

# Corps finis et courbes elliptiques

---

Guillaume Hanrot - LORIA / INRIA Lorraine

Rencontres arithmétique de l'Informatique Mathématique

22-25 janvier 2007, Montpellier.

# Plan

---

1. Introduction
2. Généralités
3. Corps finis
  - (a) Aspects mathématiques
  - (b) Grande caractéristique
  - (c) Petite caractéristique
4. Courbes elliptiques
  - (a) Aspects mathématiques
  - (b) Aspects algorithmiques

# Introduction

---

Pourquoi calculer avec des corps finis et des courbes elliptiques ?

- Parce que ce sont des objets mathématiques classiques et importants ;

# Introduction

---

Pourquoi calculer avec des corps finis et des courbes elliptiques ?

- Parce que ce sont des objets mathématiques classiques et importants ;
- Parce que ca sert à chiffrer en crypto ;

# Introduction

---

Pourquoi calculer avec des corps finis et des courbes elliptiques ?

- Parce que ce sont des objets mathématiques classiques et importants ;
- Parce que ca sert à chiffrer en crypto ;
- Parce que ca sert à factoriser ;

# Introduction

---

Pourquoi calculer avec des corps finis et des courbes elliptiques ?

- Parce que ce sont des objets mathématiques classiques et importants ;
- Parce que ca sert à chiffrer en crypto ;
- Parce que ca sert à factoriser ;
- **Parce que c'est rigolo.**

Comment calculer avec des corps finis et des courbes elliptiques ?

- Avec un ordinateur ;

# Introduction

---

Pourquoi calculer avec des corps finis et des courbes elliptiques ?

- Parce que ce sont des objets mathématiques classiques et importants ;
- Parce que ca sert à chiffrer en crypto ;
- Parce que ca sert à factoriser ;
- **Parce que c'est rigolo.**

Comment calculer avec des corps finis et des courbes elliptiques ?

- Avec un ordinateur ;
- Le plus vite possible.

# La multiprécision en 1 transparent

---

(R)appel : entiers machine : entiers modulo  $2^w$  (sauf division).

## • Représentation

- Grand entier = tableau d'entiers machine ;
- Polynôme = tableau de coefficients ;
- Taille  $n = O(\log N)$  ou  $O(d)$  ;

# La multiprécision en 1 transparent

---

(R)appel : entiers machine : entiers modulo  $2^w$  (sauf division).

## • Représentation

• Grand entier = tableau d'entiers machine ;

• Polynôme = tableau de coefficients ;

• Taille  $n = O(\log N)$  ou  $O(d)$  ;

• **Addition, soustraction** en  $O(n)$  ;

# La multiprécision en 1 transparent

---

(R)appel : entiers machine : entiers modulo  $2^w$  (sauf division).

## • Représentation

• Grand entier = tableau d'entiers machine ;

• Polynôme = tableau de coefficients ;

• Taille  $n = O(\log N)$  ou  $O(d)$  ;

• **Addition, soustraction** en  $O(n)$  ;

• **Multiplication** en  $M(n) := O(n^2)$

# La multiprécision en 1 transparent

---

(R)appel : entiers machine : entiers modulo  $2^w$  (sauf division).

## • Représentation

• Grand entier = tableau d'entiers machine ;

• Polynôme = tableau de coefficients ;

• Taille  $n = O(\log N)$  ou  $O(d)$  ;

• **Addition, soustraction** en  $O(n)$  ;

• **Multiplication** en  $M(n) := O(n^2) \rightarrow O(n \log n(\log \log n))$  ;

# La multiprécision en 1 transparent

---

(R)appel : entiers machine : entiers modulo  $2^w$  (sauf division).

## • Représentation

• Grand entier = tableau d'entiers machine ;

• Polynôme = tableau de coefficients ;

• Taille  $n = O(\log N)$  ou  $O(d)$  ;

• **Addition, soustraction** en  $O(n)$  ;

• **Multiplication** en  $M(n) := O(n^2) \rightarrow O(n \log n (\log \log n))$  ;

• **Division** =  $O(M(n))$ .

# La multiprécision en 1 transparent

---

(R)appel : entiers machine : entiers modulo  $2^w$  (sauf division).

## • Représentation

• Grand entier = tableau d'entiers machine ;

• Polynôme = tableau de coefficients ;

• Taille  $n = O(\log N)$  ou  $O(d)$  ;

• **Addition, soustraction** en  $O(n)$  ;

• **Multiplication** en  $M(n) := O(n^2) \rightarrow O(n \log n (\log \log n))$  ;

• **Division** =  $O(M(n))$ .

Morales :

• Division  $>$  multiplication  $>>$  addition, soustraction.

• Vraie vie  $\neq$  asymptotique.

# La multiprécision en 2 transparents

---

## Exponentiation.

$g^n$  peut être calculé en  $O(\log n)$  au moyen des formules récursives

$$\begin{aligned}g^{2n} &= (g^n)^2 = (g^2)^n \\g^{2n+1} &= g \cdot (g^2)^n = g \cdot (g^n)^2\end{aligned}$$

## Inverse modulaire.

Algorithme d'Euclide étendu : ( $A = \mathbb{Z}, \mathbb{K}[X]$ ) si  $p, q \in A$ , on peut trouver en  $O(M(n) \log n)$  des éléments  $u$  et  $v$  tels que  $pu + qv = \gcd(u, v)$ .

---

# Partie I – Corps finis

# Corps finis - mathématiques

---

## **Théorème.**

- Tout corps fini est de cardinal  $p^k$ ,  $p$  premier.

