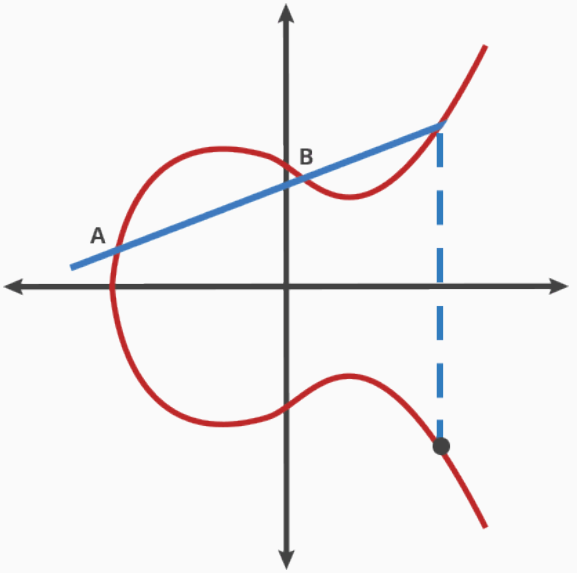
Criptografia:
o que o Heron tem a ver com isso?

Beatriz Motta
Universidade Federal de Juiz de Fora

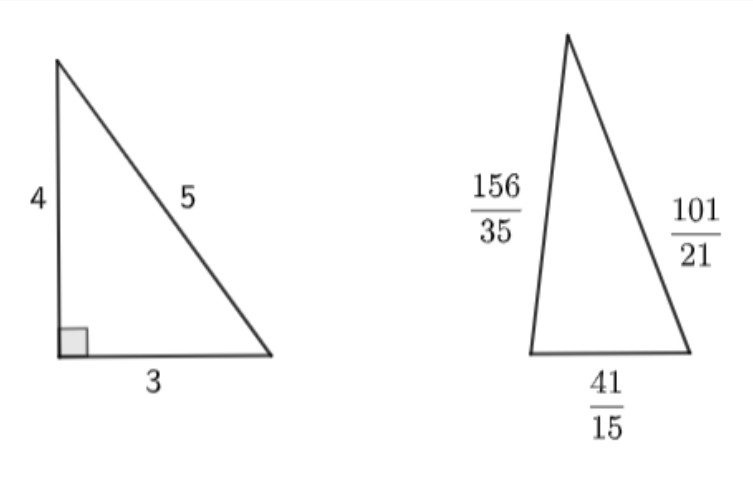
21 de novembro de 2018

OU: Como uma ideia do século I se relaciona com a segurança de dados no século XXI?



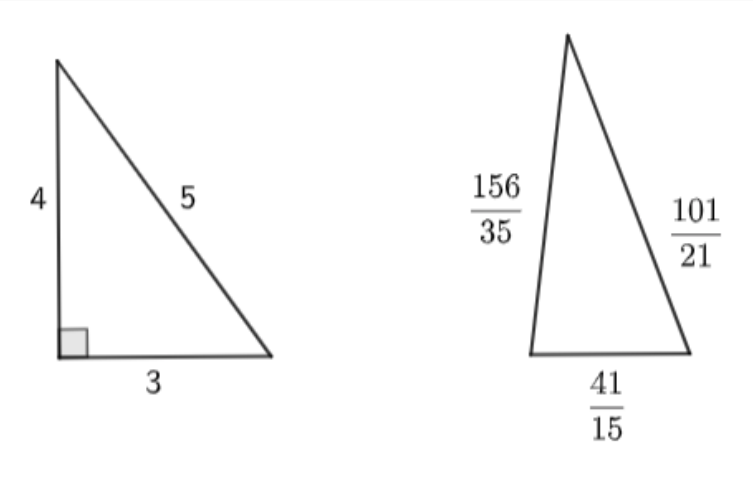
Parte 1: Um problema muito antigo

Os dois triângulos abaixo têm o mesmo perímetro:



$3+4+5=12$ e

$$\frac{41}{15}+\frac{101}{21}+\frac{156}{35}=\frac{287+505+468}{105}=12$$



Os triângulos têm também a mesma área!

Fórmula de Heron:

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

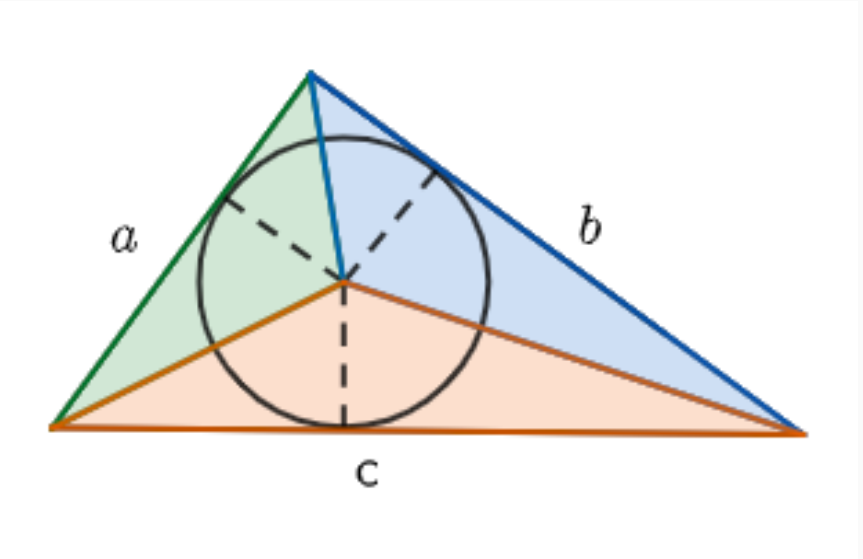
a, b, c são as medidas dos lados do triângulo

$s = \frac{1}{2}(a+b+c)$ é o semiperímetro.

