CiberSegurança
MEET, MEIC, MEIM

Criptografia com curvas elípticas (ECC)

2021–2022

INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

O protocolo de Diffie Hellman e a cifra de ElGamal estão baseados no **problema do logaritmo discreto** em $\mathbf{Z}_p$, isto é, na dificuldade de encontrar, a partir de α, β e p, um expoente a tal que

$$\alpha^a = \beta (\bmod p)$$

Este tipo de questão pode formular-se em qualquer conjunto G que tenha uma estrutura de **grupo**[1] e tal que

- dado $\alpha \in G$ e $a > 0$, o cálculo das potências α^a pode ser implementado de modo eficiente;
- dados $\alpha, \beta \in G$, o problema de calcular a tal que $\beta = \alpha^a$ é computacionalmente difícil.

[1] *G é um grupo se em G está definida uma operação interna associativa, com elemento neutro e com elemento inverso*

- As curvas elípticas, mais precisamente, o conjunto de pontos de uma curva elíptica sobre um corpo finito, admite uma estrutura de grupo que verifica as duas condições anteriores.
- A utilização em criptografia de curvas elípticas foi sugerida, de modo independente, por Neal Koblitz e Victor S. Miller já em 1985, embora os algoritmos só começaram a ter uso público em 2004.
- Apresentaremos unicamente *curvas elípticas* sobre $\mathbf{Z}_p$, com p um número primo. É possível trabalhar com curvas elípticas usando qualquer **corpo de Galois**, mas as mais usadas são, de facto, sobre $\mathbf{Z}_p$, com p primo.

Comparativa: tamanho da chave

Minimum Size (bits) of Public Keys	
RSA	**ECC**
1024	160
2048	224
3072	256
7680	384
15360	512

Em criptografia, uma **curva elíptica** é o conjunto de pontos que verificam uma equação do tipo

$$y^2 = x^3 + ax + b \quad \text{(Equação de Weierstrass)}$$

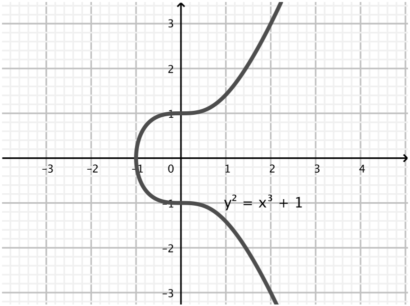
com $4a^3 + 27b^2 \neq 0$, ao qual se adiciona um ponto extra, chamado **ponto do infinito** O_∞.

$\rightsquigarrow$ A condição $4a^3 + 27b^2 \neq 0$ aparece no estudo das raízes do polinómio $r(x) = x^3 + ax + b$. No caso em que $4a^3 + 27b^2 = 0$, este polinómio possui raízes múltiples o que é muito inconveniente nas manipulações algébricas que estão na base dos cálculos com curvas elípticas.

$\rightsquigarrow$ O nome de *curvas elípticas* deve-se a que estas curvas aparecem no cálculo dos comprimentos de arco de elipses, mas **não são** elipses (um elipse está definida por uma equação $\frac{x^2}{a^2} + \frac{y^2}{b^2} = r^2$).

A equação $y^2 = x^3 + 1$ define uma *curva elíptica* no plano real:

$$\mathcal{E}_{\mathbf{R}} = \{(x, y) \in \mathbf{R} \times \mathbf{R} : y^2 = x^3 + 1\} \cup \{O_\infty\}$$



No exemplo anterior os pontos considerados (x, y) têm coordenadas **reais** mas observe-se que uma equação do tipo

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

com a e b inteiros, também pode ser evaluada em outros conjuntos, como os dos inteiros modulares $\mathbf{Z}_p$, com p um número primo $(p > 2, 3)$.

$\rightsquigarrow$ Em $\mathbf{Z}_p$ a condição que estamos a exigir aos coeficientes da curva é simplesmente:

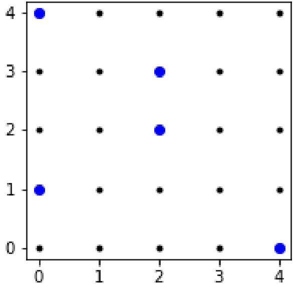
$$4a^2 + 27b^2 \not\equiv 0 \pmod p$$

No plano $\mathbf{Z}_5 \times \mathbf{Z}_5$, que contém 25 pontos, a curva elíptica definida pela equação $y^2 = x^3 + 1$ é o conjunto

$$\mathcal{E}_{\mathbf{Z}_5} = \{(0,1),(4,0),(0,4),(2,2),(2,3)\} \cup \{O_\infty\}$$

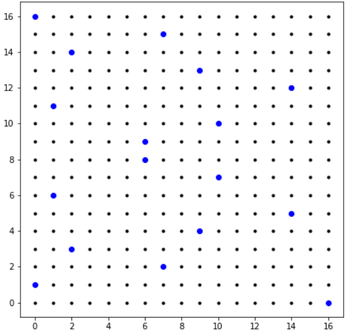
Por exemplo, o ponto $(x,y) = (2,2)$ está efetivamente na curva:

$$y^2 = 4 \qquad x^3 + 1 = 2^3 + 1 = 9 \equiv 4 \pmod 5$$



No caso dos inteiros módulo 17,

$$\mathcal{E}_{\mathbf{Z}_{17}} = \{(0,1),(0,16),(1,6),(1,11),(2,3),(2,14),(6,8),(6,9),(7,2),$$
$$(7,15),(9,4),(9,13),(10,7),(10,10),(14,5),(14,12),(16,0)\} \cup \{O_\infty\}$$