# Corps finis - mathématiques

---

## Théorème.

- Tout corps fini est de cardinal  $p^k$ ,  $p$  premier.
- Pour tout  $(p, k)$ , il existe un corps de cardinal  $p^k$ , unique à *isomorphisme près*.

# Corps finis - mathématiques

---

## Théorème.

- Tout corps fini est de cardinal  $p^k$ ,  $p$  premier.
- Pour tout  $(p, k)$ , il existe un corps de cardinal  $p^k$ , unique à *isomorphisme près*.
- Si  $P(x) \in \mathbb{Z}[X]$  de degré  $k$ , est irréductible modulo  $p$ ,  $\mathbb{Z}[X]/(p, P(X))$  est un/le corps fini à  $p^k$  éléments.

# Corps finis - mathématiques

---

## Théorème.

- Tout corps fini est de cardinal  $p^k$ ,  $p$  premier.
- Pour tout  $(p, k)$ , il existe un corps de cardinal  $p^k$ , unique à *isomorphisme près*.
- Si  $P(x) \in \mathbb{Z}[X]$  de degré  $k$ , est irréductible modulo  $p$ ,  $\mathbb{Z}[X]/(p, P(X))$  est un/le corps fini à  $p^k$  éléments.

On “le” note  $\mathbb{F}_{p^k}$  ou  $GF(p^k)$ . Concrètement (et ensemblistement),

$$\mathbb{F}_{p^k} = \left\{ \sum_{i=0}^{k-1} a_i X^i, a_i \in (\mathbb{F}_p)^k \right\}.$$

$p$  est la *caractéristique* du corps, et  $\mathbb{F}_p \subset \mathbb{F}_{p^k}$ .

Deux cas typiques (et cousins) :

- $k = 1$  : corps premier.

# Corps finis - mathématiques

---

## Théorème.

- Tout corps fini est de cardinal  $p^k$ ,  $p$  premier.
- Pour tout  $(p, k)$ , il existe un corps de cardinal  $p^k$ , unique à *isomorphisme près*.
- Si  $P(x) \in \mathbb{Z}[X]$  de degré  $k$ , est irréductible modulo  $p$ ,  $\mathbb{Z}[X]/(p, P(X))$  est un/le corps fini à  $p^k$  éléments.

On “le” note  $\mathbb{F}_{p^k}$  ou  $GF(p^k)$ . Concrètement (et ensemblistement),

$$\mathbb{F}_{p^k} = \left\{ \sum_{i=0}^{k-1} a_i X^i, a_i \in (\mathbb{F}_p)^k \right\}.$$

$p$  est la *caractéristique* du corps, et  $\mathbb{F}_p \subset \mathbb{F}_{p^k}$ .

Deux cas typiques (et cousins) :

- $k = 1$  : corps premier.
- $p = 2$  ou  $p$  petit : grand degré.

# Corps finis - mathématiques

---

## Théorème.

- Tout corps fini est de cardinal  $p^k$ ,  $p$  premier.
- Pour tout  $(p, k)$ , il existe un corps de cardinal  $p^k$ , unique à *isomorphisme près*.
- Si  $P(x) \in \mathbb{Z}[X]$  de degré  $k$ , est irréductible modulo  $p$ ,  $\mathbb{Z}[X]/(p, P(X))$  est un/le corps fini à  $p^k$  éléments.

On “le” note  $\mathbb{F}_{p^k}$  ou  $GF(p^k)$ . Concrètement (et ensemblistement),

$$\mathbb{F}_{p^k} = \left\{ \sum_{i=0}^{k-1} a_i X^i, a_i \in (\mathbb{F}_p)^k \right\}.$$

$p$  est la *caractéristique* du corps, et  $\mathbb{F}_p \subset \mathbb{F}_{p^k}$ .

Deux cas typiques (et cousins) et un mal fichu :

- $k = 1$  : corps premier.
- $p = 2$  ou  $p$  petit : grand degré.
- $p$  moyen et  $k$  moyen,  $\log p \asymp k$ .

# Tordons le cou à quelques idées reçues.

---

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.$$

# Tordons le cou à quelques idées reçues.

---

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$$

$$\mathbb{F}_{p^n} \neq (\mathbb{Z}/p\mathbb{Z})^n$$

# Tordons le cou à quelques idées reçues.

---

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$$

$$\mathbb{F}_{p^n} \neq (\mathbb{Z}/p\mathbb{Z})^n \text{ (encore que...)}$$

# Un peu de philosophie

---

- Arithmétique des corps finis : catalogue d'idées.
- Cours non exhaustif. Cf. HEHCC.

# Un peu de philosophie

---

- Arithmétique des corps finis : catalogue d'idées.
- Cours non exhaustif. Cf. HEHCC.
- Différentes représentations  $\Rightarrow$  différentes opérations.

# Un peu de philosophie

---

- Arithmétique des corps finis : catalogue d'idées.
- Cours non exhaustif. Cf. HEHCC.
- Différentes représentations  $\Rightarrow$  différentes opérations.
- Le bon choix dépend :
  - de la taille de corps ;
  - du type de corps (premier, grand degré) ;
  - du type d'opérations à effectuer.

Analyse asymptotique peu utile dans le choix de la meilleure solution (le diable est dans les constantes des  $O$ ).