Problema:

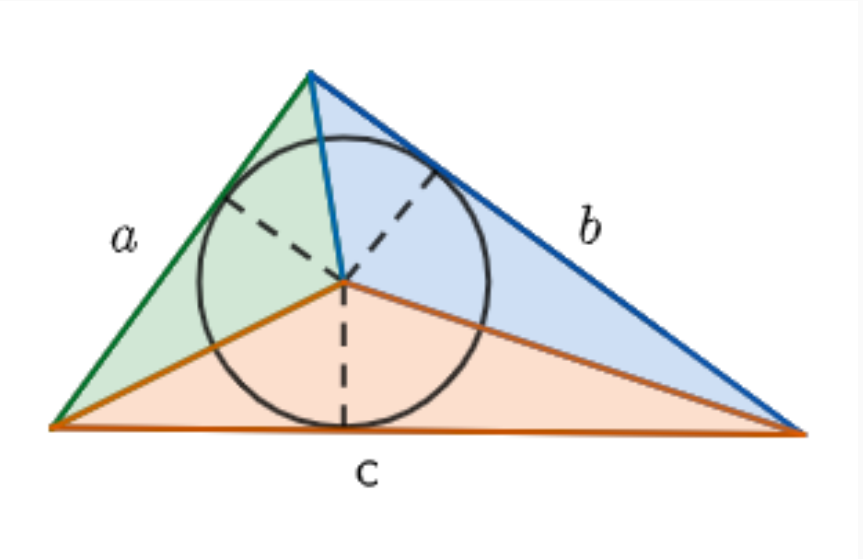
como encontrar mais triângulos com a mesma área e o mesmo perímetro?

Todo triângulo de lados a, b, c tem um círculo de raio r inscrito:



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

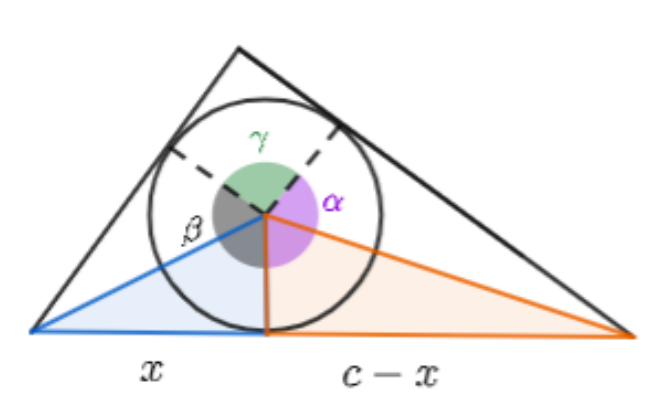
Todo triângulo de lados a, b, c tem um círculo de raio r inscrito:



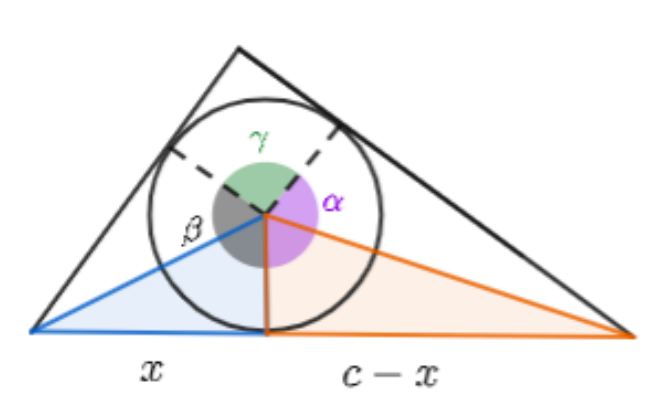
$$A = A_{\text{verde}} + A_{\text{azul}} + A_{\text{laranja}} = \frac{ar}{2} + \frac{br}{2} + \frac{cr}{2} = r\,\frac{a+b+c}{2} = rs$$

Logo, todo triângulo de mesma área e mesmo perímetro tem o círculo inscrito de mesmo raio.

Considerando os ângulos α, β, γ:

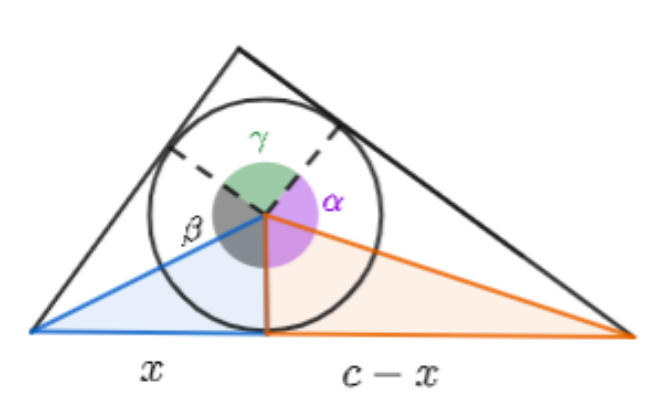


Considerando os ângulos α, β, γ:



Usando o triângulo azul: $\text{tg}\left(\frac{\beta}{2}\right) = \frac{x}{r}$.

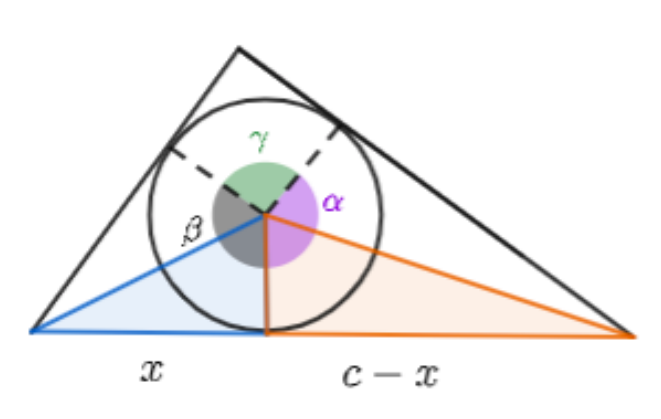
Considerando os ângulos α, β, γ:



Usando o triângulo azul: $\text{tg}\left(\frac{\beta}{2}\right) = \frac{x}{r}$.