Por exemplo $(0,16)$ está na curva:

$$y^2 = (16)^2 \bmod 17 = 1 \bmod 17,$$
$$x^3 + 1 = 0 + 1 = 1 \bmod 17$$

Também $(7,2)$ porque:

$$y^2 = 2^2 = 4 \bmod 17$$
$$x^3 + 1 = 7^3 + 1 = 344 = 4 \bmod 17$$

A curva elíptica **secp256k1**

A curva elíptica definida por pela equação

$$y^2 = x^3 + 7$$

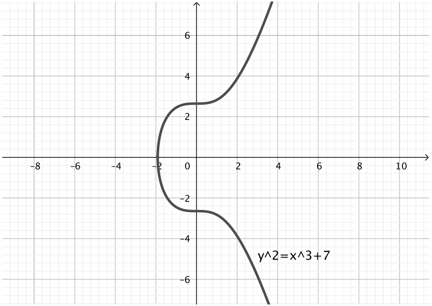
é uma das curvas elípticas mais usadas em criptografia e costuma ser denotada por **secp256k1**.

Considerando coordenadas reais, a curva **secp256k1** tem o aspeto à direita.

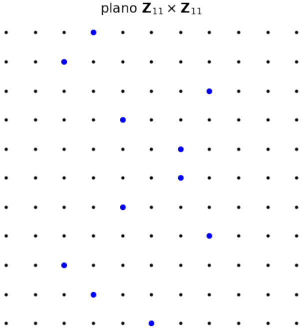
Em criptografia, considera-se a curva definida sobre o corpo $\mathbf{Z}_p$, com

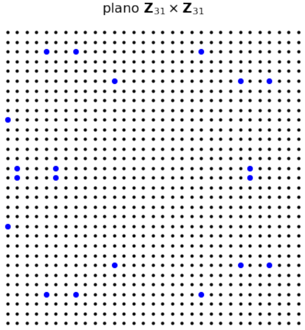
$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1,$$

Frequentemente, esta curva é referida como a **curva de Koblitz secp256k1**.



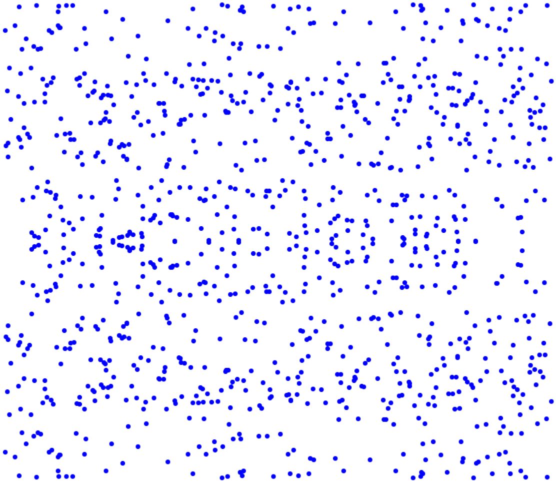
A curva elíptica **secp256k1** $y^2 = x^3 + 7$, considerando aritmética módulo 11 e arimética módulo 31:





A equação $y^2 = x^3 + 7$, **NÃO** define uma curva elíptica sobre $\mathbf{Z}_7$, porque $4a^2 + 27b^2 \equiv 0 \bmod 7$.

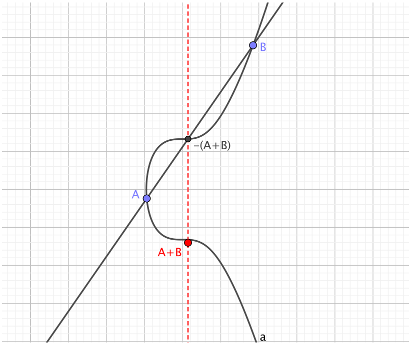
A curva **secp256k1** sobre $\mathbf{Z}_{997}$ contém 1056 pontos, mais o ponto do infinito O_∞.



Curvas elípticas em criptografia?

As curvas elípticas possuem uma propriedade curiosa: é possível definir uma **adição** nos pontos da curva.

No caso de curvas sobre **R**, a adição de pontos da curva pode definir-se geometricamente.



- O elemento neutro é o ponto do infinito, O_∞;
- O simétrico de um ponto A da curva elíptica é o ponto simétrico relativamente ao eixo x, ou seja, se $A = (x_A, y_A)$ então

$$-A = (x_A, -y_A)$$

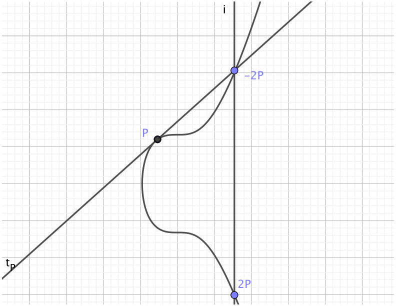
  Observe-se que se $A = (x_A, y_A)$ verifica uma equação do tipo $y^2 = x^3 + ax + b(\bmod p)$ então $(x_A, -y_A)$ também a verifica;
- Se A,B e C são três pontos distintos da curva e colineares, então

$$A + B + C = O_\infty$$

  Por outras palavras, a interseção da recta que passa por A e por B com a curva elíptica é o simétrico de $A + B$, $C = -(A + B)$.

