes.

A operação pode ser vista em termos das coordenadas de P e Q usando a ideia descrita na subseção 2.1. Dados $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ tais que $P \neq -Q$, seja $m = \dfrac{y_1 - y_2}{x_1 - x_2}$. Temos que $P \oplus Q = (x, y)$ tem coordenadas

$$x = m^2 - x_1 - x_2 \qquad \text{e} \qquad y = -y_1 + m(x_1 - x)$$

Vamos ver um exemplo. Consideramos a curva $y^2 = x^3 - 5x + 4$ e os pontos $P = (1, 0)$ e $Q = (0, 2)$. Você pode somá-los geometricamente, mas aqui vamos fazer com a fórmula vista. Primeiro, notamos que

$$m = \frac{y_1 - y_2}{x_1 - x_2} = -2$$

Agora, calculamos:

$$x = (-2)^2 - 1 = 3 \qquad \text{e} \qquad y = -2(1 - 3) = 4$$

Assim, obtemos

$$P \oplus Q = (1, 0) \oplus (0, 2) = (3, 4)$$

Agora, se $P = (x_1, y_1)$ não tem $y_1 = 0$, definimos $m = \dfrac{3x_1^2 + a}{2y_1}$ (esse a é o da equação da curva $y^2 = x^3 + ax + b$) e temos que $2P = P \oplus P = (x, y)$ tem coordenadas

$$x = m^2 - 2x_1 \qquad \text{e} \qquad y = -y_1 + m(x_1 - x)$$

Voltando ao exemplo anterior, vamos calcular $2Q$, onde $Q = (0, 2)$. Temos

$$m = \frac{3x_1^2 + a}{2y_1} = \frac{-5}{4}$$

e podemos calcular

$$x = (-5/4)^2 = 25/16 \qquad \text{e} \qquad y = -2 + (5/4)(25/16) = -3/64$$

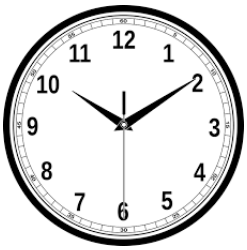
Portanto

$$2Q = (0, 2) + (0, 2) = \left(\frac{25}{16}, \frac{-3}{64}\right)$$

Queremos ter uma ideia de como essas curvas e a operações descritas até aqui podem ser utilizadas para codificar informações. Para isso, é importante que tanto as curvas quanto o conjunto de números com os quais estejamos trabalhando tenham um número finito de elementos. Para isso, vamos dar um passo na aritmética modular na seção a seguir.

3 Um pouco de aritmética modular

Vamos começar pensando em um relógio de ponteiros tradicional.



Uma pergunta simples: se o ponteiro marcar inicialmente 3 horas e se passarem 10 horas, onde estará o ponteiro? Sabemos que não existe a hora 13 no relógio, quando o ponteiro alcança o 12, recomeça a contagem. Assim, 10 horas de pois das 3 horas é 1 hora. Essa matemática do relógio é parte do nosso cotidiano e também um exemplo bem simples de aritmética modular.

Dado um número inteiro $n \geq 2$, vamos dizer que a é equivalente a b módulo n e escrever

$$a \equiv b \pmod{n}$$

quando n dividir a diferença $a - b$, ou seja, quando a e b tiverem o mesmo resto na divisão por n. Assim, a aritmética modular é a aritmética dos restos.

Vejamos alguns exemplos:

$$13 \equiv 1 \pmod{12}, \qquad 12 \equiv 21 \pmod{9}, \qquad -3 \equiv 17 \pmod{5}$$

Pensando apenas na definição dada, podemos provar várias propriedades (fica como exercício):

1. $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ e $c \in \mathbb{Z} \Rightarrow a + c \equiv b + c \pmod{n}$
3. $a \equiv b \pmod{n}$ e $c \in \mathbb{Z} \Rightarrow ac \equiv bc \pmod{n}$
4. $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$
5. $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$
6. $a \equiv b \pmod{n}$ e $r \geq 2 \Rightarrow a^r \equiv b^r \pmod{n}$

Podemos usar essas propriedades para simplificar nossas contas. Por exemplo, digamos que queremos calcular o resto da divisão de 7^{200} por 50. Temos que:

$$7^2 = 49 \equiv -1 \pmod{50}$$

Assim, usando a última propriedade e o fato de que $7^{200} = (7^2)^{100}$, temos que

$$7^{200} \equiv (-1)^{100} \equiv 1 \pmod{50},$$

ou seja, o resto é 1.

