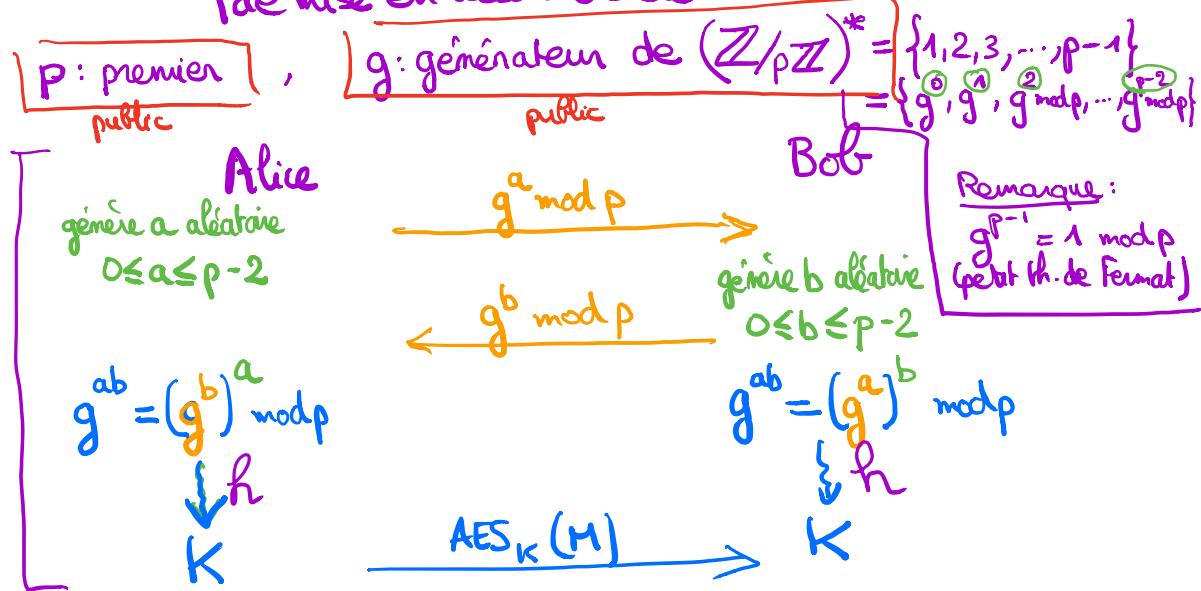


ch 2 : Diffie-Hellman et courbes elliptiques

I] Protocole de Diffie-Hellman

① Rappel

Protocole d'échange de clé
de mise en accord de clé



Remarque : En général, on ne prend pas $K = g^{ab} \text{ mod } p$

- Raison n° 1 : $g^{ab} \text{ mod } p$ n'est en général pas directement dans le format voulu d'une clé de cryptographie symétrique.

- Raison n° 2 : même si on "tranche" $g^{ab} \text{ mod } p$ pour obtenir K de 128 bits (par exemple) il peut y avoir un pb de sécurité

ex: $p = 19$

$$g^{ab} \text{ mod } p \in (\mathbb{Z}/19\mathbb{Z})^* = \{1, 2, 3, \dots, 18\}$$

codé sur 5 bits

On peut décider que $K = 4$ bits de poids
faible de $g^{ab} \bmod p$

$g^{ab} \bmod p$	K (4 bits)
1	0001 X
2	0010 X
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	(1) 0000
17	(1) 0001 X
18	(1) 0010 X

répartie de façon uniforme dans $(\mathbb{Z}/p\mathbb{Z})^*$

apparaissent une seule fois

mais :

0001 et 0010 apparaissent 2 fois

Solution possible : prendre $K = h(g^{ab} \bmod p)$ tronqué à n bits où h est une fonction de hachage.

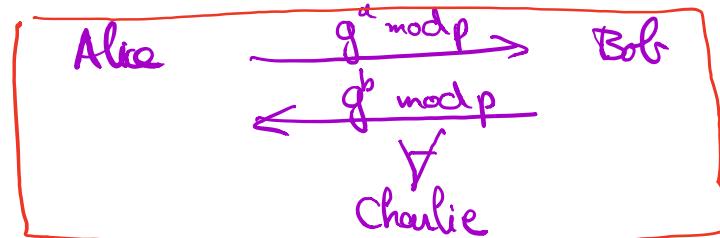
Remarque : Historiquement, la 1ère version du standard (NIST)

utilisait un générateur d'aleas de n bits basé sur une "mauvaise" troncation d'éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ et ça donné lieu à une attaque de cryptanalyse

DSA
Digital Signature Algorithm
(variante d'ElGamal)