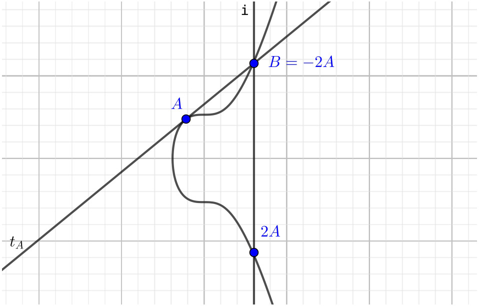
E a soma $P + P$?

As definições anteriores determinaram o elemento neutro, o simétrico de um ponto P e a soma de dois pontos distintos A e B.
Para definir $P + P$ é usada a mesma construção geométrica, com a tangente à curva em P.



Que acontece se C é igual a A ou B?

A recta definida por dois pontos distintos A e B de uma curva elíptica intersecta a curva elíptica só em dois pontos se ela é tangente à curva num deles (um ponto de interseção dupla).



Por exemplo, se a recta for tangente em A, o terceiro ponto de interseção da recta definida por A e B seria o próprio A, donde $A + B = -A$, ou equivalentemente, $B = -2A$, pelo que as duas construções geométricas anteriores são coerentes.

Uma EC é um grupo

A adição numa EC é uma operação que verifica todas as características de uma operação de grupo comutativo: associativa, comutativa, elemento neutro e elemento inverso.

O ponto chave da construção anterior, que permite considerar a curva um grupo, é a associatividade da operação definida. Isto é, é preciso provar, para todos os P, Q, R da curva elíptica que

$$(P + Q) + R = P + (Q + R)$$

As demonstrações existentes da associatividade são difíceis (ou seja, precisam de conceitos matemáticos avançados) ou complicadas (não precisam de conceitos matemáticos avançados mas de apoio computacional para resolver longas equações ....). Geometricamente, é fácil convencer-se que sim ...

Adiçao numa curva elíptica mod p

Em criptografia, em que as curvas elípticas são definidas sobre corpos finitos, a operação de grupo obtém-se simplesmente "traduzindo" as definições e as construções geométricas anteriores a noções algébricas.

Nomeadamente:

- uma recta com coordenadas em $\mathbf{Z}_p$ são pares de pontos cujas coordenadas verificam uma equação de primeira ordem (linear);
- a interseção de duas retas com coordenadas em $\mathbf{Z}_p$ são pares de pontos que verificam (módulo p) as duas equações das retas;
- a reta tangente num ponto também é definida por uma equação de primeira ordem.

Dois pontos **distintos** $A(x_A, y_A)$ e $B(x_B, y_B)$ com coordenadas em $\mathbf{Z}_p$ determinam uma única recta, definida pela equação:

$$\alpha(x - x_A) + \beta(y - y_A) = 0, \qquad \alpha = (y_B - y_A),\ \beta = -(x_B - x_A) \mod p$$

E se $x_A - x_B \not\equiv 0 (\mod p)$, podemos escrever a equação da recta no formato usual:

$$y - y_A = m(x - x_A), \qquad \text{com } m = (y_B - y_A)(x_B - x_A)^{-1} (\mod p)$$

Exemplo:
Considere-se, módulo 5, os pontos $A(2, 2)$ e $B(0, 4)$. A equação da recta definida por A e B em $\mathbf{Z}_5 \times \mathbf{Z}_5$ é

$$y - 2 = (4 - 2)(0 - 2)^{-1}(x - 2) \mod 5$$

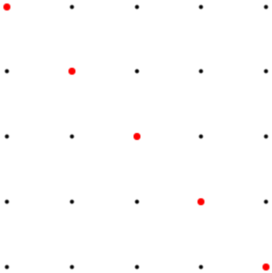
ou seja

$$y + 3 = 4x + 2 \mod 5 \iff y = 4x - 1 \mod 5$$

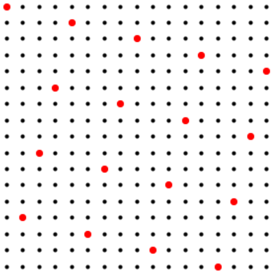
$\rightsquigarrow$ **O cálculo da equação da recta foi realizado com operações módulo 5, no caso de trabalhar com outro módulo, a equação pode mudar!**

Retas de equação $y = 4x - 1$ em $\mathbf{Z}_p$

Recta $y = 4x - 1 \bmod 5$



Recta $y = 4x - 1 \bmod 17$



$\rightsquigarrow$Os pontos $A(2,2)$ e $B(0,4)$ pertencem à recta $y = 4x - 1 \bmod 5$ mas não à recta $y = 4x - 1 \bmod 17$.

$\rightsquigarrow$ **Uma recta em $\mathbf{Z}_p \times \mathbf{Z}_p$ tem exatamente p pontos:**

$$r := A + t\vec{AB}, \ \ t \in \{0, 1, 2, \ldots, p-1\}$$

Em particular, para calcular $-A$ e $A + B$, com A e B pontos distintos de uma curva elíptica, podemos replicar em $\mathbf{Z}_p$ a construção geométrica usando equações:

1. o simétrico de um ponto A, se $A = (x_A, y_A)$, define-se como
$$-A = (x_A, -y_A)$$
com $-y_A$ o simétrico de y_A em $\mathbf{Z}_p$;

2. a interseção da recta que une A e B com a curva elíptica, ou seja, a solução de um sistema:
$$\begin{cases} y^2 = x^3 + ax + b \pmod p \\ y - y_A = m(x - x_A) \pmod p \end{cases},$$
determina um terceiro ponto C que é o simétrico de $A + B$.