Usando a noção de que $a \equiv r \pmod{n}$, onde r é o resto da divisão de a por n, e sabendo que $0 \leq r \leq n-1$, vemos que podemos dividir todos os números inteiros em n conjuntos de acordo com os restos que deixam na divisão por n. Por exemplo, na divisão por 2, só podemos ter resto 0 ou 1. Os inteiros que deixam resto 0 são os pares, os que deixam resto 1 são os ímpares. Não há inteiros que não sejam pares ou ímpares. Na divisão por 3, podemos ter restos 0, 1 ou 2. Dividimos os números então:

$$[0] = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$[1] = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$[2] = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Fazendo isso para qualquer número $n \geq 2$, podemos formar o conjunto das classes dos restos da divisão por n, que vamos chamar de $\mathbb{Z}_n$:

$$\mathbb{Z}_n = \{[0],\ [1],\ [2],\ \ldots\ [n-1]\}$$

Dentro desse conjunto, usando as propriedades, podemos fazer operações:

$$[a] + [b] = [a+b] \qquad \text{e} \qquad [a][b] = [ab]$$

Por exemplo, trabalhando em $\mathbb{Z}_3$, ou seja, no conjunto de restos na divisão por 3, temos que

$$[1] + [2] = [1+2] = [0]\,,$$

porque $1 + 2 = 3$ deixa resto 0 na divisão por 3. Já em $\mathbb{Z}_{12}$ (o relógio!), temos que

$$[6] + [7] = [6+7] = [1] \qquad \text{e} \qquad [2][6] = [2 \cdot 6] = [0]$$

Outro exemplo está dado na tabela a seguir, que apresenta todos os produtos de dois elementos do conjunto $\mathbb{Z}_{13}$.

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

Figura 9: Todos os produtos em $\mathbb{Z}_{13}$.

O conjunto $\mathbb{Z}_n$ com as operações definitas tem uma estrutura algébrica bastante útil na matemática, em particular na criptografia, como veremos nas próximas seções.

4 Curvas sobre $\mathbb{Z}_p$

Para a criptografia sobre curvas elípticas, vamos trabalhar com as curvas

$$y^2 = x^3 + ax + b$$

com os coeficientes a, b dentro de um conjunto $\mathbb{Z}_p$ de restos na divisão por um número primo p, mas não vamos usar os colchetes para não carregar a notação. A curva elíptica inclui todos os pontos $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ que satisfazem a equação, além do ponto $\mathcal{O}$, como vimos na seção 2.

Vamos ver um exemplo. Consideremos a curva $y^2 = x^3 + 3x + 7$ em $\mathbb{Z}_{13}$. Como só existem 13 valores possíveis para x e 13 valores possíveis para y, podemos encontrar todos os pontos (x, y) da curva usando a curva. Substituimos cada um dos valores $0, 1, \ldots, 12$ em x e vemos se o número obtido é um quadrado perfeito em $\mathbb{Z}_{13}$. Para isso, podemos usar a tabela da figura 9. Por exemplo, para $x = 0$, temos $x^3 + 3x + 7 = 7$ que não é um quadrado perfeito. Já para $x = 3$, temos que $x^3 + 3x + 7 = 43$, que, em $\mathbb{Z}_{13}$, é o mesmo que 4, que por sua vez é um quadrado perfeito. Fazendo essa conta com todos os valores possíveis para x, obtemos

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 + 3x + 7$	7	11	8	4	5	4	7	7	10	9	10	6	3

Figura 10: Todos os valores de $x^3 + 3x + 7$.