---

# Partie 1.1 – Corps premiers

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Représentation

- $x \in \mathbb{Z}/p\mathbb{Z} \leftrightarrow \tilde{x} \in [0, p - 1]$ .
- $x \in \mathbb{Z}/p\mathbb{Z} \leftrightarrow \tilde{x} \in [-(p - 1)/2, (p - 1)/2]$ .
- Représentations redondantes :  $x \in \mathbb{Z}/p\mathbb{Z} \leftrightarrow$  un  $\tilde{x} \in [-a(p - 1), b(p - 1)]$ .
- dans deux ou trois transparents : représentation de Montgomery.

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Addition, soustraction

- $x, y \in \mathbb{Z}/p\mathbb{Z}$ ,  $[x], [y] \in \mathbb{Z}$  leur représentation ;
- $u \leftarrow [x] \pm [y]$  ;

En général,  $u$  n'est pas une représentation valide

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Addition, soustraction

- $x, y \in \mathbb{Z}/p\mathbb{Z}$ ,  $[x], [y] \in \mathbb{Z}$  leur représentation ;
- $u \leftarrow [x] \pm [y]$  ;

En général,  $u$  n'est pas une représentation valide  $\Rightarrow$  ajouter une étape de *réduction*.

- $[z] \leftarrow RED(u, N)$ .

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Réduction.

Donnée :  $x \in \mathbb{Z}, p$ ; Résultat :  $[x]$ , une représentation valide de  $x \pmod{p}$ .

Représentation  $[0, p - 1]$  :  $RED(x) = x - \lfloor x/p \rfloor p$ .

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Réduction.

Donnée :  $x \in \mathbb{Z}, p$ ; Résultat :  $[x]$ , une représentation valide de  $x \pmod{p}$ .

Représentation  $[0, p - 1]$  :  $RED(x) = x - \lfloor x/p \rfloor p$ .

Représentation centrée :  $RED(x) = x - \lfloor x/p \rfloor p$ .

Coût = 1 division avec reste =  $O(M(\log p))$ .

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Réduction.

Donnée :  $x \in \mathbb{Z}, p$ ; Résultat :  $[x]$ , une représentation valide de  $x \pmod{p}$ .

Représentation  $[0, p - 1]$  :  $RED(x) = x - \lfloor x/p \rfloor p$ .

Représentation centrée :  $RED(x) = x - \lfloor x/p \rfloor p$ .

Coût = 1 division avec reste =  $O(M(\log p))$ .

**Prétraitement** :  $\alpha \approx 1/p$  en précision suffisante  $\Rightarrow \lfloor x/p \rfloor = \lfloor \alpha x \rfloor$ .

Coût = 1 multiplication.

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Réduction.

Donnée :  $x \in \mathbb{Z}, p$ ; Résultat :  $[x]$ , une représentation valide de  $x \pmod p$ .

Représentation  $[0, p - 1]$  :  $RED(x) = x - \lfloor x/p \rfloor p$ .

Représentation centrée :  $RED(x) = x - \lfloor x/p \rfloor p$ .

Coût = 1 division avec reste =  $O(M(\log p))$ .

**Prétraitement** :  $\alpha \approx 1/p$  en précision suffisante  $\Rightarrow \lfloor x/p \rfloor = \lfloor \alpha x \rfloor$ .

Coût = 1 multiplication.

**Retour sur l'addition** :  $\text{tmp} \in [0, 2p - 2]$

if ( $\text{tmp} \geq p$ )  $\text{tmp} -= p$  ;

• Coût total = 2 additions/soustractions entières.

• Représentation redondante : évitent les réductions systématiques.

*Permettent des réductions "approchées". Certaines valeurs de  $p$  permettent des réductions rapides, eg.  $p = 2^N - 1$ .*

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Multiplication

•  $u \leftarrow [x][y]$

•  $[z] \leftarrow RED(u, p).$

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Multiplication

•  $u \leftarrow [x][y]$

•  $[z] \leftarrow RED(u, p).$

Possibilité de mélanger multiplication et réduction.

Coût : 1 multiplication + 1 division avec reste.

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$

---

## Multiplication

- $u \leftarrow [x][y]$
- $[z] \leftarrow RED(u, p)$ .

Possibilité de mélanger multiplication et réduction.

Coût : 1 multiplication + 1 division avec reste.

## Division

- Inversion (via Euclide étendu et alias) + multiplication + réduction ;
- Très coûteux, doit être évité autant que possible.

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$ – Montgomery

---

## Représentation de Montgomery :

- $R > p$ ,  $\gcd(R, p) = 1$ . Précalcul de  $p' = p^{-1} \bmod R$  et de  $R' = R^{-1} \bmod p$ .
- $x \in \mathbb{Z}/p\mathbb{Z} \leftrightarrow F(x) = (xR \bmod p) \in [0, N - 1]$ .

## Changements de représentation :

- Représentation “usuelle”  $\rightarrow$  Montgomery :

$$[x] \rightarrow F(x) = RED(xR, p).$$

- Montgomery  $\rightarrow$  naturelle :

$$F(x) \rightarrow [x] = RED(F(x)R', p).$$

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$ – Montgomery (II)

---

**Changement de représentation (II)** : Montgomery REDC. Hyp :  $u < p^2$ .

REDC( $u$ ,  $p$ )

$k \leftarrow -up' \pmod R$

$t \leftarrow (u + kp) / R$

if ( $t < p$ ) return  $t$  else return ( $t - p$ )

Résultat  $x \in [0, p - 1]$  avec  $F(x) = u \pmod p$ .

**Intérêt** : si  $R = 2^{nw}$ , REDC = 2 multiplications + 1 test + 1.5 addition/soustraction ; souvent  $< 1$  multiplication + 1 division avec reste.