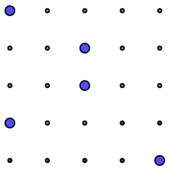
Exemplo 1: a curva $y^2 = x^3 + 1 \bmod 5$

No plano $\mathbf{Z}_5 \times \mathbf{Z}_5$, que contém 25 pontos, a curva elíptica definida pela equação $y^2 = x^3 + 1$ é o conjunto

$$\mathcal{E}_{\mathbf{Z}_5} = \{(0,1),(4,0),(0,4),(2,2),(2,3)\} \cup \{O_\infty\}$$

Tem-se que

$$-O_\infty = O_\infty, \quad -(0,1) = (0,4), \quad -(4,0) = (4,0), \quad -(2,2) = (2,3)$$



Exemplo 1: adição em $y^2 = x^3 + 1 \bmod 5$

Recordemos que curva elíptica $y^2 = x^3 + 1$, sobre $\mathbf{Z}_5$ está formada pelos pontos:

$$\mathcal{E}_{\mathbf{Z}_5} = \{(0,1),(4,0),(0,4),(2,2),(2,3)\} \cup \{O_\infty\}$$

Para calcular a soma dos pontos $A(2,2)$ e $B(0,4)$ procedemos do modo seguinte:

1. Calculamos a recta que une A e B que, como vimos no exemplo anterior, é definida pela equação: $y + 3 = 4x + 2$
2. Procuramos soluções do sistema, módulo 5:

$$\begin{cases} y^2 = x^3 + 1 \pmod 5 \\ y + 3 = 4x + 2 \pmod 5 \end{cases}$$

Trata-se de uma equação de grau três que, neste caso particular, pode resolver-se por verificação direta. A solução do sistema C distinta de A e de B é

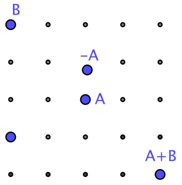
$$C = (4,0)$$

Finalmente, o ponto $A + B$ é o simétrico relativamente ao eixo x do ponto C obtido, ou seja,

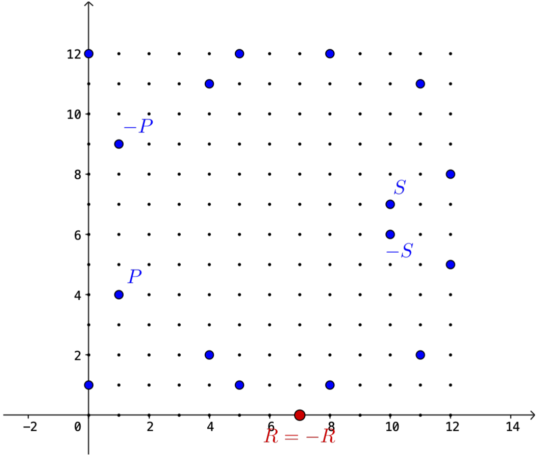
$$A + B = -C = (4, -0) = (4, 0) \qquad (\text{em } y^2 = x^3 + 1, \bmod 5)$$

Em resumo, a adição dos pontos A e B desta curva elíptica é:

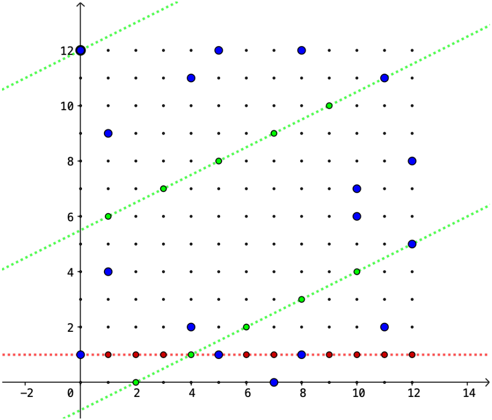
$$A + B = (2, 2) + (0, 4) = (4, 0).$$



Exemplo 2: a curva $y^2 = x^3 + x + 1 \bmod 13$



Exemplo 2: adição em $y^2 = x^3 + x + 1 \bmod 13$.



A adição $P+P$ é definida através da tangente à curva em P.

- Se $P=(x_P,y_P)$ verifica que $y_P=0$, e ou seja $P=(x_P,0)$, então $-P=(x_P,0)=P$, isto é, P é o seu próprio simétrico, pelo que $P+P=O_\infty$

  $\rightsquigarrow$ Em $\mathbf{R}$ imagina-se uma tangente vertical, que intersecta na curva no ponto do infinito ...

- Se considerarmos $P=(x_P,y_P)$, com $y_P\neq 0$, a derivada *formal* da equação da curva elíptica verifica:

$$2yy' = 3x^2 + a$$

  A recta *tangente* à curva elíptica que passa por P pode então definir-se pela equação:

$$y - y_P = m(x - x_P) \quad \text{com} \quad m = (3x_P^2 + a)(2y_P)^{-1}$$

  E então, $2P$ será o simétrico da interseção desta recta com a curva elíptica (módulo p).