Usando o triângulo laranja: $\text{tg}\left(\frac{\alpha}{2}\right) = \frac{c-x}{r}$.

Considerando os ângulos α, β, γ:



Usando o triângulo azul: $\text{tg}\left(\frac{\beta}{2}\right) = \frac{x}{r}$.

Usando o triângulo laranja: $\text{tg}\left(\frac{\alpha}{2}\right) = \frac{c-x}{r}$.

Assim: $c = r\left(\text{tg}\left(\frac{\beta}{2}\right) + \text{tg}\left(\frac{\alpha}{2}\right)\right)$

Fazendo isso para os demais triângulos:

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

Fazendo isso para os demais triângulos:

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

Juntando as duas fórmulas:

$$A = rs \quad \text{e} \quad s = r\left(\text{tg}\left(\frac{\beta}{2}\right) + \text{tg}\left(\frac{\alpha}{2}\right) + \text{tg}\left(\frac{\gamma}{2}\right)\right)$$

Fazendo isso para os demais triângulos:

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

Juntando as duas fórmulas:

$$A = rs \quad \text{e} \quad s = r\left(\operatorname{tg}\left(\frac{\beta}{2}\right) + \operatorname{tg}\left(\frac{\alpha}{2}\right) + \operatorname{tg}\left(\frac{\gamma}{2}\right)\right)$$

Temos:

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

Chamando de x, y, z as tangentes e usando um pouco de trigonometria, temos:

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

Como $\frac{s^2}{A}$ é uma constante k, reescrevemos:

$$x^2y + xy^2 = kxy - k$$

Uma curva muito interessante

A equação

$$x^2y + xy^2 = kxy - k$$

define uma *curva* no plano cartesiano cada vez que fixamos um k.

Uma curva muito interessante

A equação

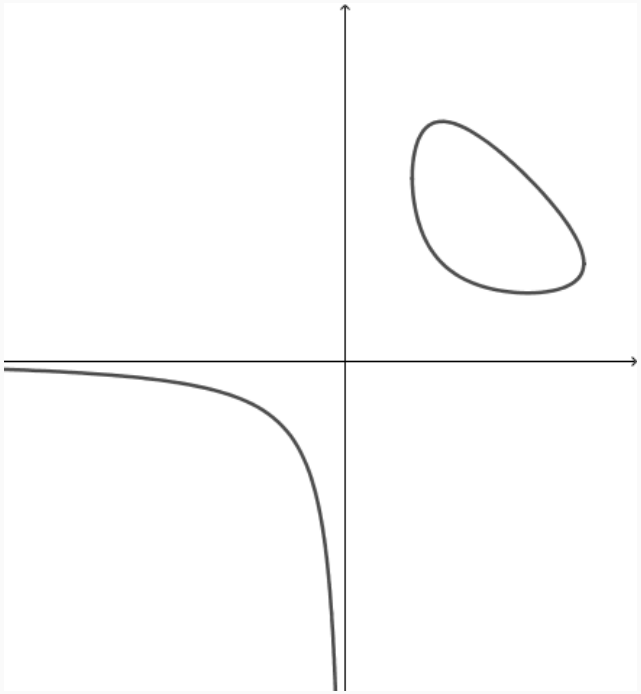
$$x^2y + xy^2 = kxy - k$$

define uma *curva* no plano cartesiano cada vez que fixamos um k.

- Cada triângulo de área A e semiperímetro s é um *ponto* na curva com $k = \frac{s^2}{A}$.
- Cada ponto da curva, em uma certa parte do plano, é um triângulo com mesma área e semiperímetro.

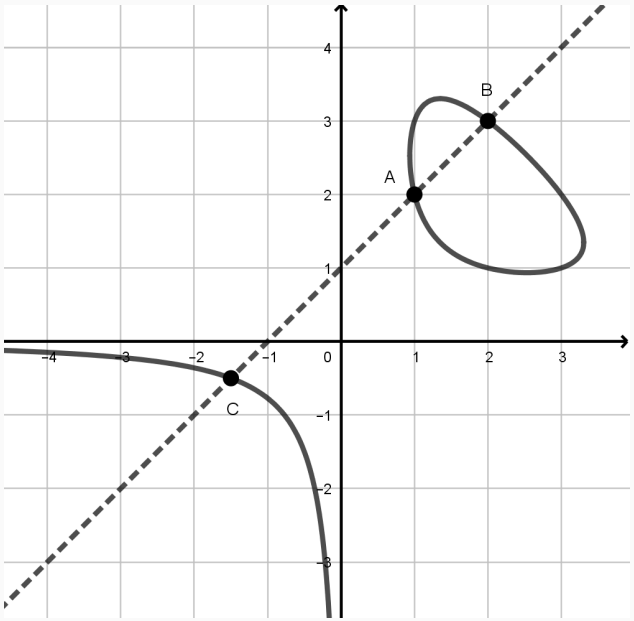
A curva que parametriza a família de triângulos que inclui os dois que vimos, isto é, com área 6 e semiperímetro também 6 é

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



Encontrando pontos em uma curva

Dados dois pontos *A* e *B* em uma curva elíptica, traçando a reta secante à curva definida por tais pontos, encontramos mais um ponto na curva.



Um exemplo com a curva

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

e os pontos

$A = (1, 2)$ e $B = (2, 3)$.

Encontrar as coordenadas desse novo ponto depende das coordenadas de *A* e *B*.