Verificando na tabela da figura 9, vemos quais desses valores são quadrados (a saber: 3, 4, 9, 10) e então determinamos suas raízes, novamente utilizando a tabela. Dessa forma, obtemos os 13 pontos dessa curva:

$$\{\mathcal{O}, (3, 2), (3, 11), (5, 2), (5, 11), (8, 6), (8, 7), (9, 3), (9, 10), (10, 6), (10, 7), (12, 4), (12, 9)\}.$$

Atenção: é uma coinciência estarmos trabalhando em $\mathbb{Z}_{13}$ e termos obtido 13 pontos!

Perceba que, então, a curva não tem mais uma cara de curva como estamos acostumados a ver, mas sim é um conjunto finito de pontos no plano. No entanto, podemos ainda usar o algoritmo de soma de pontos que vimos no capítulo 2.

No exemplo que estamos fazendo, vamos começar com o ponto $P_1 = (3, 2)$. Tomando $P_2 = (3, 11)$, temos que $2 \equiv -11 \pmod{13}$, ou seja, $P_2 = -P_1$ e, assim, $P_1 \oplus P_2 = \mathcal{O}$. Agora, vamos somar $P_1 = (2, 3)$ com $P_3 = (5, 11)$. Primeiro, devemos calcular

$$m \equiv \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} \Leftrightarrow m(x_2 - x_1) = y_2 - y_1$$

ou seja

$$m(5 - 3) \equiv 11 - 2 \pmod{13} \Leftrightarrow 2m \equiv 9 \pmod{13}$$

Utilizando mais uma vez a tabela da figura 9 (ou simplesmenta procurando um número entre 0 e 12 tal que o dobro menos 9 seja múltiplo de 13), temos que $m = 11$. Calculamos então as coordenadas de $P_1 \oplus P_3 = (x, y)$ como:

$$x = 11^2 - 5 - 3 = 113, \text{ que é o mesmo que } 9$$

$$y = 11(3 - 9) - 2 = -68, \text{ que é o mesmo que } 10$$

ou seja $(2,3) \oplus (5,11) = (9,10)$ Repetindo esse processo, podemos somar todos os pontos da curva:

$\oplus$	O	(3,2)	(3,11)	(5,2)	(5,11)	(8,6)	(8, 7)	(9,3)	(9,10)	(10,6)	(10,7)	(12, 4)	(12, 9)
O	O	(3,2)	(3,11)	(5,2)	(5,11)	(8,6)	(8, 7)	(9,3)	(9,10)	(10,6)	(10,7)	(12, 4)	(12, 9)
(3,2)	(3,2)	(8,6)	O	(5,11)	(9,10)	(12,9)	(3,11)	(5,2)	(10,6)	(12,4)	(9,3)	(8,7)	(10,7)
(3,11)	(3,11)	O	(8,7)	(9,3)	(5,2)	(3,2)	(12,4)	(10,7)	(5,11)	(9,10)	(12,9)	(10,6)	(8,6)
(5,2)	(5,2)	(5,11)	(9,3)	(3,11)	O	(9,10)	(10,7)	(8,7)	(3,2)	(8,6)	(12,4)	(12,9)	(10,6)
(5,11)	(5,11)	(9,10)	(5,2)	O	(3,2)	(10,6)	(9,3)	(3,11)	(8,6)	(12,9)	(8,7)	(10,7)	(12,4)
(8,6)	(8,6)	(12,9)	(3,2)	(9,10)	(10,6)	(10,7)	O	(5,11)	(12,4)	(8,7)	(5,2)	(3,11)	(9,3)
(8,7)	(8,7)	(3,11)	(12,4)	(10,7)	(9,3)	O	(10,6)	(12,9)	(5,2)	(5,11)	(8,6)	(9,10)	(3,2)
(9,3)	(9,3)	(5,2)	(10,7)	(8,7)	(3,11)	(5,11)	(12,9)	(12,4)	O	(3,2)	(10,6)	(8,6)	(9,10)
(9, 10)	(9,10)	(10,6)	(5,11)	(3,2)	(8,6)	(12,4)	(5,2)	O	(12,9)	(10,7)	(3,11)	(9,3)	(8,7)
(10,6)	(10,6)	(12,4)	(9,10)	(8,6)	(12,9)	(8,7)	(5,11)	(3,2)	(10,7)	(9,3)	O	(5,2)	(3,11)
(10,7)	(10,7)	(9,3)	(12,9)	(12,4)	(8,7)	(5,2)	(8,6)	(10,6)	(3,11)	O	(9,10)	(3,2)	(5,11)
(12, 4)	(12,4)	(8,7)	(10,6)	(12,9)	(10,7)	(3,11)	(9,10)	(8,6)	(9,3)	(5,2)	(3,2)	(5,11)	O
(12, 9)	(12,9)	(10,7)	(8,6)	(10,6)	(12,4)	(9,3)	(3,2)	(9,10)	(8,7)	(3,11)	(5,11)	O	(5,2)