**Remarque** : normal  $\rightarrow$  Montgomery peut aussi se calculer comme  $F(x) = REDC(xp^2)$  (précalcul de  $p^2 \pmod R$ ).

*Version 2-adique du précalcul de  $1/p$ , sans les problèmes de précision.*

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$ – Montgomery (III)

---

## Multiplication

$$\begin{aligned} F(x)F(y) &= xyR^2 \bmod p \\ &= F(xy)R \bmod p, \\ &= F(F(xy)), \end{aligned}$$

ou encore  $F(xy) = REDC(F(x)F(y), p)$ .

Coût = 1 multiplication + 1 REDC < 1 multiplication + 1 RED.

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$ – Montgomery (III)

---

## Racine carrée

- Tonelli-Shanks, Berlekamp.
- Polynomial probabiliste.
- Déterministe sous GRH.

# Corps premiers, i.e. $\mathbb{Z}/p\mathbb{Z}$ – Montgomery (III)

---

## Racine carrée

- Tonelli-Shanks, Berlekamp.
- Polynomial probabiliste.
- Déterministe sous GRH.

Berlekamp :  $u \in \mathbb{Z}/p\mathbb{Z}$  carré ; pour  $\alpha \in_R \mathbb{Z}/p\mathbb{Z}$ , calculer

$$\gcd((X - \alpha)^{(p-1)/2} - 1, X^2 - u).$$

Avec proba.  $1/2$ ,  $X = t$  avec  $t^2 = u$ .

*Attention au calcul du pgcd!!*

---

# Partie 1.2 – Caractéristique 2

# $\mathbb{F}_{2^n}$ – structure

---

## Structure additive.

- $\mathbb{F}_{p^n}$  est un  $\mathbb{F}_p$ -ev de dimension  $n$  ;
- $\Rightarrow (e_i)_{0 \leq i < n}$  base ;
- addition coordonnée par coordonnée dans  $\mathbb{Z}/p\mathbb{Z}$  ;
- choisir des bases facilitant la multiplication.

# $\mathbb{F}_{2^n}$ – structure

---

## Structure additive.

- $\mathbb{F}_{p^n}$  est un  $\mathbb{F}_p$ -ev de dimension  $n$  ;
- $\Rightarrow (e_i)_{0 \leq i < n}$  base ;
- addition coordonnée par coordonnée dans  $\mathbb{Z}/p\mathbb{Z}$  ;
- choisir des bases facilitant la multiplication.

## Structure multiplicative.

- $(\mathbb{F}_{p^n})^*$  est cyclique ;
- $\exists x \in \mathbb{F}_{p^n}; \mathbb{F}_{p^n} = \{0\} \cup \{x^\ell, \ell \in [0, p^n - 2]\}$ .
- Représenter  $y$  par  $\ell = \log_x y$  ?
- Multiplication peu coûteuse ;
- Addition : table ou revenir en représentation “linéaire” ;
- Passage d’une représentation à l’autre = log discret  $\Rightarrow$  trop cher ;
- Limité aux petits corps.

# $\mathbb{F}_{2^n}$ – logarithme de Zech

---

Représentation adaptée aux très petits corps.

- $\alpha$  générateur de  $(\mathbb{F}_{p^n})^*$  ;
- $u \in \mathbb{F}_{2^n} \leftrightarrow [u] = k$  avec  $u = \alpha^k$ .
- $T[k] \leftarrow j$  tel que  $\alpha^j = 1 + \alpha^k$ .
- On a

$$\alpha^u + \alpha^v = \alpha^u(1 + \alpha^{v-u}),$$

d'où  $[u] + [v] = [u + T[(v - u) \bmod (2^n - 1)] \bmod (2^n - 1)]$ .

- $[u][v] = [u + v \bmod (2^n - 1)]$ .

Stockage  $O(2^n) \Rightarrow$  réservé aux petits corps.

# $\mathbb{F}_{2^n}$ – représentation polynomiale

---

Soit  $P$  irréductible de degré  $n$  sur  $\mathbb{F}_2$ . On a

$$\mathbb{F}_{p^k} = \left\{ \sum_{i=0}^{k-1} a_i X^i, a_i \in (\mathbb{F}_p)^k \right\}.$$

Base  $1, X, \dots, X^{k-1}$ .

Ex.  $n = 2, P = X^2 + X + 1$ .

$$\mathbb{F}_4 = \{0, 1, X, X + 1\}.$$

**Représentation.**  $u \in \mathbb{F}_{2^n} \leftrightarrow [u] \in \mathbb{Z}/2\mathbb{Z}[X]$ , de degré  $< k$ .

**Addition, soustraction.** Coordonnée par coordonnée. Pas de réduction.

Ex.  $X + (X + 1) = 1, (X + 1) + 1 = X$ .

# $F_{2^n}$ – représentation polynomiale

---

## Réduction.

- $RED(u, P) = u - (u \operatorname{div} P)P$ . 1 division avec reste.
- Précalcul de  $1/P \bmod X^n \Rightarrow 2$  multiplications de degré  $n + 1$  soustraction.
- Cas d'un polynôme  $P$  creux : si  $w(P) = k$ , la division coûte  $kn$  opérations.

Pratique : utiliser un trinôme pour  $P$  (binôme si  $p \neq 2$ ), à défaut un pentanôme.