② Sécurité de Diffie-Hellman

- Sécurité contre un attaquant passif



Objectif: connaître $g^{ab} \text{ mod } p \rightsquigarrow K$

Pb Diffie-Hellman calculatoire

Etant donné p premier,
 g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$
 $\boxed{g^a \text{ mod } p}$ et $\boxed{g^b \text{ mod } p}$
trouver $g^{ab} \text{ mod } p$

Pb du logarithme discret

Etant donné p premier
 g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$
et $g^a \text{ mod } p$
trouver a

Savoir résoudre le pb
du log. discret

savoir résoudre
le pb D.H



Le meilleur algorithme connu
a une complexité

$$O(e^{c(\ln p)^{1/3}(\ln \ln p)^{2/3}}) \text{ avec } c \approx 1,92$$

(méthode du calcul d'indices)

Remarque: la complexité du meilleur algo connu pour
la factorisation d'un entier n est
 $O(e^{c(\ln n)^{1/3}(\ln \ln n)^{2/3}})$ avec $c \approx 1,92$

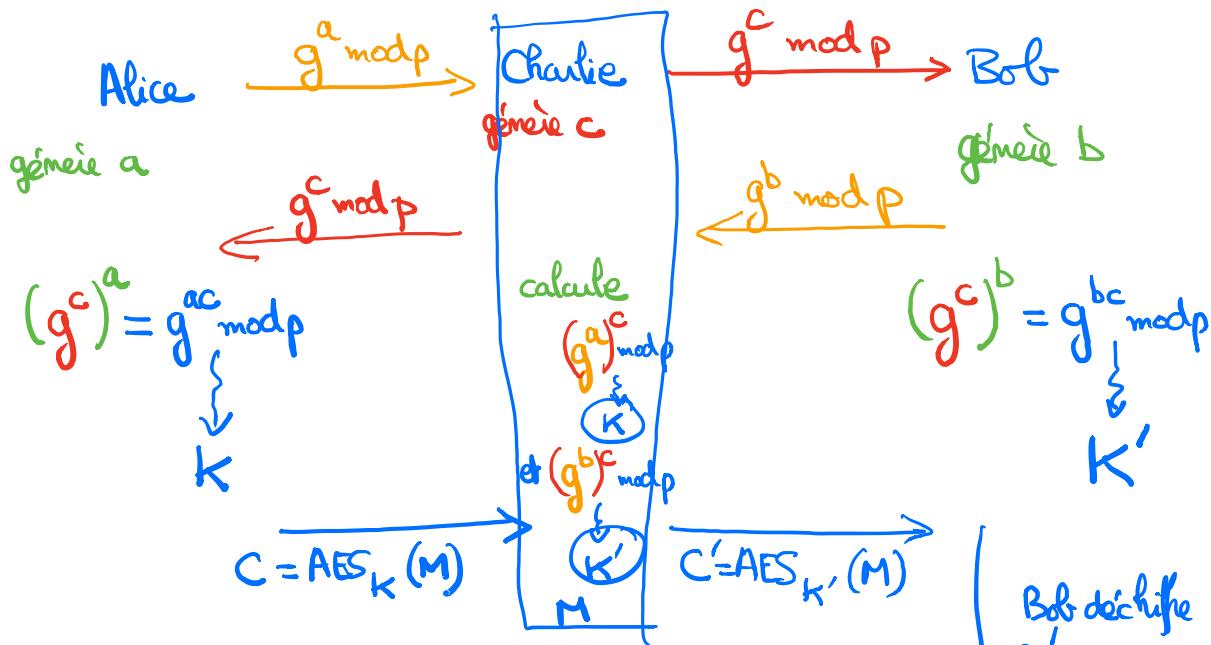
RSA

Pour Diffie-Hellman, on veut que (par exemple)

$$e^{c(\ln p)^{1/3}(\ln \ln p)^{2/3}} \geq 280$$

↪ OK pour p d'au moins 1024 bits

- Sécurité contre un attaquant actif
- Attaque "man in the middle" (homme au milieu)