Figura 11: Somas dos pontos da curva $x^3 + 3x + 7$ em $\mathbb{Z}_{13}$.

5 Criptografia

5.1 Um brevíssima história da criptografia

Criptografia (do grego *escrita escondida*) é o estudo das técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário correto. Existem vários tipos de criptografia, mas, em geral, a ideia é que se você tem uma mensagem que quer enviar a outra pessoa e não quer que seja lida por pessoas indevidas, você deve protegê-la com uma chave e só quem também tiver uma chave poderá recuperar a mensagem. É como se você estivesse colocando a mensagem dentro de um baú que só pode ser aberto por quem tiver a chave. Porém, não estamos falando fisicamente de baús e chaves: estamos falando sobre usar a matemática para mudar essa mensagem de forma que outra pessoa também precise usar matemática para lê-la.

Figura 12: Esquema da criptografia.

Um dos exemplos mais antigos e duradouro é a criptografia de substituição. Nesse tipo de criptografia, trocamos cada letra do alfabeto por outra letra, de forma a embaralhar a mensagem para que a pessoa que a receba a desembaralhe usando as trocas inversas. Um das mais famosas criptografias de substituição foi usada por Julio Cesar, o imperador romano. Diz-se que César costumava "andar" com o alfabeto algumas unidades para a direita para fazer essas trocas.

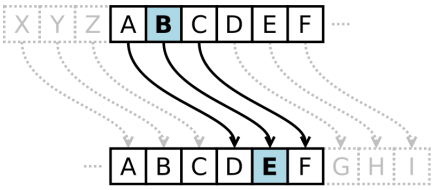


Figura 13: Exemplo de criptografia de César.

Por exemplo, na figura, andamos 3 letras: A $\rightarrow$ D, B $\rightarrow$ E, C $\rightarrow$ F, ... e quando o alfabeto acaba, ou seja, quando W $\rightarrow$ Z, voltamos pro início: X $\rightarrow$ A, Y $\rightarrow$ B, Z$\rightarrow$ C. Usando essas trocas, fazemos um exemplo. A pessoa que receber a mensagem cifrada (ou codificada) deve apenas usar a troca inversa para ler. Assim, a pessoa que recebe a mensagem precisa saber qual foi a troca que a pessoa que enviou a mensagem fez. A chave secreta no caso é quantas posições o alfabeto andou. A ideia é que uma pessoa que intercepte a mensagem indevidamente e não saiba qual foi a troca feita, não saberá ler a mensagem. Porém, isso não é totalmente verdade... Primeiro: se sabemos que o alfabeto apenas andou, então podemos fazer todas as possibilidades e encontrar a mensagem (é só um pouco trabalhoso). Além disso, ao longo do tempo, a linguistica trouxe informações sobre a frequência das letras e de algumas palavras em cada língua, fazendo com que fosse possível analisar mensagens codificadas, mesmo com trocas que não fossem simplesmente andar com o alfabeto, para tentar encontrar a mensagem original.