*Proba d'irréductibilité  $\approx 1/n$  ; nombre de trinômes  $\approx n$  ; nombre de pentanômes  $\approx n^3$ .*

*Représentations redondantes : calculer modulo  $P$  très creux ayant un facteur irréductible de degré  $n$ .*

# $\mathbb{F}_{2^n}$ – représentation polynomiale

---

## Multiplication.

- Comme dans le cas premier :
- $t \leftarrow [u][v]$
- $[w] \leftarrow RED(t, P)$ .
- Multiplication polynomiale, puis réduction modulo  $P$  ;
- 1 multiplication + 1 réduction.
- On peut mélanger les deux.

## Division

- Euclide étendu (ou autre), puis multiplication.

## Frobenius – $x \mapsto x^2$ .

- Opération importante dans certaines applications ;
- Au pire, une multiplication.

# $F_{2^n}$ – bases normales

---

Choisir  $\beta$  tel que  $\beta, \beta^2, \dots, \beta^{2^{n-1}}$  base.

**Addition, soustraction.** Coordonnée par coordonnée.

**Frobenius.** Décalage cyclique des coordonnées :

$$\left( \sum_{i=0}^{n-1} a_i \beta^{2^i} \right) = \sum_{i=0}^n a_i \beta^{2^{i+1}}$$

# $F_{2^n}$ – bases normales

---

**Multiplication.** Précalculer la matrice  $\beta \cdot \beta^{2^i} = \sum_{j=0}^{n-1} m_{ij} \beta^{2^j}$ . Table complète :

$$\beta^{2^h} \cdot \beta^{2^i} = \left( \beta \cdot \beta^{2^{i-h}} \right)^{2^h} = \sum_{j=0}^{n-1} m_{i-h, j-h} \beta^{2^j}.$$

# $F_{2^n}$ – bases normales

---

**Multiplication.** Précalculer la matrice  $\beta \cdot \beta^{2^i} = \sum_{j=0}^{n-1} m_{ij} \beta^{2^j}$ . Table complète :

$$\beta^{2^h} \cdot \beta^{2^i} = \left( \beta \cdot \beta^{2^{i-h}} \right)^{2^h} = \sum_{j=0}^{n-1} m_{i-h, j-h} \beta^{2^j}.$$

$$\sum_{j=0}^{n-1} u_j \beta^{2^j} \sum_{j=0}^{n-1} v_j \beta^{2^j} = \sum_{j=0}^{n-1} \left( \sum_{k,l=0}^{n-1} u_k v_l t_{k-l, j-l} \right) \beta^{2^j}.$$

Coût de la multiplication lié au poids de la matrice  $M$ .

*Bases normales optimales :  $w(M) = 2n - 1$ . N'existe pas toujours.*

# $\mathbb{F}_{p^k}$ , $p$ , $k$ moyens

---

Addition, soustraction RAS.

Problème :

- multiplication de polynômes de degré moyen ;
- multiplication de coefficients de taille moyenne ;

# $\mathbb{F}_{p^k}$ , $p$ , $k$ moyens

---

Addition, soustraction RAS.

Problème :

- multiplication de polynômes de degré moyen ;
- multiplication de coefficients de taille moyenne ;
- utilisation d'algorithmes quadratiques ;
- ... alors que l'objet manipulé est globalement grand.
- eg  $k \approx 10$ ,  $\log_2 p \approx 100$ .

# Représentation de Kronecker-Schönhage

---

• Calcul de

$$P \cdot Q = \sum_{l=0}^{2k-1} X^l \sum_{i+j=l} p_i q_j$$

;

• Coefs de  $PQ$  sont  $\leq k(p-1)^2$ .

# Représentation de Kronecker-Schönhage

---

• Calcul de

$$P \cdot Q = \sum_{l=0}^{2k-1} X^l \sum_{i+j=l} p_i q_j$$

;

- Coefs de  $PQ$  sont  $\leq k(p-1)^2$ .
- Choisir  $A = 2^z > k(p-1)^2$ .
- Calculer  $B = P(A)Q(A)$  (taille  $k \log_2 p$ , multiplication rapide);
- On a  $B = PQ(A)$ ;

# Représentation de Kronecker-Schönhage

---

- Calcul de

$$P \cdot Q = \sum_{l=0}^{2k-1} X^l \sum_{i+j=l} p_i q_j$$

;

- Coefs de  $PQ$  sont  $\leq k(p-1)^2$ .
- Choisir  $A = 2^z > k(p-1)^2$ .
- Calculer  $B = P(A)Q(A)$  (taille  $k \log_2 p$ , multiplication rapide);
- On a  $B = PQ(A)$ ;

Les coefs de  $PQ$  sont est le développement en base  $2^z$  de  $B$ .

---

# Partie II – Courbes elliptiques

# Courbes elliptiques

---

Déf.  $E/\mathbb{K} : a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$ .

Modèle de Weierstraß : courbe d'équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