Considerando então a curva $x^2y + xy^2 = 6xy - 6$ e os pontos $A = (1, 2)$ e $B = (2, 3)$ devemos resolver:

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

ou seja, devemos encontrar a terceira raiz de

$$2x^3 - 3x^2 - 5x + 6 = 0\,.$$

Considerando então a curva $x^2y + xy^2 = 6xy - 6$ e os pontos $A = (1, 2)$ e $B = (2, 3)$ devemos resolver:

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

ou seja, devemos encontrar a terceira raiz de

$$2x^3 - 3x^2 - 5x + 6 = 0\,.$$

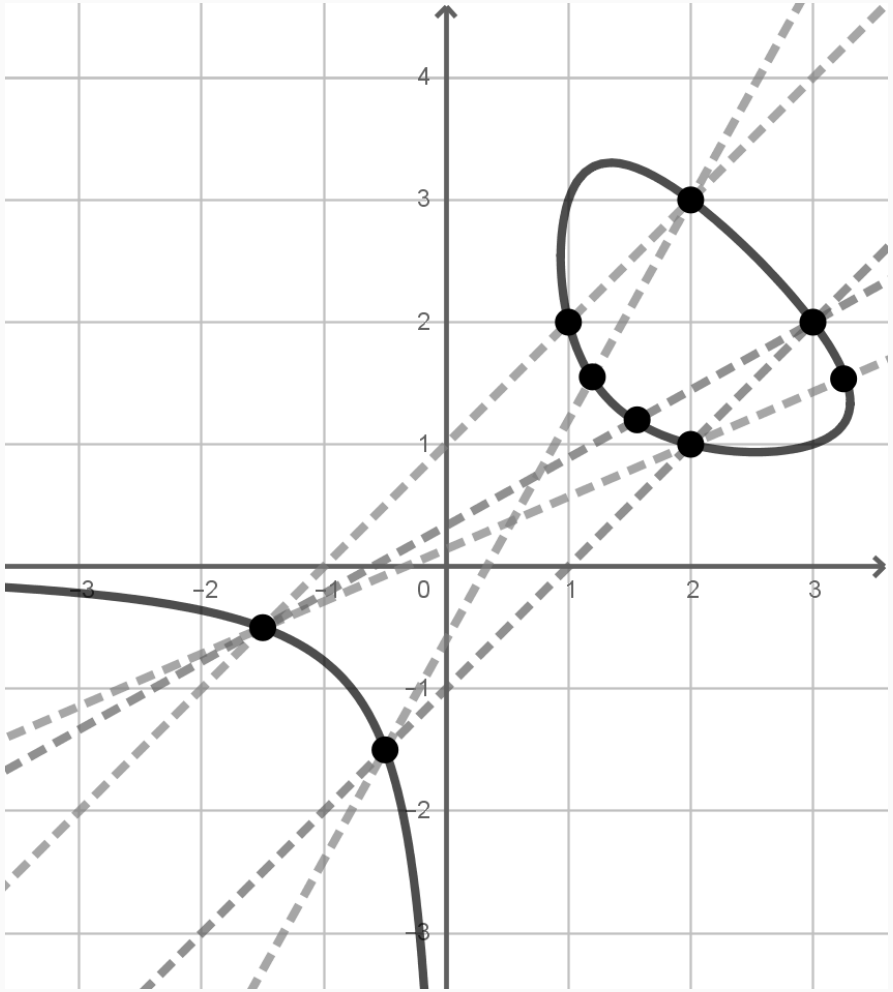
Como

$$2x^3 - 3x^2 - 5x + 6 = (x - 1)(x - 2)(2x + 3)\,,$$

concluimos que o terceiro ponto é $C = (-3/2, -1/2)$.

Repetindo esse processo, podemos encontrar infinitos pontos com coordenadas racionais na curva

$$x^2y + xy^2 = 6xy - 6\,.$$

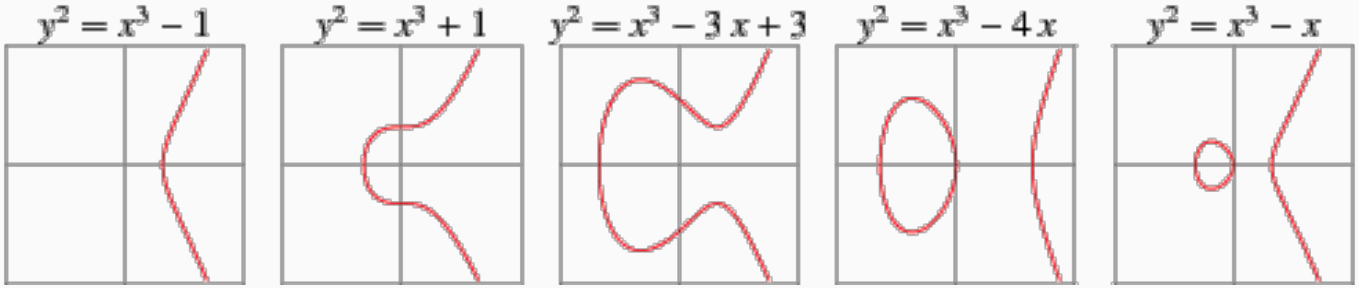


Curvas Elípticas

Essas curvas que parametrizam famílias de triângulos fazem parte de uma família maior chamada