O impressionante é que, mesmo com tudo isso, as criptografias de substituição sobreviveram muitos séculos como a codificação mais usada no mundo: desde Júlio César (há mais de 2000 anos) até a 2ª Guerra Mundial (1939 a 1945). Nessa guerra, os alemãs usaram uma máquina de codificar chamada Enigma, que quase os tornou invencíveis. A ideia da máquina é, a cada letra digitada em seu teclado são feitas dezenas de substituições, como se fosse feita a criptografia de César diversas vezes com mudanças diferentes em cada uma das letras digitadas. Assim, a mensagem se tornava praticamente indecifrável. A Inglaterra formou então uma equipe multidisciplinar, contando com matemáticos, engenheiros, linguistas, entre outros, para tentar decifrar o funcionamento da máquina e decodificar de vez as mensagens. Dessa equipe, fazia parte Alan Turing, que, por volta de 1942, propôs a máquina que, enfim, decifraria a Enigma e, hoje em dia, é considerada o primeiro computador, bisavô dos computadores que usamos hoje. Com isso, veio a necessidade de procurar por outras formas para proteger as informações.

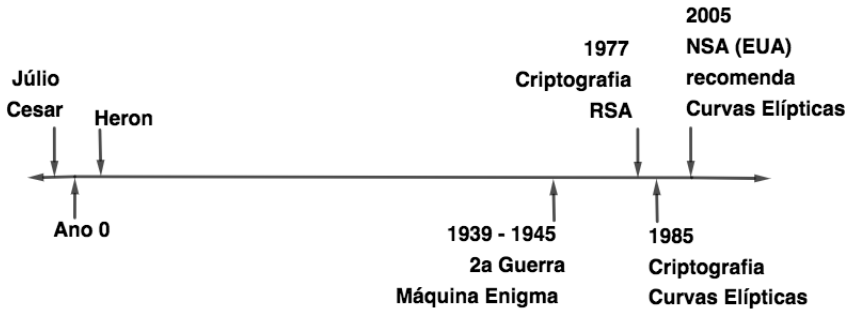


Figura 14: Linha do tempo.

Em 1977, Rivest, Shamir e Adleman, propuseram o sistema de criptografia RSA, considerado a mais bem sucedida implementação de criptografia na questão de segurança e ainda utilizado por bancos,

trocas de e-mails, compras online, entre outros. O RSA utiliza um par de chaves: uma pública e outra privada (que só é conhecida pelo remetente e destinatário da mensagem) e está baseado na Teoria dos Números: utiliza o fato de que fatorar números muito grandes é computacionalmente difícil. Você pode consultar a apostila do PIC (referência [2]) para saber mais sobre esse tipo e criptografia. Vamos dar apenas uma ideia rápida.

Se A quer enviar uma mensagem para B, o primeiro a ser feito é escolher dois números primos p e q grandes (da ordem de 100^{10}, por exemplo), a chave secreta é o par p, q. Em seguida, é necessário calcular $n = pq$, essa será a chave pública. Se A tem uma mensagem b já passada para números (usando por exemplo a tabela que veremos na figura 15), deve codificar a mensagem fazendo

$$C(b) = \text{o resto da divisão de} b^3 \text{ por } n$$

Ou seja, $C(b) \equiv b^3 \pmod{n}$. Em geral, esse número ao qual A eleva b não precisa (nem deve) ser 3, utilizamos aqui apenas para não entrar nessa discussão. Então, A envia a mensagem para B, que pode decodificá-la usando um número d que satisfaça

$$3d \equiv 1 \pmod{(p-1)(q-1)}$$

e calculando

$$D(C(b)) = \text{o resto da divisão de } (C(b))^d \text{ por } n$$

Você pode tentar mostrar porque esse processo funciona.

Embora o RSA tenha sido implementado com enorme sucesso, sua eficiência pode ser ameaçada pelo desenvolvimento cada vez mais veloz da informática. Assim, continuou-se a estudar novos algoritmos de criptografia. Em 1985, foi proposta a utilização teórica de curvas elípticas em criptografia. A utilização de fato ainda levou alguns anos, porém, um marco para a área foi o fato de, em 2005, a agência nacional de segurança dos EUA ter emitido uma recomendação de que empresas migrassem da criptografia RSA para a criptografia de curvas elípticas. Vamos ver a seguir como essa criptografia funciona.