Exemplo: $P + P$ em $y^2 = x^3 + 1 \bmod 5$

A curva elíptica $y^2 = x^3 + 1$, sobre $\mathbf{Z}_5$ está formada pelos pontos:

$$\mathcal{E}_{\mathbf{Z}_5} = \{(0,1),(4,0),(0,4),(2,2),(2,3)\} \cup \{O_\infty\}$$

Seja $A = (2,2)$ para calcular $2A$, calculamos em primeiro lugar a *tangente*, módulo 5:

$$m = (3 \cdot 2^2 + 0)(2 \cdot 2)^{-1} \bmod 5 = 3 \bmod 5$$

isto é,

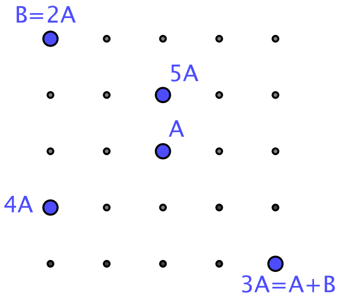
$$y - 2 = 3(x-2) \bmod 5 \Leftrightarrow y = 3x - 4 \bmod 5 \Leftrightarrow y = -2x + 1 \bmod 5$$

A interseção desta recta com a curva elíptica, que podemos calcular por verificação direta, consiste no ponto A e no ponto $(0,1)$, pelo que $2A$ é o simétrico de $(0,1)$ isto é $(0,4)$:

$$2A = (0,4)$$

$\rightsquigarrow$ Aproveitando os cálculos anteriores, como $B = (0,4)$, obtemos também

$$3A = A + B = (4,0) \quad 4A = (0,1), \quad 5A = (2,3), \quad 6A = O_\infty$$


B=2A
5A
A
4A
3A=A+B

Nos exemplo anteriores, a resolução do sistema

$$\begin{cases} y^2 = x^3 + ax + b \pmod p \\ y - y_A = m(x - x_A) \pmod p \end{cases}$$

foi realizada por procura exaustiva.

$\rightsquigarrow$ Em geral não é fácil resolver sistemas com equações não lineares mas, neste caso, precisamente pelo tipo de equação cúbica, existem fórmulas para calcular as soluções.

Seja $\mathcal{E}$ uma curva elíptica em $\mathbf{Z}_p$, com p um primo tal que $p > 3$, definida pela equação

$$y^2 = x^3 + ax + b, \quad \text{com} \quad 4a^3 + 27b^2 \not\equiv 0 (\bmod p).$$

Sejam $A = (x_A, y_A)$ e $B = (x_B, y_B)$ dois pontos de $\mathcal{E}$, distintos do ponto do infinito O_∞ e

$$A + B = (x_{A+B}, y_{A+B})$$

a adição dos pontos A e B na curva elíptica.

1. Se $x_A \neq x_B$, ou seja, $x_A - x_B \not\equiv 0(\bmod p)$, então:

$$\begin{cases} x_{A+B} & \equiv & (m^2 - x_A - x_B)(\bmod p) \\ y_{A+B} & \equiv & -(y_A + m(x_{A+B} - x_A))(\bmod p) \end{cases} \qquad \text{com } m = (y_A - y_B)(x_A - x_B)^{-1}(\bmod p)$$

2. Se $x_A \equiv x_B(\bmod p)$ e $y_A \equiv y_B(\bmod p)$, estamos no caso em que $A = B$ e há duas possibilidades:
   1. $y_A \equiv 0(\bmod p)$, então tem-se que $A = -A$ (o ponto é o seu próprio simétrico), pelo que

$$2A = A + A = O_\infty$$

   2. $y_A \not\equiv 0(\bmod p)$ e então $2A = A + A$ é definido por

$$\begin{cases} x_{A+A} & \equiv & (m^2 - x_A - x_B)(\bmod p) \\ y_{A+A} & \equiv & -(y_A + m(x_{A+B} - x_A))(\bmod p) \end{cases} \qquad \text{com } m = (3x_A^2 + a)(2y_A)^{-1}(\bmod p)$$

3. Se $x_A \equiv x_B(\bmod p)$ e $y_A \equiv -y_B(\bmod p)$, estamos no caso em que $A \neq B$ mas $A = -B$ e portanto

$$A + B = O_\infty$$

Os pontos A e B verificam a equação da curva elíptica, pelo que se $x_A = x_B$ em $\mathbf{Z}_p$, tem-se que $y_A^2 = y_B^2$ em $\mathbf{Z}_p$, ou seja, $y_A \equiv \pm y_B(\bmod p)$. Por outras palavras, se $x_A = x_B$ em $\mathbf{Z}_p$, então $A = B$ ou $A = -B$, não há outras possibilidades.

O ponto do infinito O_∞

Nas implementações da adição em curvas elípticas, o ponto do infinito O_∞ levanta problemas, pelo seu caracter *especial* de ponto adicionado *ad hoc*.

Uma solução eficiente (com forte justificação matemática que a sustenta) é a utilização das chamadas *coordenadas homogéneas*.

Muito resumidamente, introduzir coordenadas homogéneas consiste em adicionar uma coordenada igual a 1 para os pontos distintos de O_∞ e definir as coordenadas *homogéneas* de O_∞ como $(0, 1, 0)$. Assim, os pontos da curva elíptica $y^2 = x^3 + 1$ definidos no exemplo anterior são:

$$\mathcal{E}_{\mathbf{Z}_5} = \{(0, 1, 0), (0, 1, 1), (0, 4, 1), (2, 2, 1), (2, 3, 1), (4, 0, 1)\}$$

$\rightsquigarrow$ As coordenadas homogéneas permitem, de facto, tratar o ponto do infinito igual aos outros.