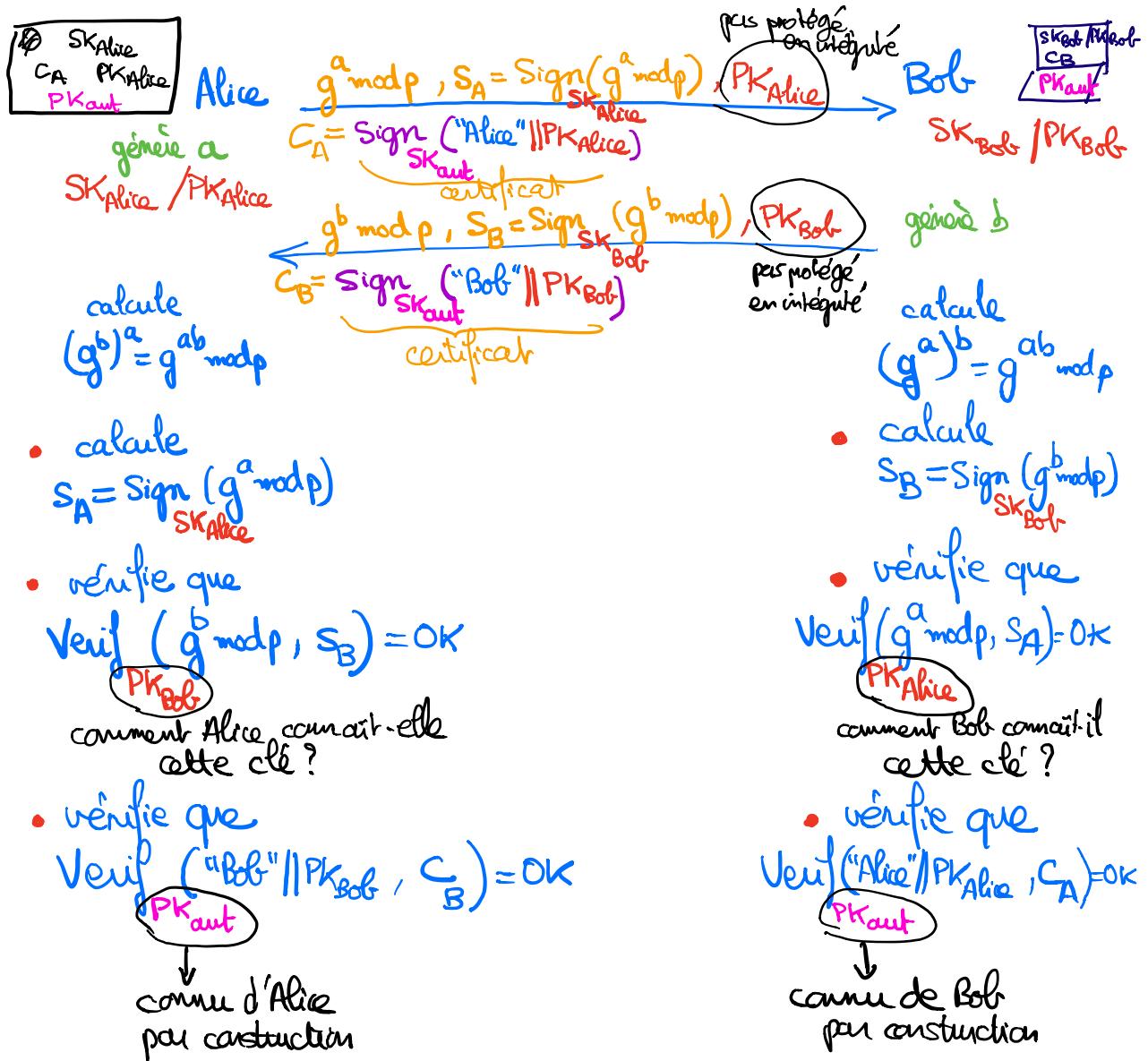


Remarque : le protocole D.H a été publié en 1976
dans : W. Diffie, M. Hellman, "New Directions in Cryptography"

Bob déchiffre C' avec sa clé K' et trouve M

Solution possible : protocole de Diffie-Hellman authentifié

Idee : garantir à Bob que les messages reçus ont bien été émis par Alice et vice versa

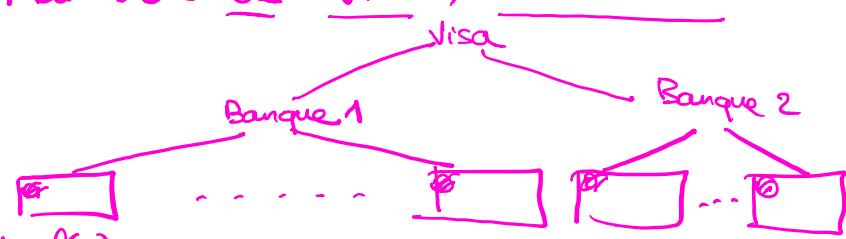


Autorité : système de paiement bancaire

ex : Alice = carte bancaire
Bob = terminal d'un commerçant

Autorité = ex : Visa, Mastercard

PK I
(Public key infrastructure)
= IGC
(Infrastructure de gestion de clés)