5.2 Criptografia sobre curvas elípticas

Para que duas pessoas A e B troquem informações criptografadas usando curvas elípticas, devem começar escolhendo uma curva

$$y^2 = x^3 + ax + b$$

sobre um corpo $\mathbb{Z}_p$ e um ponto P nessa curva. Nesse sistema, tanto a curva quanto o ponto são chaves públicas, ou seja, podem ser conhecidos por todos, não só pelas duas pessoas.

Há duas chaves privadas m e n, números inteiros positivos, cada um escolhido por uma das pessoas em particular, mas não compartilhados com ninguém (nem um com o outro). A pessoa A calcula $Q = nP$ e envia para B. Já a pessoa B calcula $R = mP$ e envia para A. Notamos que:

$$mQ = mnP = nmP = nR$$

Esse ponto $S = mQ = nR$ é a chave secreta comum do sistema, que só os dois sabem, mesmo que alguém saiba Q e/ou P. Ela será usada para decodificar a mensagem pela pessoa que a recebe.

A codificação da mensagem se dá da seguinte forma: tendo uma mensagem em forma de ponto M da curva, o remetente faz a soma

$$C(M) = M \oplus S$$

e envia ao destinatário. Por sua vez, esse pode decodificar fazendo

$$C(M) \oplus (-S) = M$$

Resumimos o processo nos passos a seguir:

- A e B escolhem a curva e um ponto P, são as chaves públicas;
- A escolhe n e calcula nP, envia nP para B;
- B escolhe m e calcula mP, envia nP para A;
- Ambos calculam $S = nmP$;
- A codifica a mensagem M fazendo $C(M) = M \oplus S$, envia para B;
- B decodifica a mensagem fazendo $C(M) \oplus -S = M$.

Vamos ver um exemplo na curva que usamos na seção 3: $y^2 = x^3 + 3x + 7$ sobre $\mathbb{Z}_{13}$. Digamos que A e B tenham escolhido o ponto $P = (12, 9)$ e que A e B tenham escolhido, respectivamente, $n = 5$ e $m = 7$. Usando a tabela 11, verificamos que:

$$\begin{aligned}
2P &= P \oplus P = (12,9) \oplus (12,9) = (5,2) \\
3P &= P \oplus 2P = (12,9) \oplus (5,2) = (10,6) \\
4P &= P \oplus 3P = (12,9) \oplus (10,6) = (3,11) \\
5P &= P \oplus 4P = (12,9) \oplus (3,11) = (8,6) \\
6P &= P \oplus 5P = (12,9) \oplus (8,6) = (9,3) \\
7P &= P \oplus 6P = (12,9) \oplus (9,3) = (9,10)
\end{aligned}$$

Dessa forma, as chaves secretas de A e B, respectivamente, são

$$nP = 5P = (8,6) \qquad \text{e} \qquad mP = 7P = (9,10)$$

A chave secreta comum é então

$$S = nmP = 5(9,10) = (3,2)$$

Um problema agora é: se A quer enviar uma mensagem a B, como pode transformá-la em um ponto da curva? Uma forma simples de fazer isso é transformar a mensagem em um número usando uma tabela comum e, em seguida, usar uma outra tabela para associar cada algarismo a um ponto da curva.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Figura 15: Tabela que associa cada letra a um número.

Algarismo	0	1	2	3	4	5	6	7	8	9
Ponto	(3,2)	(3,11)	(5,2)	(5,11)	(8,6)	(8,7)	(9,3)	(9,10)	(10,6)	(10,7)

Figura 16: Tabela que associa cada algarismo a um ponto da curva.