Ordem de uma curva elíptica.

O número de elementos de um grupo costuma chamar-se **ordem** do grupo.

O número pontos de uma curva elíptica (a *ordem da EC*) pode calcular-se usando o algoritmo de Schoof.

Exemplos:

Considere-se a curva elíptica definida pela equação $y^2 = x^3 + 7$,

1. Sobre $\mathbf{Z}_5$, a ordem da curva é igual a 6;
2. Sobre $\mathbf{Z}_{13}$, a ordem da curva é igual a 7
3. Sobre $\mathbf{Z}_{101}$, a ordem da curva é igual a 102
4. Sobre $\mathbf{Z}_{613}$, a ordem da curva é igual a 567
5. Sobre $\mathbf{Z}_{997}$, a ordem da curva é igual a 1057.

O exemplo anterior parece mostrar que o número de pontos de uma curva elíptica está na ordem de grandeza do primo p.

Efetivamente ...

Teorema de H. Hasse (1933) Para uma curva elíptica definida sobre um corpo $\mathbf{Z}_p$, o número de pontos N da curva verifica:

$$(p+1)-\sqrt{p} \leq N \leq (p+1)+\sqrt{p}$$

Observe-se que, dado um ponto P de uma curva elíptica sobre um corpo finito $\mathbf{Z}_p$, se calculamos todos os múltiplos P:

$$P, 2P, \ldots, nP, \ldots$$

como o número de pontos da curva é finito, algures, obrigatoriamente, existirão n_1 e n_2 tais que

$$n_1 P = n_2 P$$

Atendendo às propriedades de grupo, esto significa que $(n_1 - n_2)P = O_\infty$, ou seja, para cada ponto P da curva elíptica, existe k_P tal que

$$k_P P = O_\infty$$

Seja P um ponto de uma curva elíptica sobre um corpo finito. O menor k tal que

$$kP = O_\infty$$

diz-se **ordem** do ponto P e denota-se por $\operatorname{ord} P$.

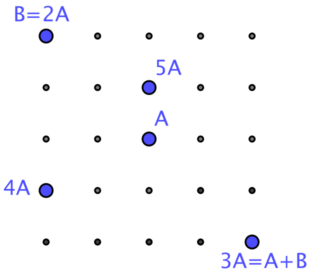
Exemplo 1: $y^2 = x^3 + 1$ sobre $\mathbf{Z}_5$

Considere-se a curva elíptica $y^2 = x^3 + 1$ sobre $\mathbf{Z}_5$, que verifica:

$$\mathcal{E}_{\mathbf{Z}_5} = \{(0,1),(4,0),(0,4),(2,2),(2,3)\} \cup \{O_\infty\}$$

A ordem do ponto $A = (2,2)$, como calculado anteriormente:

$$2A = (0,4),\ 3A = (4,0),\ 4A = (0,1),\ 5A = (2,3),\ 6A = O_\infty$$



Se considerarmos o ponto $B = (0,4)$, tem-se que

$$B = 2A = (0,4),\ 2B = 4A = (0,1),\ 3B = 6A = O_\infty$$

por outras palavras, a ordem de B é 3.
De facto, verifica-se que:

$$\mathrm{ord}\, O_\infty = 1,\ \mathrm{ord}\,(2,2) = 6,\ \mathrm{ord}\,(0,4) = 3$$

$$\mathrm{ord}\,(2,3) = 6,\ \mathrm{ord}\,(4,0) = 2,\ \mathrm{ord}\,(0,1) = 3$$

Ordem de um ponto e ordem da EC

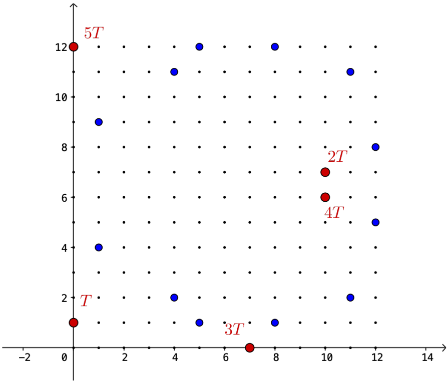
O exemplo anterior mostra uma relação fundamental que existe entre a ordem de um grupo (no nosso caso, o número de pontos da curva elíptica) e a ordem de um elemento do grupo:

A ordem de um ponto de uma curva elíptica sobre um corpo finito divide à ordem da curva elíptica, isto é, ao número de pontos da curva elíptica.

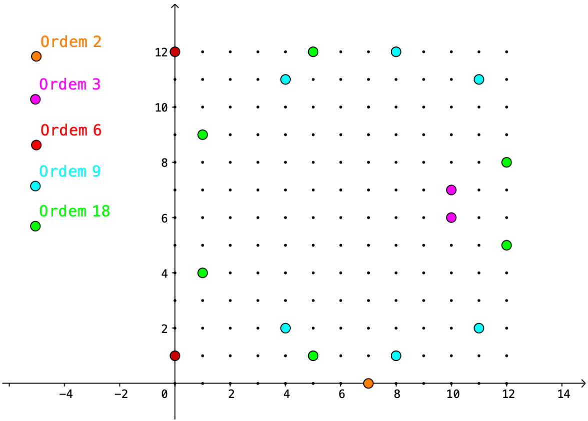
Esta propriedade é consequência de um teorema mais geral de teoria de grupos, chamado *Teorema de Lagrange*