- https

↓
sécurisé par le système SSL / TLS

↓
Diffie-Hellman

ex: Alice = navigateur
 Bob = site de la FNAC
 Autorité = Centplus, Verisign,

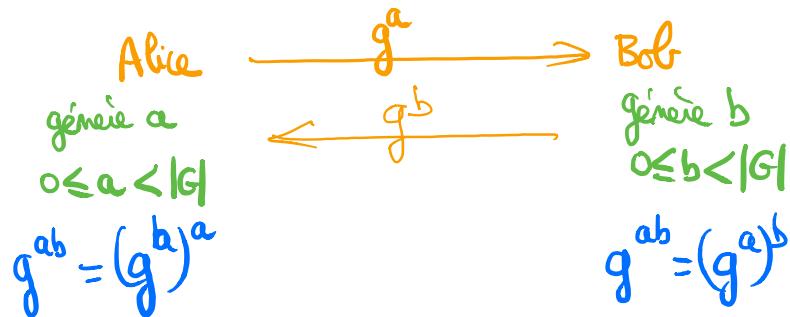
II] Cryptographie à base de courbes elliptiques

① Diffie-Hellman sur un groupe

(G, \times) groupe cyclique, de générateur g

$$G = \{g^0, g^1, g^2, g^3, \dots, g^{|G|-1}\} = \langle g \rangle$$

Rémarque: $\underbrace{g^{|G|}}_{\text{Th. de Lagrange}} = 1 (=g^0)$ (notamment, quand $G = (\mathbb{Z}/p\mathbb{Z})^\times$
 ou c'est le petit th. de Fermat: $g^{p-1} = 1 \pmod{p}$)



La Sécurité (passive) repose sur la difficulté du pb D-H,
 qui elle-même repose sur la difficulté du pb du logarithme discret

pb du log discret: Étant donné G engendré par g
 et g^a , trouver a

Exemple: $G = (\mathbb{Z}/p\mathbb{Z})^*$ \rightarrow complémenté du log discret
 $O(e^{c(\ln p)^{1/3}(\ln \ln p)^{2/3}})$

\rightarrow on prend p de 1024 bits
 pour une sécurité en 2^{80}

$$|G| \approx 2^{1024}$$

Question: Peut-on trouver des groupes G "plus petits" tout en gardant une sécurité en 2^{80} ? [courbes elliptiques]

ex: $G = (\mathbb{Z}/p\mathbb{Z}, +)$ \rightarrow générateur g

pb du log discret: étant donné $y = g + g + \dots + g$ (a fois)
 trouver a

$$y = a \cdot g \Leftrightarrow a = y \cdot g^{-1} \pmod{p}$$

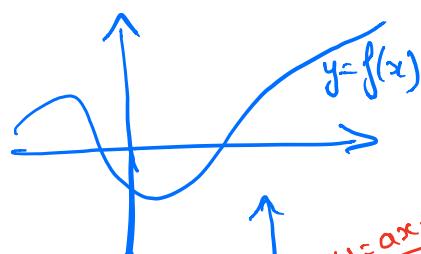
algorithme d'Euclide étendu

② Courbes elliptiques

Courbe: $f(x, y) = 0$

- f : polynôme de degré 1

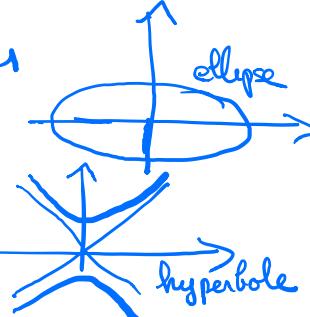
$$y = ax + b \rightarrow \text{droites}$$



- f : polynôme de degré 2

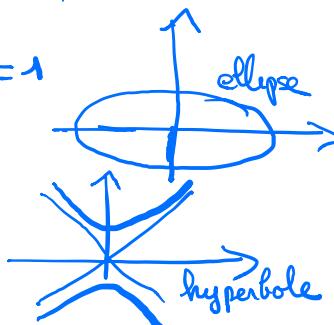
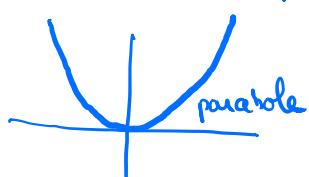
coniques