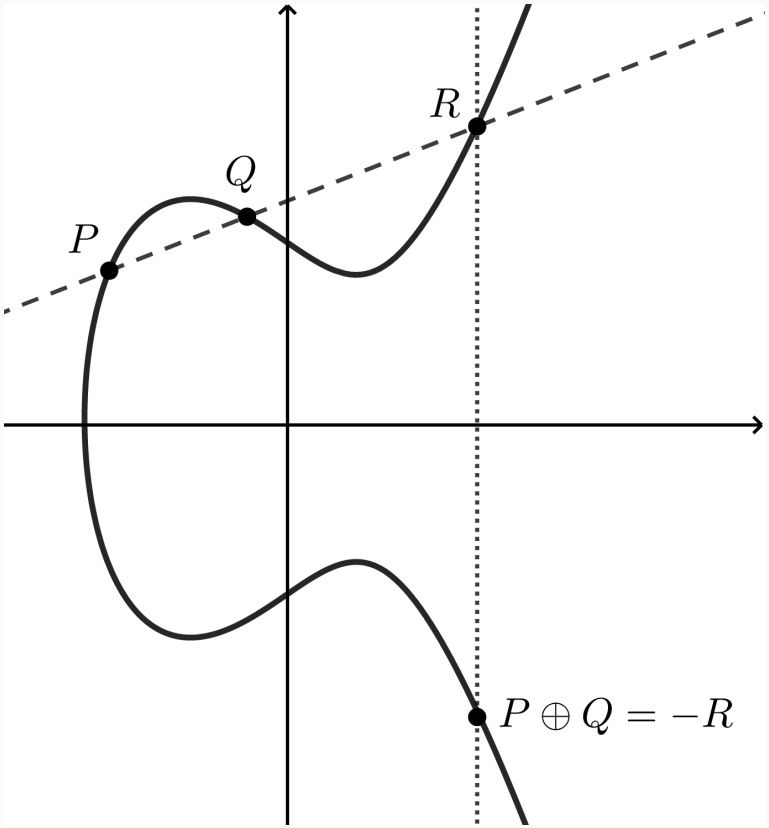
Curvas Elípticas

$$y^2 = x^3 + ax + b, \text{ onde } 4a^3 + 27b^2 \neq 0$$



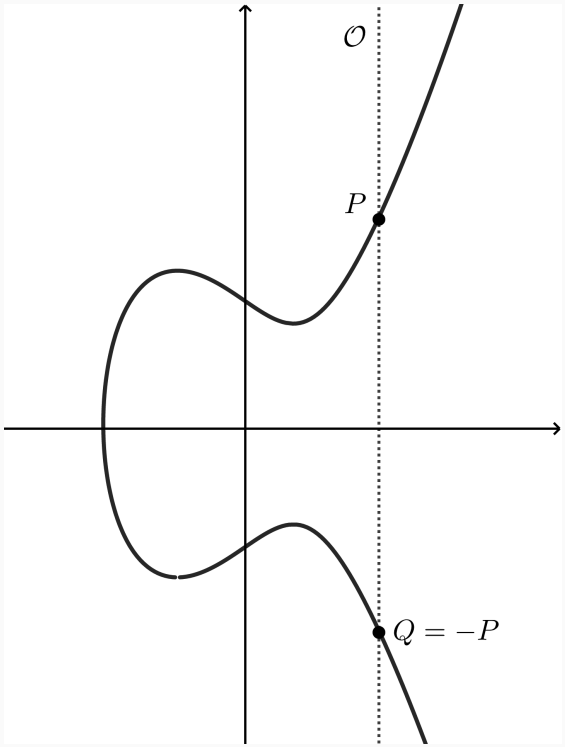
Uma operação entre pontos

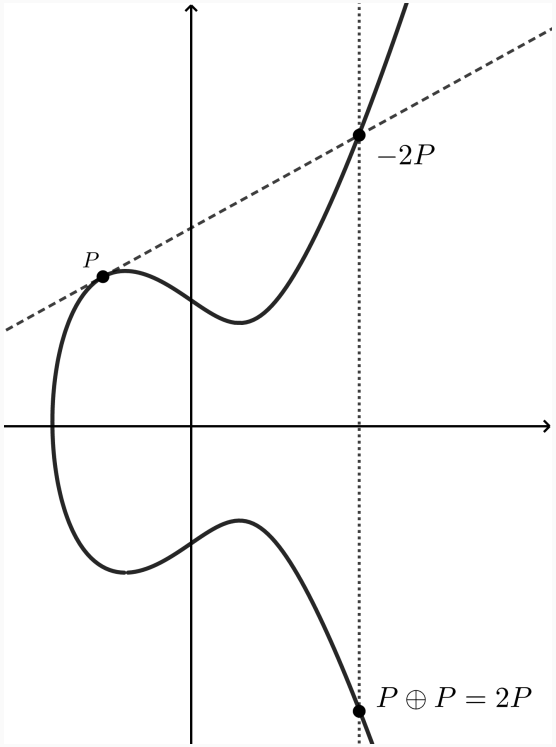
A definição de uma operação entre pontos de uma curva elíptica é dada geometricamente.



Uma operação entre pontos

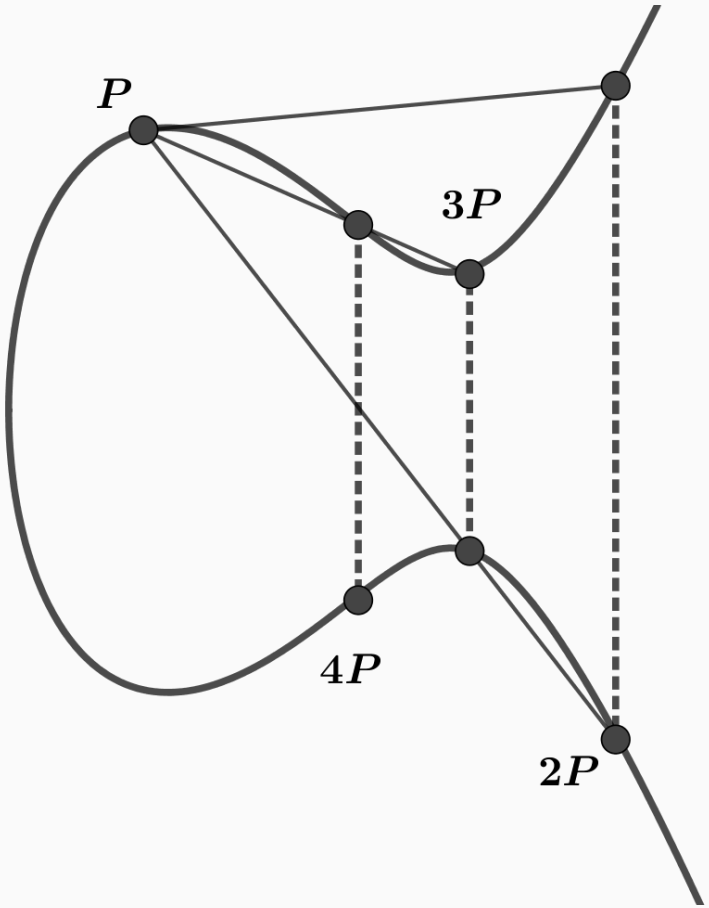
Outros casos:





Uma operação entre pontos

Na figura a seguir, vemos a soma de um ponto *P* com *P* algumas vezes:



Uma operação entre pontos

A operação assim definida satisfaz tudo que esperamos de uma operação:

Comutativa: $P \oplus Q = Q \oplus P$

Elemento neutro: $P \oplus \mathcal{O} = P$

Elemento inverso: $P \oplus (-P) = \mathcal{O}$

Associativa: $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$

Uma operação entre pontos

Existe uma fórmula!