**+ non singulier + ajouter un point “ $y \rightarrow \infty$ ”.**

Si  $c(K) > 3$ , on se ramène à

$$Y^2 = X^3 + AX + B,$$

**+  $4A^3 + 27B^2 \neq 0$  + toujours un point “ $y \rightarrow \infty$ ”.**

Si  $c(K) = 2$ , on se ramène à

$$y^2 + xy = x^3 + Ax^2 + B \text{ ou } y^2 + Ay = x^3 + Bx + C.$$

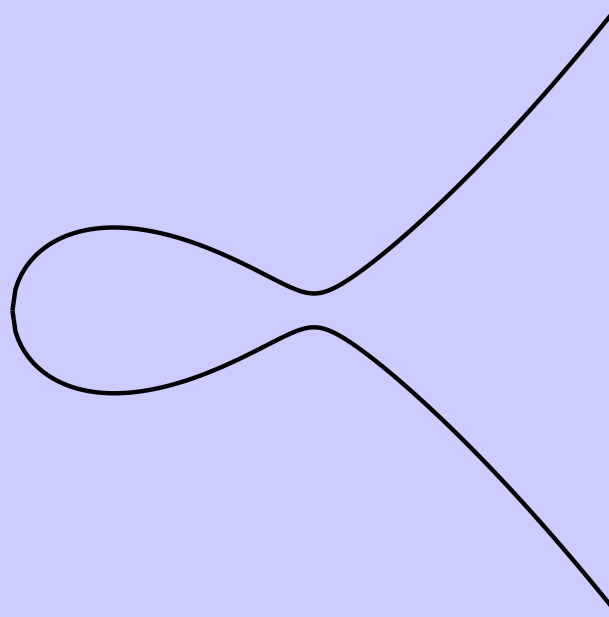
(plus etc...)

Dans la suite,  $c(K) > 3$ .

# Courbes elliptiques – loi de groupe

---

Trois points alignés se somment à 0.

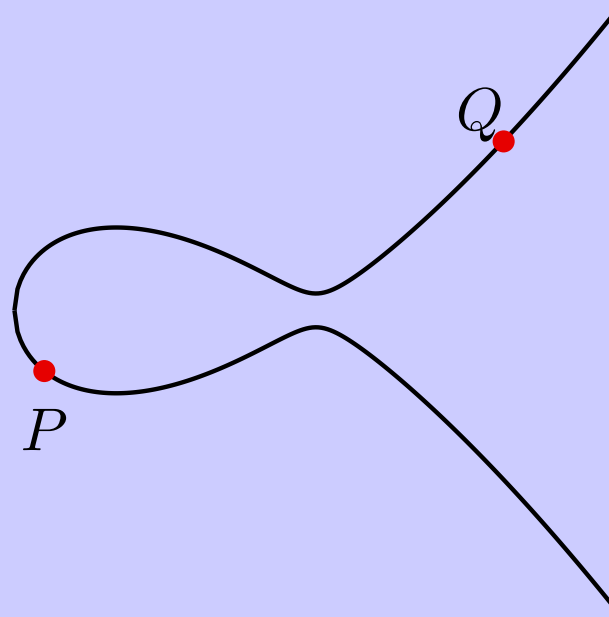


↑ (loin) :  $0_E = \infty$

# Courbes elliptiques – loi de groupe

---

Trois points alignés se somment à 0.