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$



$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

$$\text{parabole: } y = ax^2$$

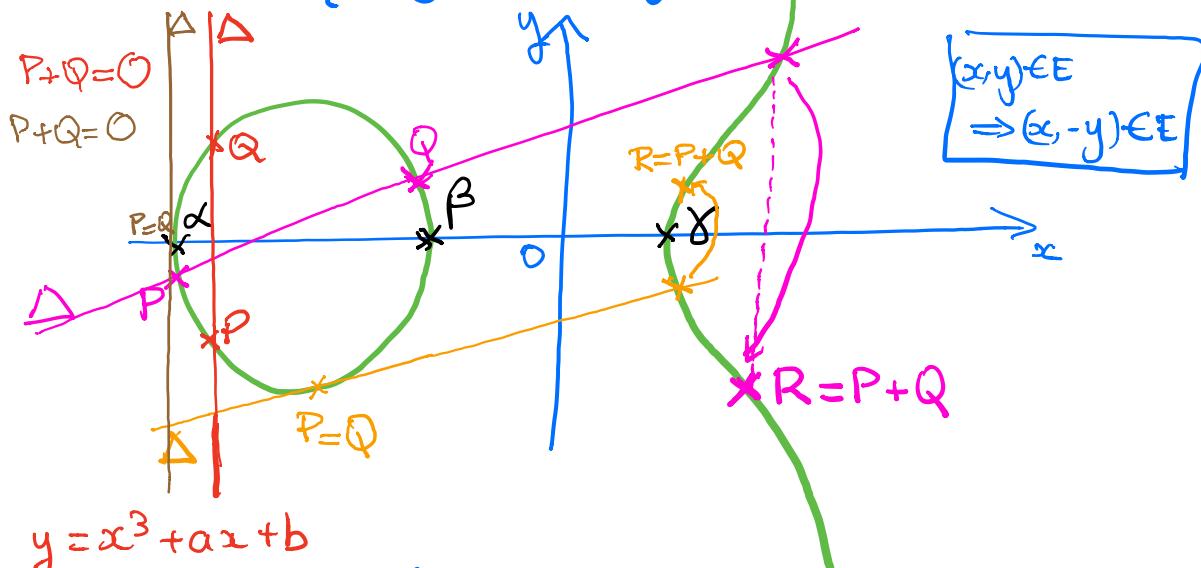


- f : polynôme de degré 3
 \rightarrow cubiques

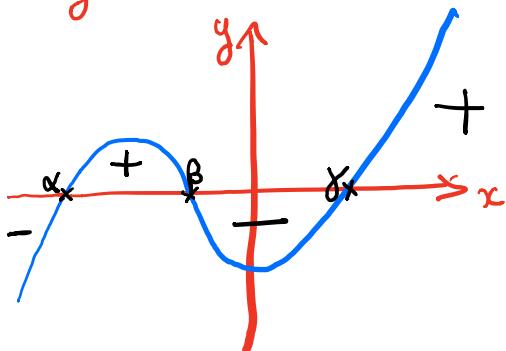
dont les courbes elliptiques, d'équation :

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

$$E = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b\}$$



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



On définit une addition sur E

- À partir de deux points P et Q

on considère la droite
 $\Delta = (PQ)$

si $P \neq Q$
et
 $\Delta = (PQ)$
n'est pas verticale

- cette droite recoupe E
en un 3^e point
- dont on prend le symétrique
par rapport à l'axe des
abscisses

pb : la définition est incomplète

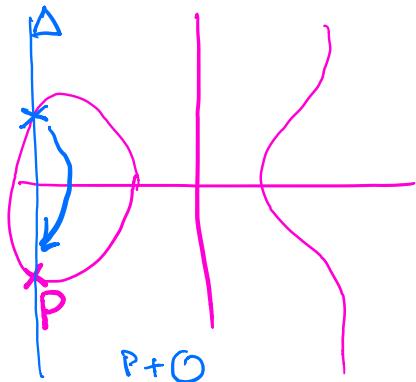
→ que faire si $P = Q$?

→ que faire si Δ est verticale ?

(P et Q sont
sur la même verticale)

• Si $P = Q$: Δ = tangente à E
en ce point

dans \mathbb{R} , l'équation $x^2 = -1$ n'a pas de solution
 → on introduit $i \rightarrow \mathbb{C}$



- On ajoute un point spécial à E qu'on appelle "point à l'infini" et que l'on note \mathcal{O}

Quand Δ est verticale, on pose par définition : $P+\mathcal{O} = P$

$$E = \{(x,y) \in \mathbb{R}^2 / y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

- Par définition, on pose :

$$\forall P \in E, \quad P + \mathcal{O} = P$$

$$\mathcal{O} + P = P$$

$$\text{En particulier } \mathcal{O} + \mathcal{O} = \mathcal{O}$$

Théorème : $(E, +)$ est un groupe [commutatif] (abélien)
 à condition que $4a^3 + 27b^2 \neq 0$

Démonstration :