Considerando $T = (0, 1)$, obtem-se

$$2T = (10, 7), \quad 3T = (7, 0), \quad 4T = (10, 6), \quad 5T = (0, 12), \quad 6T = O_\infty$$



Exemplo 2: Ordens dos pontos de $y^2 = x^3 + x + 1 \bmod 13$



Exemplo: EC $y^2 = x^3 + 7$ sobre $\mathbf{Z}_7$ e $\mathbf{Z}_{101}$

1. Sobre $\mathbf{Z}_{13}$, a ordem da curva é igual a 7, podemos ter elementos de ordem 1 e 7. De facto, como a ordem de um ponto divide a ordem da curva, tem-se que TODOS os pontos da curva, menos o neutro O_∞, têm ordem 7. Por exemplo $A = (7, 5)$ é um elemento de ordem 7.
2. Sobre $\mathbf{Z}_{101}$, a ordem da curva é igual a 102 e como $102 = 2 \cdot 3 \cdot 17$, podemos ter elementos de ordem 1, 2,3,6,17, 34, 51 e 102. De facto $A = (4, 24)$ é um elemento de ordem 102, e a partir dele conseguimos elementos de todas as outras ordens:

$$\begin{array}{rcl}
B = 2A & \text{tem ordem igual a} & 51 \\
C = 3A & \text{tem ordem igual a} & 34 \\
D = 6A & \text{tem ordem igual a} & 17 \\
E = 17A & \text{tem ordem igual a} & 6 \\
F = 34A & \text{tem ordem igual a} & 3 \\
G = 51A & \text{tem ordem igual a} & 2
\end{array}$$

(Observe que o único elemento de ordem 1 é O_∞)

No exemplo anterior, a curva apresentada tinha pontos com a *máxima ordem possível*, a ordem da curva elíptica.

Por outras palavras, tinham pontos A tais que a sequência $A, 2A, 3A, \cdots, nA$ gera todos os pontos possíveis da curva.

Este tipo de curvas são chamadas **cíclicas**, o exemplo anterior é uma curva cíclica.

A criptografia em curvas elípticas precisa de pontos de ordem elevada: por exemplo, no caso da famosa curva **Secp256k1**, é possível escolher um ponto com a ordem igual à ordem da curva, isto é, um **gerador** de toda a curva (é uma curva cíclica).

Exemplo: EC não cíclica

Considere-se a curva elíptica definida pela equação $y^2 = x^3 + x + 9$, sobre o corpo $\mathbf{Z}_{11}$. Tem-se que:

$$\mathcal{E}_{\mathbf{Z}_{11}} = \{(0,3),(0,8),(1,0),(4,0),(6,0),(8,1),(8,10)\} \cup \{O_\infty\}$$

A ordem desta curva é igual a 8, em princípio, podemos ter elementos de ordem 1,2, 4 e 8. No entanto, verifica-se que:

$$\mathrm{ord}\,(0,3) = 4,\ \ \mathrm{ord}\,(0,8) = 4,\ \ \mathrm{ord}\,(1,0) = 2,\ \ \mathrm{ord}\,(4,0) = 2$$

$$\mathrm{ord}\,(6,0) = 2,\ \ \mathrm{ord}\,(8,1) = 4,\ \ \mathrm{ord}\,(8,10) = 4$$

Por outras palavras, esta curva não contém pontos de ordem máxima 8. Não existe nenhum ponto que *gere* todos os pontos da curva. A curva $y^2 = x^3 + x + 9$, sobre o corpo $\mathbf{Z}_{11}$ não é cíclica.

A criptografia de chave pública que usa curvas elípticas é uma generalização do **problema do logaritmo discreto** em $\mathbf{Z}_p$. Mais precisamente, escolhida adequadamente uma curva elíptica

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

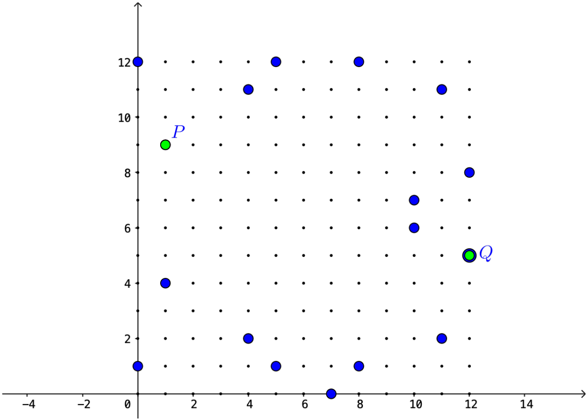
e um corpo de Galois (por exemplo $\mathbf{Z}_p$, com p primo), tais que:

- dado um ponto P adequado da curva elíptica, o cálculo dos pontos $2P, 3P, \ldots, nP$ pode ser implementado de modo eficiente;
- dado um ponto Q da curva elíptica, é computacionalmente intratável encontrar n tal que

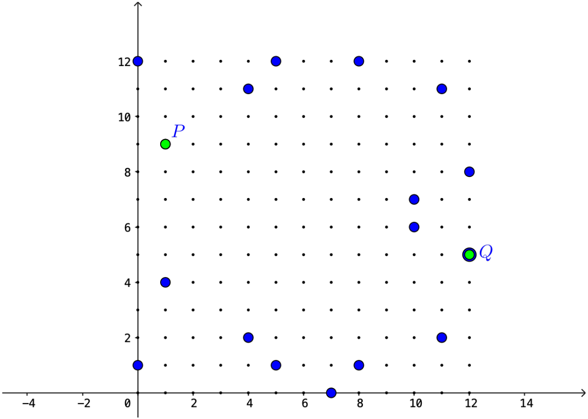
$$Q = nP$$

O ponto $P = (1, 9)$ é um *gerador* da curva (ordem 18).