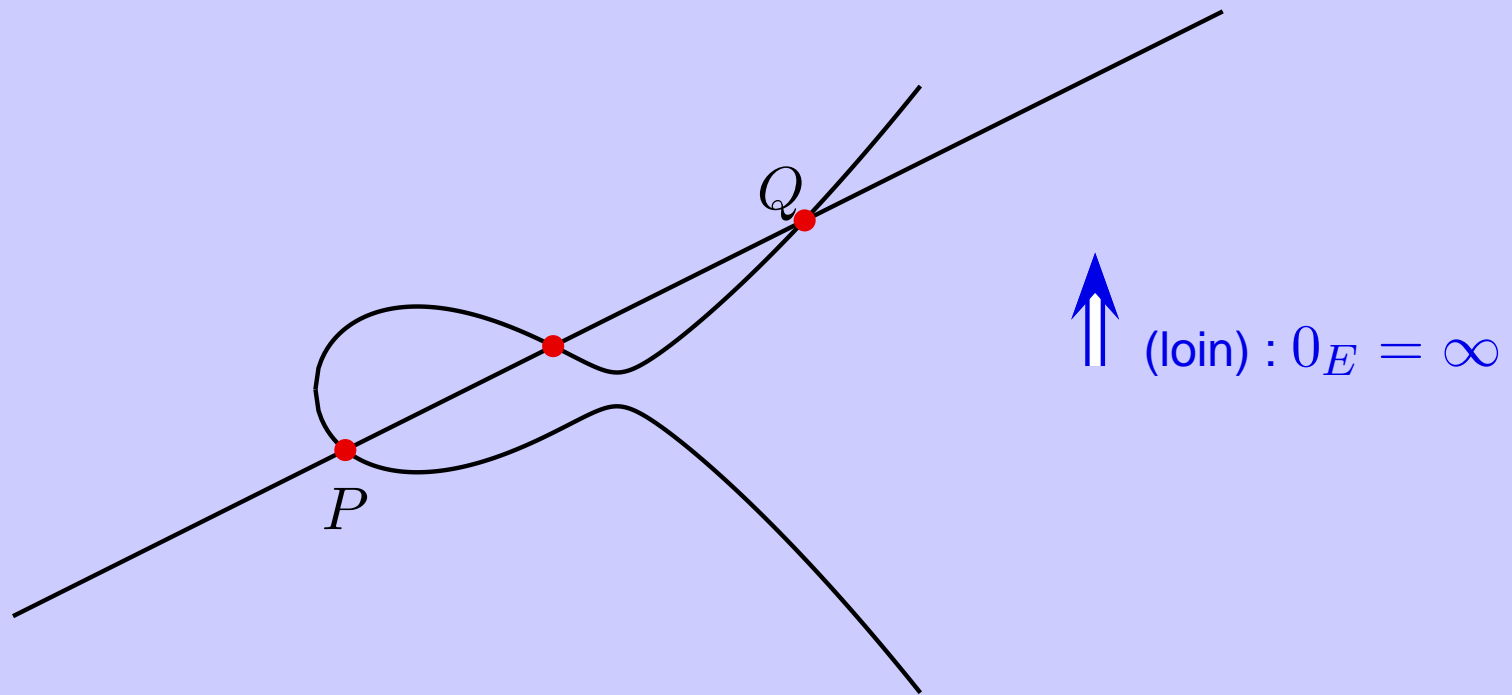


↑ (loin) :  $0_E = \infty$

# Courbes elliptiques – loi de groupe

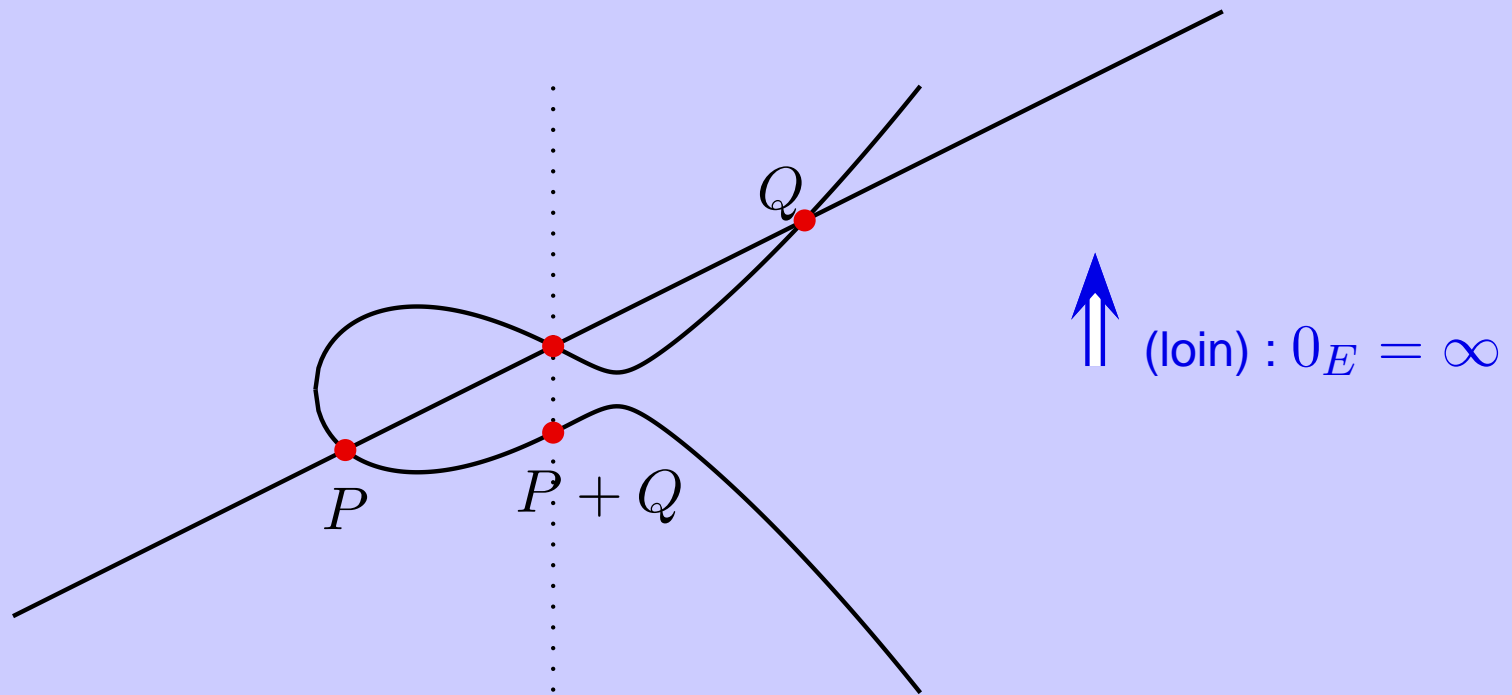
---

Trois points alignés se somment à 0.



# Courbes elliptiques – loi de groupe

Trois points alignés se somment à 0.



Opposé de  $(x, y) = (x, -y)$ .

# Courbes elliptiques – représentation des points

---

C'est là que les ennuis commencent.

- on veut aller très vite (encore que...);
- différentes représentations possibles ;
- il faut encore réfléchir (et c'est dur).

# Courbes elliptiques – représentation des points

---

C'est là que les ennuis commencent.

- on veut aller très vite (encore que...);
- différentes représentations possibles ;
- il faut encore réfléchir (et c'est dur).

Coordonnées *affines* :  $(x, y) \leftrightarrow (x, y)$ . Infini à part.

# Courbes elliptiques – représentation des points

---

C'est là que les ennuis commencent.

- on veut aller très vite (encore que...);
- différentes représentations possibles;
- il faut encore réfléchir (et c'est dur).

Coordonnées *affines* :  $(x, y) \leftrightarrow (x, y)$ . Infini à part.

Coordonnées *projectives* :  $(x, y) \in \mathbb{K}^2 \leftrightarrow (u : v : w), u/w = x, v/w = y$ . Redondant.

Infini  $\leftrightarrow (0 : 1 : 0)$ .

# Courbes elliptiques – représentation des points

---

C'est là que les ennuis commencent.

- on veut aller très vite (encore que...);
- différentes représentations possibles;
- il faut encore réfléchir (et c'est dur).

Coordonnées *affines* :  $(x, y) \leftrightarrow (x, y)$ . Infini à part.

Coordonnées *projectives* :  $(x, y) \in \mathbb{K}^2 \leftrightarrow (u : v : w), u/w = x, v/w = y$ . Redondant.  
Infini  $\leftrightarrow (0 : 1 : 0)$ .