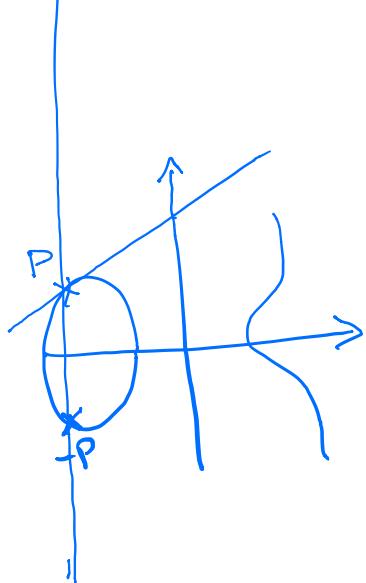
- $E \neq \emptyset$ car $\mathcal{O} \in E$
- L'opération $+$ est intérieure : par définition OK
- Élément neutre : il existe un élément N tel que $\forall P \in E, P + N = N + P = P$

Oui : avec $N = \mathcal{O}$

- Tout élément P admet un élément symétrique Q , c'est à dire tel que $P + Q = Q + P = \mathcal{O}$

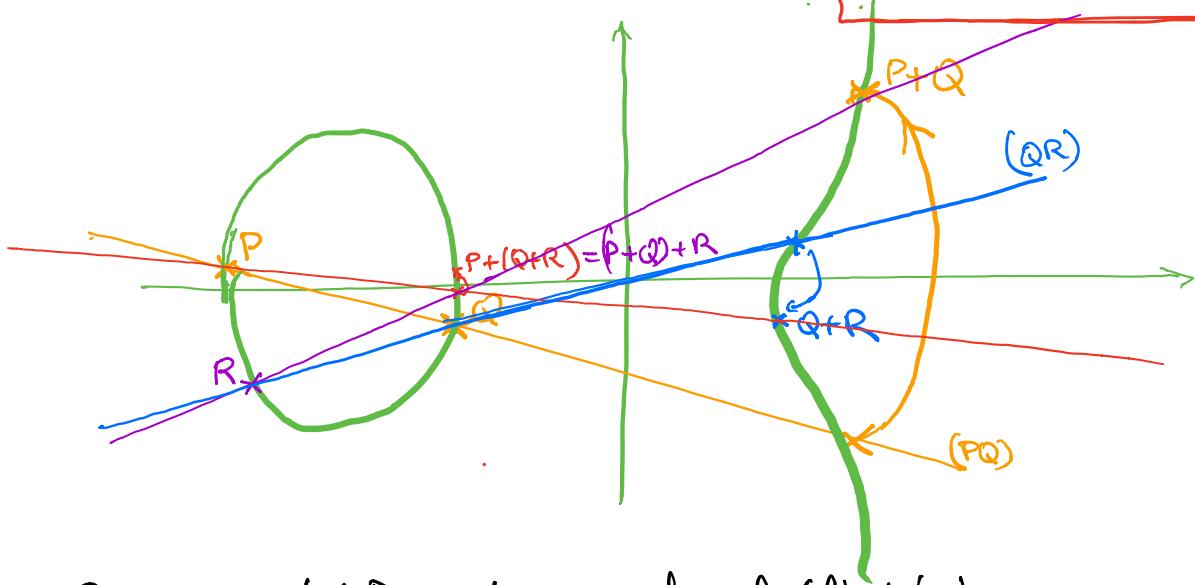
Oui : avec $Q = -P$ = point symétrique de P
par rapport à l'axe des abscisses

(l'élément symétrique de \mathcal{O} est \mathcal{O})



• Associativité :

$$\forall P, Q, R \in E, (P+Q)+R = P+(Q+R)$$



Remarque : c'est Descartes qui a formalisé l'idée de lier les questions de nature géométrique à des calculs sur des nombres réels (via les coordonnées cartésiennes)

$$E = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b\} \cup \{G\}$$

Formules d'addition

$$P = (x_P, y_P) \quad Q = (x_Q, y_Q)$$

$$R = P+Q = (x_R, y_R)$$

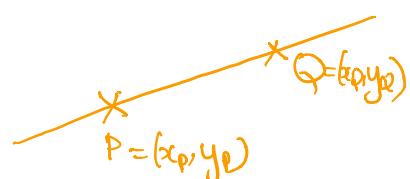
Pb : trouver x_R et y_R en fonction de x_P, y_P, x_Q, y_Q

Cas $P \neq Q$: On considère la droite $\Delta = (PQ)$

⇒ elle a pour équation

$$y = ux + v$$

avec
$$u = \frac{y_Q - y_P}{x_Q - x_P}$$



et $v = y_p - ux_p$ ($\Leftrightarrow P \in \Delta$)

$E \cap \Delta$?