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

Sejam $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ na curva, com $P \neq -Q$.

Uma operação entre pontos

Existe uma fórmula!

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

Sejam $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ na curva, com $P \neq -Q$.

Seja $m = \dfrac{y_1 - y_2}{x_1 - x_2}$.

Uma operação entre pontos

Existe uma fórmula!

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

Sejam $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ na curva, com $P \neq -Q$.

Seja $m = \dfrac{y_1 - y_2}{x_1 - x_2}$.

Temos que $P \oplus Q = (x, y)$ tem coordenadas

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

Uma operação entre pontos

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

Para a soma de um ponto $P = (x_1, y_1)$ com ele mesmo, definimos

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

Temos que $2P = P \oplus P = (x, y)$ tem coordenadas

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

Parte 2: Aritmética modular

Uma pergunta simples: se agora o relógio marcar 3 horas, após 10 horas, onde estará o ponteiro?

Sejam $a, b, c \in \mathbb{Z}$, $n \geq 2$.

Vamos 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

Exemplos

Na divisão de 25 por 4, temos $25 = 4 \times 6 + 1$. Assim:

$$25 \equiv 1 \pmod{4}$$

Na divisão de 345 por 7, temos $345 = 7 \times 49 + 2$. Assim:

$$345 \equiv 2 \pmod{7}$$

Na divisão de 1000 por 4, temos $1000 = 4 \times 250 + 0$. Assim:

$$1000 \equiv 0 \pmod{4}$$

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

$$a \equiv b \pmod{n} \text{ e } c \equiv d \pmod{n}$$

$$\Rightarrow a + c \equiv b + d \pmod{n} \text{ e } ac \equiv bd \pmod{n}$$

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

$$a \equiv b \pmod{n} \text{ e } c \equiv d \pmod{n}$$

$$\Rightarrow a + c \equiv b + d \pmod{n} \text{ e } ac \equiv bd \pmod{n}$$

Em particular:

$$a \equiv b \pmod{n} \text{ e } r \geq 2 \Rightarrow a^r \equiv b^r \pmod{n}$$

Exemplo

Qual é o algarismo das unidades de 3^{2019} ?

Vamos começar com:

$$3^2 \equiv -1 \pmod{10}$$

Exemplo

Qual é o algarismo das unidades de 3^{2019} ?

Vamos começar com:

$$3^2 \equiv -1 \pmod{10}$$

$$(3^2)^{1009} \equiv (-1)^{1009} \pmod{10}$$

$$3^{2018} \equiv -1 \pmod{10}$$

Exemplo

Qual é o algarismo das unidades de 3^{2019} ?

Vamos começar com:

$$3^2 \equiv -1 \pmod{10}$$

$$(3^2)^{1009} \equiv (-1)^{1009} \pmod{10}$$

$$3^{2018} \equiv -1 \pmod{10}$$

Portanto:

$$3^{2019} \equiv 3^{2018} \cdot 3 \equiv -1 \cdot 3 \equiv -3 \equiv 7 \pmod{10}$$

O conjunto $\mathbb{Z}_n$

Vamos denotar por $\mathbb{Z}_n$ o conjunto dos restos possíveis na divisão de um inteiro qualquer por n:

$$\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$$

O conjunto $\mathbb{Z}_n$

Nesse conjunto, vamos fazer operações módulo *n*, por exemplo:

$$4 + 2 = 0 \text{ em } \mathbb{Z}_6$$

$$4 + 2 = 1 \text{ em } \mathbb{Z}_5$$

$$4 \cdot 2 = 2 \text{ em } \mathbb{Z}_6$$

$$4 \cdot 2 = 3 \text{ em } \mathbb{Z}_5$$

Exemplo

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

$\cdot$	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

Curvas elípticas 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 e os elementos dos pares (x, y) dentro de um conjunto $\mathbb{Z}_p$ de restos na divisão por um número primo p.

Nesse caso, usando a aritmética modular, podemos encontrar todos os pontos da curva.

Exemplo

$$y^2 = x^3 + 3x + 7 \text{ sobre } \mathbb{Z}_{13}$$

Substituimos cada um dos valores $0, 1, \ldots, 12$ em x.

Verificamos se o número obtido é um quadrado perfeito em $\mathbb{Z}_{13}$.

$x = 0 \Rightarrow x^3 + 3x + 7 = 7$ que não é um quadrado perfeito.

$x = 10 \Rightarrow x^3 + 3x + 7 = 1037$, que é $10 = 6^2$ em $\mathbb{Z}_{13}$.