Exemplo do problema do logaritmo discreto em esta curva:
Considerando $Q = (12, 5)$, qual é o n tal que $nP = Q$?



Dados $P = (1, 9)$ e $Q = (12, 5)$ tem-se que $Q = 7P$.



A situação ótima em ECC supõe uma curva elíptica cíclica e um ponto base P, gerador da curva, isto é, um ponto tal que

$$\mathcal{E} = \{O_\infty, P, 2P, \ldots, (N-1)P\} \qquad (N = \text{ordem da curva }).$$

Nem sempre é possível assegurar estas as condições. No entanto, é sempre possível, para cada divisor primo n de N, encontrar um ponto P cuja ordem é igual a n.

Exemplo:
Considere-se a curva elíptica definida pela equação $y^2 = x^3 + 4x + 2$, módulo $p = 59$. É uma curva não cíclica, de ordem ordem 68. Tem-se que $68 = 4 \cdot 17$ e que:

- Os pontos $(9, 0)$, $(22, 0)$ e $(28, 0)$ são os pontos de ordem 2;
- Os pontos $(14, 18)$, $(14, 41)$, $(26, 10)$, $(26, 49)$, $(29, 9)$, $(29, 50)$, $(31, 2)$, $(31, 57)$, $(37, 2)$, $(37, 57)$, $(44, 15)$, $(44, 44)$, $(50, 2)$, $(50, 57)$, $(57, 24)$ e $(57, 35)$ são os pontos de ordem 17.

(Não há pontos de ordem 4 ou de ordem 68, todos os outros pontos são de ordem 34)

I. Parâmetros do domínio para ECC

Os parámetros do domínio para uma curva elíptica são seis:

- p : um número primo;
- a, b : os coeficientes que definem a equação $y^2 = x^3 + ax + b$ da curva elíptica;
- n: um número divisor de N (ordem da curva);
- G: ponto da curva elíptica de ordem n;
- h: inteiro tal que $h \cdot n = N$, com N o número de pontos da curva elíptica sobre $\mathbf{Z}_p$.

$\rightsquigarrow$ **Se n é primo existe sempre G nas condições requeridas.**

Exemplo 1: parámetros de domínio numa EC cíclica

A curva elíptica $y^2 = x^3 + 2x + 4$ módulo 31 é cíclica de ordem 35.

- $p = 31$ (um número primo);
- $a = 2,\ b = 4$ (coeficientes da curva elíptica);
- $n = 35$;
- $G = (0, 2)$ (ponto da curva elíptica de ordem 35);
- $h = 1$ (inteiro tal que $h \cdot n = 1 \cdot 35 = 35 = N$, com N a ordem da curva).

A curva elíptica $y^2 = x^3 + 4x + 2$ módulo 59 é uma curva não cíclica de ordem 68.

- $p = 59$ (um número primo);
- $a = 4,\ b = 2$ (coeficientes da curva elíptica);
- $n = 17$ (número primo divisor de $N = 68$);
- $G = (14, 18)$ (ponto da curva elíptica de ordem n);
- $h = 4$ (inteiro tal que $h \cdot n = 4 \cdot 17 = 68 = N$, com N a ordem da curva).

A curva *secp256k1* foi desenhada de modo a permitir cálculos eficientes (30% mais rápida que curvas análogas, com implementações adequadas). É uma curva cíclica.

- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, em hexa:

  $p =$0xffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffffe fffffc2f
- $a = 0,\ b = 7$;
- $n =$0xffffffff ffffffff ffffffff fffffffe baaedce6 af48a03b bfd25e8c d0364141
- $G = (x_G, y_G)$ onde

  x_G =0x79be667e f9dcbbac 55a06295 ce870b07 029bfcdb 2dce28d9 59f2815b 16f81798

  y_G =0x483ada77 26a3c465 5da4fbfc 0e1108a8 fd17b448 a6855419 9c47d08f fb10d4b8
- $h = 1$.

II. Cálculo de chaves

- A chave privada d é um inteiro aleatório em $\{1, \ldots, n-1\}$;
- A chave pública é o ponto $H = dG$, com G o ponto base.

III. Protocolo ECDH - Elliptic Curve Diffie Hellman

- Alice e Bob geram as suas chaves privadas d_A, d_B e as suas chaves públicas H_A, H_B;
- Alice calcula $d_A H_B$ e Bob calcula $d_B H_A$, obtendo os dois a mesma chave partilhada:

$$K = d_A d_B G = d_B d_A G$$

Exemplo: ECDH com $y^2 = x^3 + 2x + 4,\ p = 31$

- Parâmetros públicos de domínio:
  - $p = 31$
  - $a = 2,\ b = 4$
  - $n = 35;$
  - $G = (0, 2)$
  - $h = 1$
- Chaves privadas de Alice e Bob:

$$d_A = 17 \qquad d_B = 13$$

- Chaves públicas de Alice e Bob:

$$H_A = 17G = (1, 10) \qquad H_B = 13G = (27, 5)$$

- Chave partilhada:

$$K = d_A d_B G = d_B d_A G = 221G = 11G = (10, 30)$$

https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/