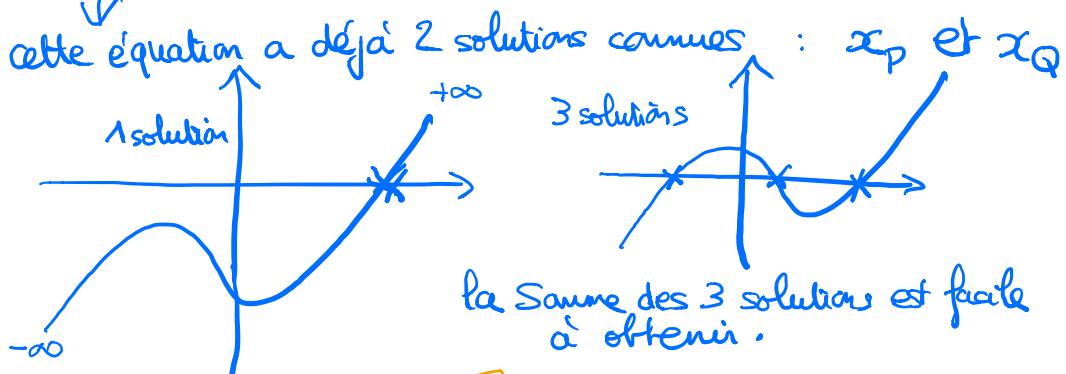
$$(x,y) \in E \cap \Delta \Leftrightarrow \begin{cases} y^2 = x^3 + ax + b \\ y = ux + v \end{cases}$$

$$\Leftrightarrow \begin{cases} (ux + v)^2 = x^3 + ax + b \\ y = ux + v \end{cases}$$

$$\Leftrightarrow \begin{cases} x^3 - u^2 x^2 + (a - 2uv)x + (b - v^2) = 0 \\ y = ux + v \end{cases}$$

Remarque :

- [Il existe des familles (dites de Cardan) pour résoudre les équations du 3^e degré]
- [Il existe des familles pour les équations du 4^e degré]
- [Il n'existe pas de familles générales quand le degré est ≥ 5 (Abel, Galois)]



$$\begin{aligned} & x^3 - u^2 x^2 + (a - 2uv)x + (b - v^2) = 0 \\ & \Leftrightarrow (x - x_p)(x - x_Q)(x - x_R) = 0 \\ & \Leftrightarrow x^3 - \underline{(x_p + x_Q + x_R)} x^2 + \dots = 0 \end{aligned}$$

Donc

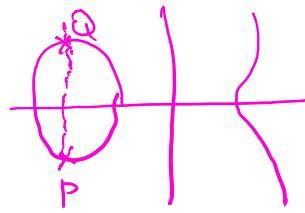
$$x_R = u^2 - x_p - x_Q$$

$$y_R = -(ux_R + v)$$

$P \neq Q$

$$\begin{aligned} u &= \frac{y_Q - y_P}{x_Q - x_P} \neq 0 \\ v &= y_P - ux_P \\ x_R &= u^2 - x_p - x_Q \\ y_R &= -(ux_p + v) \end{aligned}$$

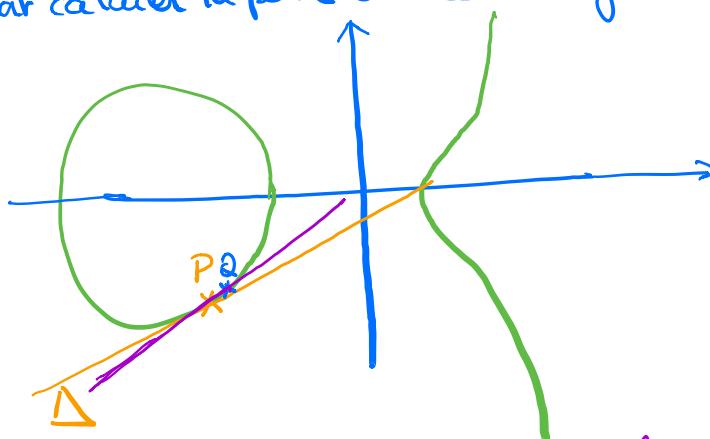
\Rightarrow dans le cas



$$P+Q=0$$

$P = Q$

$\Delta = \text{tangente à } E \text{ en } P (= Q)$
On doit calculer la pente de cette tangente



$$Q \neq P, \quad u = \frac{y_Q - y_P}{x_Q - x_P}$$

Que se passe-t-il quand $Q \rightarrow P$?