Exemplo

Repetindo para todos os valores possíveis de *x*:

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

Exemplo

Repetindo para todos os valores possíveis de *x*:

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

Só são quadrados:

$$3 \equiv 4^2 \equiv 9^2 \pmod{13} \qquad 9 \equiv 3^2 \equiv 10^2 \pmod{13}$$
$$4 \equiv 2^2 \equiv 11^2 \pmod{13} \qquad 10 \equiv 7^2 \equiv 6^2 \pmod{13}$$

Exemplo

Repetindo para todos os valores possíveis de *x*:

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

Só são quadrados:

$$3 \equiv 4^2 \equiv 9^2 \pmod{13} \qquad 9 \equiv 3^2 \equiv 10^2 \pmod{13}$$
$$4 \equiv 2^2 \equiv 11^2 \pmod{13} \qquad 10 \equiv 7^2 \equiv 6^2 \pmod{13}$$

Todos os pontos da curva $y^2 = x^3 + 3x + 7$:

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

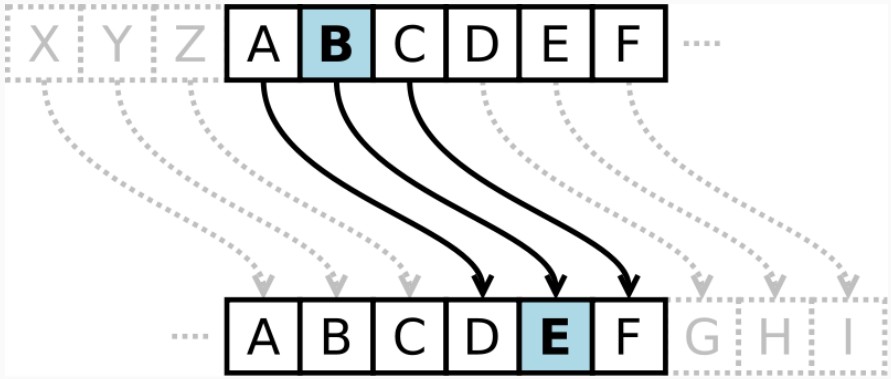
Ainda podemos usar a fórmula de soma de pontos.

$\oplus$	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)

Parte 3: Criptografia

Criptografia de César

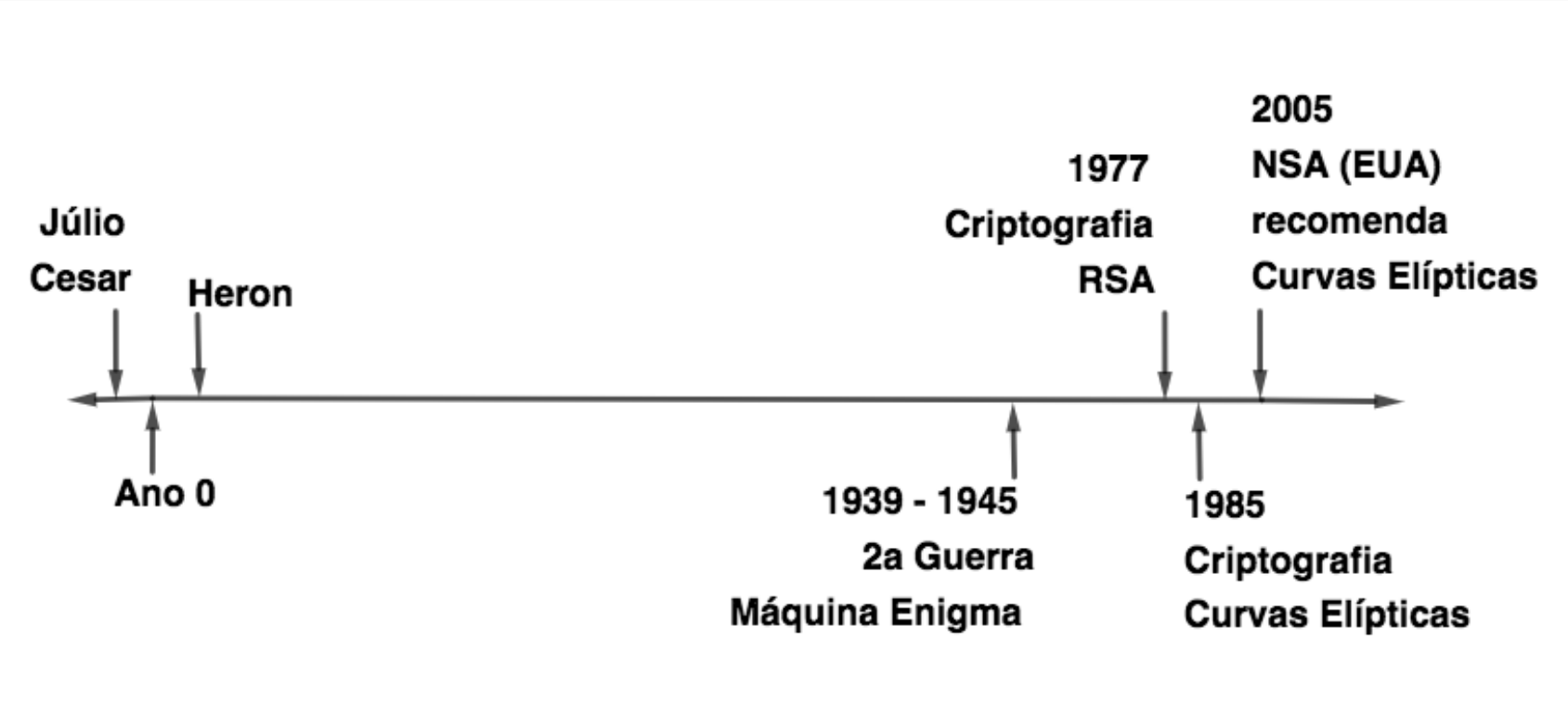
Nesse tipo de criptografia, cada letra do texto é substituída por outra, por exemplo:

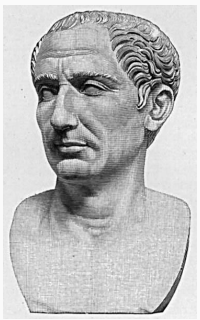


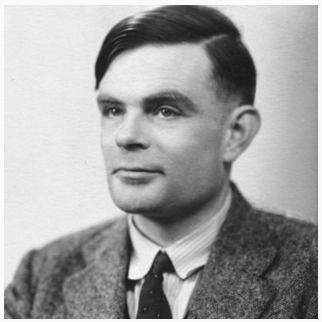
Nesse caso, poderíamos codificar:

```
Normal:  a ligeira raposa marrom saltou sobre o cachorro cansado
Cifrado: D OLJHLUD UDSRVD PDUURP VDOWRX VREUH R FDFKRUUR FDQVDGR
```

Embora simples, a criptografia de César sobreviveu, com algumas mudanças, muitos séculos.