Por exemplo, digamos que a mensagem seja um simples *OI*. Pela tabela da figuraa 15, temos o número 2418. Cada um desses algarismos é um ponto pela tabela da figura 16:

$$M_1 = (5,2),\ M_2 = (8,6),\ M_3 = (3,11),\ M_4 = (10,6)$$

O remetente A terá que codificar cada um desses pontos. Por exemplo, para codificar $M_4 = (10,6)$, fazemos:

$$C(M_4) = (10,6) \oplus (3,2) = (12,4)$$

Recebendo os 4 pontos codificados, a pessoa B vai decodificá-los fazendo, por exemplo:

$$(12,4) \oplus -(3,2) = (12,4) \oplus (3,11) = (10,6) = M_4\,,$$

onde usamos que $-(3,2) = (3,11)$ pois $-2 \equiv 11 \pmod{13}$. É importante lembrar que todas as contas são módulo 13 e que apresentamos na seção 3 uma tabela com as somas dos pontos dessa curva $y^2 = x^3+3x+7$ em $\mathbb{Z}_{13}$.

O problema de quebrar uma mensagem criptografada usando curvas elípticas, chamado problema do logaritmo discreto, é mais difícil. A ideia é que conhecendo a curva e o ponto P escolhidos, pois são públicos, e, além disso, conhecendo interceptar $Q = nP$, deva-se descobrir n. Aqui fizemos uma abordagem ingênua, em que calculamos todos os pontos da curva e todas as somas entre eles (figura 11). É claro, no entanto, que nosso exemplo é simples porque estamos trabalhando com um corpo $\mathbb{Z}_{13}$ pequeno e com n e m pequenos. Assim, uma pessoa mal intencionada poderia muito bem calcular o mesmo que fizemos e decodificar a mensagem sem ser seu destinatário oficial, caso a interceptasse. Em geral, o conjunto $\mathbb{Z}_n$ usado será bem maior, o que dificultará esse processo para o invasor.

Uma desvantagem é que realizar as soma de pontos em curvas elípticas é um processo mais lento do que efetuar a exponenciação módulo um primo, que é a operação utilizada nos sistemas tradicionais, além disso, a implementação é mais complicada. No entanto, devido a sua maior segurança e também ao fato de poder usar menos *bits* para guardar uma informação, parece ser, atualmente, a melhor escolha para criptografar infomações de forma mais segura.

6 Exercícios

Listamos a seguir alguns exercícios para que você coloque em prática o que aprendeu nesse testo.

1. Utilize as propriedades de congruência para encontrar os restos da divisão de

   (a) 2^{20} por 3 e por 8. (b) 3^{20} por 8 e por 8. (c) $2^{20} + 3^{10}$ por 24.

2. Usando o que foi visto na seção 1, determine a curva que representa a família de de triângulos com mesma área e perímetro do triângulo pitagórico de lados 5, 12, 13. Em seguida, encontre algum ponto da curva obtida que represente esse triângulo.

3. Volte à curva $y^2 = x^3 - 5x + 4$ (fim da página 7).
   (a) Calcule gometricamente a soma dos pontos $P = (1, 0)$ e $Q = (0, 2)$.
   (b) Calcule algebricamente a soma dos pontos $Q = (0, 2)$ e $S = (3, 4)$.
4. Considere a curva $y^2 = x^3 + 9x + 17$ sobre $\mathbb{Z}_{23}$. Não esqueça que todas as contas são módulo 23.
   (a) Calcule y^2 para todos os 23 valores $y \in \mathbb{Z}_{23}$.
   (b) Confira que o ponto $P = (16, 5)$ pertence à essa curva.
   (c) Usando o item (a), encontre os dois pontos Q_1 e Q_2 da curva que têm $x = 1$.
   (d) Calcule as somas $P \oplus Q_1$ e $P \oplus Q_2$.

Referências

[1] Bill McCallum, *A tale of two triangles: Heron triangles and elliptic curves*, Blog do Projeto Klein, disponível em `http://blog.kleinproject.org/?p=4` (acessado em 09/11/18)

[2] Severino Collier Coutinho, *Apostila 7: Criptografia*, Programa de Iniciação Científica da OBMEP, disponível em `http://www.obmep.org.br/docs/apostila7.pdf` (acessado em 09/11/18)

[3] Maria Cristina Antunes Lana, *Curvas Elípticas e Criptografia*, Dissertação de Mestrado - PROFMAT. Disponível em `https://repositorio.ufjf.br/jspui/handle/ufjf/4044` (acessado em 09/11/18)