$$\begin{aligned} u &= \frac{y_Q - y_P}{x_Q - x_P} = \frac{(y_Q - y_P)(y_Q + y_P)}{(x_Q - x_P)(y_Q + y_P)} = \frac{y_Q^2 - y_P^2}{(x_Q - x_P)(y_Q + y_P)} \\ &= \frac{(x_Q^3 + ax_Q + b) - (x_P^3 + ax_P + b)}{(x_Q - x_P)(y_Q + y_P)} = \frac{(x_Q^3 - x_P^3) + a(x_Q - x_P)}{(x_Q - x_P)(y_Q + y_P)} \end{aligned}$$

$$A^3 - B^3 = (A - B)(A^2 + AB + B^2)$$

$$x_Q^3 - x_P^3 = (x_Q - x_P)(x_Q^2 + x_Q x_P + x_P^2)$$

$$\Rightarrow u = \frac{(x_Q - x_P)(x_Q^2 + x_Q x_P + x_P^2) + a(x_Q - x_P)}{(x_Q - x_P)(y_Q + y_P)}$$

$$u = \frac{x_Q^2 + x_Q x_P + x_P^2 + a}{y_Q + y_P} \xrightarrow{Q \rightarrow P} \boxed{\frac{3x_P^2 + a}{2y_P}}$$

Formules d'addition

$$u = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & \text{si } P \neq Q \\ \frac{3x_P^2 + a}{2y_P} & \text{si } P = Q \end{cases}$$

$$v = y_P - ux_P$$

$$x_R = u^2 - x_P - x_Q$$

$$y_R = -(ux_R + v)$$

Autre méthode pour la tangente

Pour une courbe d'équation

$$\Phi(x, y) = 0$$

la tangente en un point $P = (x_P, y_P)$

a pour pente

$$\left| \begin{array}{l} -\frac{\partial \Phi}{\partial x}(P) \\ \frac{\partial \Phi}{\partial y}(P) \end{array} \right| \rightarrow$$

$$\text{Ici } \Phi(x, y) = y^2 - (x^3 + ax + b)$$

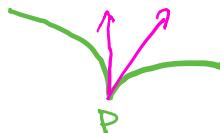
$$\frac{\partial \Phi}{\partial x}(x, y) = -3x^2 - a$$

$$\frac{\partial \Phi}{\partial y}(x,y) = 2y$$

$$\Rightarrow -\frac{\frac{\partial \Phi}{\partial x}}{\frac{\partial \Phi}{\partial y}}(x,y) = \frac{3x^2+a}{2y}$$

On doit s'assurer que $\frac{3x_p^2+a}{2y_p}$ n'est pas de la forme $\frac{0}{0}$
ou (ce qui est équivalent) que les dérivées partielles $\frac{\partial \Phi}{\partial x}$
et $\frac{\partial \Phi}{\partial y}$ ne s'annulent jamais simultanément

Supposons que cela se produise



$$\begin{cases} 3x_p^2 + a = 0 \\ 2y_p = 0 \end{cases} \Rightarrow y_p = 0 \Rightarrow x_p^3 + \underbrace{ax_p + b}_{= y_p^2} = 0$$

$$\Rightarrow \begin{cases} 3x_p^2 + a = 0 \\ x_p^3 + (-3x_p^2)x_p + b = 0 \end{cases}$$

$$\Rightarrow \begin{cases} a = -3x_p^2 \\ b = 2x_p^3 \end{cases} \Rightarrow 4a^3 + 27b^2 = 4(-3x_p^2)^3 + 27(2x_p^3)^2 = 0$$

Autrement dit : si il existe un point de E où la tangente
n'est pas définie, alors $\underline{4a^3 + 27b^2 = 0}$

Conclusion : $\begin{cases} \text{Avec l'hypothèse } 4a^3 + 27b^2 \neq 0 \\ \text{on n'a jamais cette situation} \end{cases}$

Grâce aux familles d'addition, la propriété d'associativité:

$$\forall P, Q, R \in E, \boxed{P + (Q + R) = (P + Q) + R}$$

se ramène à vérifier des identités sur des familles

$$E = \{(x, y) \in \mathbb{R}^2 / y^2 = x^3 + ax + b\} \cup \{O\}$$

$(E, +)$ est un groupe

On peut faire la même chose en remplaçant \mathbb{R} par n'importe quel corps (et en particulier par un corps fini)

en considérant que les familles d'addition
sont la définition de l'addition

& $K = \text{corps}$

$$E = \{(x, y) \in K^2, y^2 = x^3 + ax + b\} \cup \{O\}$$

$+$: opération d'addition de points définie par
les familles d'addition

alors $(E, +)$ est un groupe commutatif

Ici, On va considérer le corps $K = (\mathbb{Z}/p\mathbb{Z}, +, \times)$

$$\begin{aligned} &= \mathbb{F}_p \\ &= GF(p) \\ &= \mathbb{Z}_p \end{aligned}$$