Criptografia sobre curvas elípticas

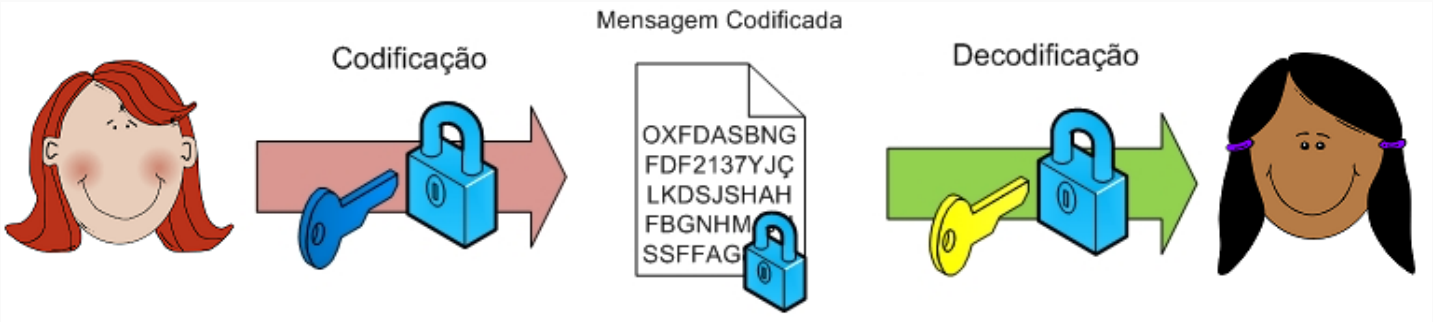
Para entender como funciona a criptografia com Curvas Elípticas, primeiro precisamos transformar uma mensagem em um número. Para isso, usamos 99 para espaço e a tabela abaixo para letras:

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

Por exemplo, JF é o número 1915.

Digamos que Ana queira enviar a mensagem JF para Bruna.



É preciso associar a mensagem-número 1915 a um ponto de uma curva.

Por exemplo, na curva $y^2 = x^3 + 3x + 7$ sobre $\mathbb{Z}_{13}$, vamos usar:

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)

Assim, 1915 é

$$(3, 11)(10, 7)(3, 11)(8, 7)$$

O processo de codificação funciona da seguinte maneira:

- Ana e Bruna escolhem a curva e um ponto P (públicos);
- Ana escolhe n (secreto) e calcula nP;
- Bruna escolhe m (secreto) e calcula mP;
- Elas trocam nP e mP;
- Ambas calculam $S = n(mP) = m(nP)$ (secreto);
- Ana codifica a mensagem M fazendo $C(M) = M \oplus S$.

O processo de codificação funciona da seguinte maneira:

- Ana e Bruna escolhem a curva e um ponto P (públicos);
- Ana escolhe n (secreto) e calcula nP;
- Bruna escolhe m (secreto) e calcula mP;
- Elas trocam nP e mP;
- Ambas calculam $S = n(mP) = m(nP)$ (secreto);
- Ana codifica a mensagem M fazendo $C(M) = M \oplus S$.

Para ler, Bruna decodifica a mensagem fazendo

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

Exemplo

Voltamos à curva $y^2 = x^3 + 3x + 7$ sobre $\mathbb{Z}_{13}$ com o ponto $P = (12, 9)$.

Ana escolheu $n = 5$
Bruna escolheu $m = 7$

Exemplo

Voltamos à curva $y^2 = x^3 + 3x + 7$ sobre $\mathbb{Z}_{13}$ com o ponto $P = (12, 9)$.

Ana escolheu $n = 5$
Bruna escolheu $m = 7$

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

Exemplo

Voltamos à curva $y^2 = x^3 + 3x + 7$ sobre $\mathbb{Z}_{13}$ com o ponto $P = (12, 9)$.

Ana escolheu $n = 5$
Bruna escolheu $m = 7$

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

A chave secreta comum é então

$$S = n(mP) = 5(9,10) = (3,2)$$

A mensagem JF é dada pelos pontos

$$(3, 11)(10, 7)(3, 11)(8, 7)$$

Por exemplo, para codificar $M_4 = (8, 7)$, fazemos:

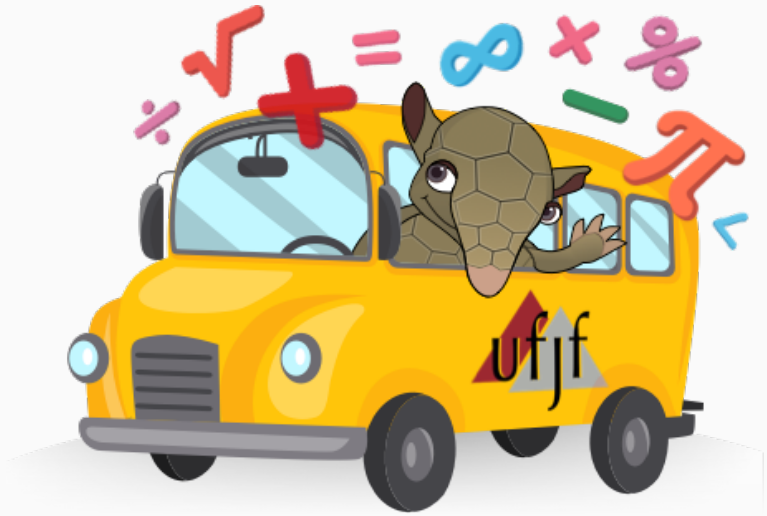
$$C(M_4) = (8, 7) \oplus (3, 2) = (3, 11)$$

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

$$(3, 11) \oplus -(3, 2) = (3, 11) \oplus (3, 11) = (8, 7) = M_4 \, ,$$

onde usamos que $-(3, 2) = (3, 11)$.

OBRIGADA



CARAVANA DA MATEMÁTICA