Coordonnées *jacobiennes* :  $(x, y) \in \mathbb{K}^2 \leftrightarrow (X : Y : Z), X/Z^2 = x, Y/Z^3 = y$ .  
Redondant. Infini  $\leftrightarrow (1 : 1 : 0)$ .

# Courbes elliptiques – formules

---

Formules dans le cas affine,  $c(K) > 3$  :  $(x_P, y_P) + (x_Q, y_Q) = (x_R, y_R)$ .

• Cas 1 :  $x_P \neq x_Q$ .

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q}, \mu = y_P - \lambda x_P$$

# Courbes elliptiques – formules

---

Formules dans le cas affine,  $c(K) > 3$  :  $(x_P, y_P) + (x_Q, y_Q) = (x_R, y_R)$ .

• Cas 1 :  $x_P \neq x_Q$ .

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q}, \mu = y_P - \lambda x_P$$

$$(x_R, y_R) = (\lambda^2 - x_P - x_Q, -\lambda x_R - \mu).$$

# Courbes elliptiques – formules

---

Formules dans le cas affine,  $c(K) > 3$  :  $(x_P, y_P) + (x_Q, y_Q) = (x_R, y_R)$ .

• Cas 1 :  $x_P \neq x_Q$ .

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q}, \mu = y_P - \lambda x_P$$

.

$$(x_R, y_R) = (\lambda^2 - x_P - x_Q, -\lambda x_R - \mu).$$

Mieux :  $y_R = \lambda(x_P - x_R) - y_P$ .

• Cas 2 :  $x_P = x_Q$ .

•  $y_P = -y_Q \Rightarrow R = \infty$ .

•  $y_P = y_Q$  :

$$\lambda = \frac{3x_P^2 + A}{2y_P},$$

reste idem.

Addition : I+2M+C ; doublement : I+2M+2C.

# Courbes elliptiques – quelle représentation ?

---

Où faire son marché ?

- Cas affine :  $I + 2M + C / I + 2M + 2C$
- Cas projectif :  $12M + 2C / 7M + 5C$
- Cas jacobien :  $12M + 4C / 4M + 6C$

Et on peut mixer tout ça. Par exemple :

- $A + A \rightarrow J : 8M + 3C ;$
- $2 \cdot A \rightarrow J : 2M + 4C.$

Le choix dépend des vitesses comparées  $I/M/C$ .

# Compression des points (Montgomery)

---

Idée :  $x_P = x_Q \Rightarrow P = \pm Q$  (travailler dans  $E/\{\pm 1\}$ ).

- représenter  $\{P, -P\}$  par  $x_P$  ;
- addition pas définie :  $\{P, -P\} + \{Q, -Q\} = \{\pm P, \pm Q\}$ .
- exponentiation définie ! :  $n\{P, -P\} = \{nP, -nP\}$ .
- opération  $(\{P, -P\}, \{Q, -Q\}, \{P - Q, Q - P\}) \mapsto \{P + Q, Q + P\}$  définie.
- formules

$$X_{P+Q} = \frac{-4B(X_P + X_Q) + (X_P X_Q - A)^2}{X_{P-Q}(X_P - X_Q)^2},$$

$$X_{2P} = \frac{(X_P^2 - A)^2 - 8BX_P}{4(X_P(X_P^2 + A) + B)}.$$

meilleures formules sur la courbe  $By^2 = x^3 + Ax^2 + x$ .

# Exponentiation avec compression, fin.

---

Calcul de  $(\{2nP, -2nP\}, \{(2n+1)P, (-2n-1)P\})$  ou  
 $(\{(2n+1)P, (-2n-1)P\}, \{(2n+2)P, (-2n-2)P\})$  via



$$(\{nP, -nP\}, \{nP, -nP\}, \{\infty, \infty\}) \rightarrow \{2nP, -2nP\}.$$

# Exponentiation avec compression, fin.

---

Calcul de  $(\{2nP, -2nP\}, \{(2n+1)P, (-2n-1)P\})$  ou  
 $(\{(2n+1)P, (-2n-1)P\}, \{(2n+2)P, (-2n-2)P\})$  via



$$(\{nP, -nP\}, \{nP, -nP\}, \{\infty, \infty\}) \rightarrow \{2nP, -2nP\}.$$



$$(\{nP, -nP\}, \{(n+1)P, -(n+1)P\}, \{P, -P\}) \rightarrow \{(2n+1)P, -(2n+1)P\}.$$



... plus méthodes binaires habituelles.

# Conclusion

---

- Sujets multiformes suivant les applications visées ;

# Conclusion

---

- Sujets multiformes suivant les applications visées ;
- Représentations différentes  $\leftrightarrow$  problèmes et qualités différentes ;

# Conclusion

---

- Sujets multiformes suivant les applications visées ;
- Représentations différentes  $\leftrightarrow$  problèmes et qualités différentes ;
- Boîtes à outils plutôt que solutions toutes faites ;

# Conclusion

---

- Sujets multiformes suivant les applications visées ;
- Représentations différentes  $\leftrightarrow$  problèmes et qualités différentes ;
- Boîtes à outils plutôt que solutions toutes faites ;
- Vérité très loin du monde asymptotique...

# Conclusion

---

- Sujets multiformes suivant les applications visées ;
- Représentations différentes  $\leftrightarrow$  problèmes et qualités différentes ;
- Boîtes à outils plutôt que solutions toutes faites ;
- Vérité très loin du monde asymptotique...
- et dépendant largement du hardware.