Introduction aux courbes elliptiques

Guillaume Hanrot - LORIA / INRIA Lorraine

École jeunes chercheurs en informatique mathématique.

Plan

1. Introduction
2. Prérequis : multiprécision, corps finis
3. Courbes elliptiques
   (a) Aspects mathématiques
   (b) Arithmétique
   (c) Autour de la cardinalité

Introduction

Pourquoi faire des courbes elliptiques ?

- Parce que ce sont des objets mathématiques classiques et importants ;
- Parce que ca sert à chiffrer en crypto (cf exposé ET) ;
- Parce que ça sert pour la primalité (cf exposé FM) ;
- Parce que ca sert à factoriser (cf exposé ET) ;
- **Parce que c'est rigolo**.

Comment calculer avec des courbes elliptiques ?

- Avec un ordinateur ;
- Le plus vite possible.

La multiprécision en 2 transparents

(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 $\gg$ 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 $pu + qv = \gcd(p, q)$.

Si $\gcd(p, q) = 1$, $v = q^{-1} \bmod p$ et $u = p^{-1} \bmod q$.

Rappels sur les corps finis

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 un moins typique :

- $k = 1$: 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.

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

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

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

Courbes elliptiques - généralités

Courbes elliptiques

Point de vue du mathématicien : courbe elliptique sur $\mathbb{K}$ = couple (C, P) où C est une courbe algébrique de genre 1 définie sur $\mathbb{K}$ et P un point de $C(K)$.

Csq. du thm de Riemann-Roch :

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 "$y \to \infty$".

Modèle de Weierstraß court

- $c(K) > 3$:

$$y^2 = x^3 + Ax + B,$$

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

- $c(K) = 2$:

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

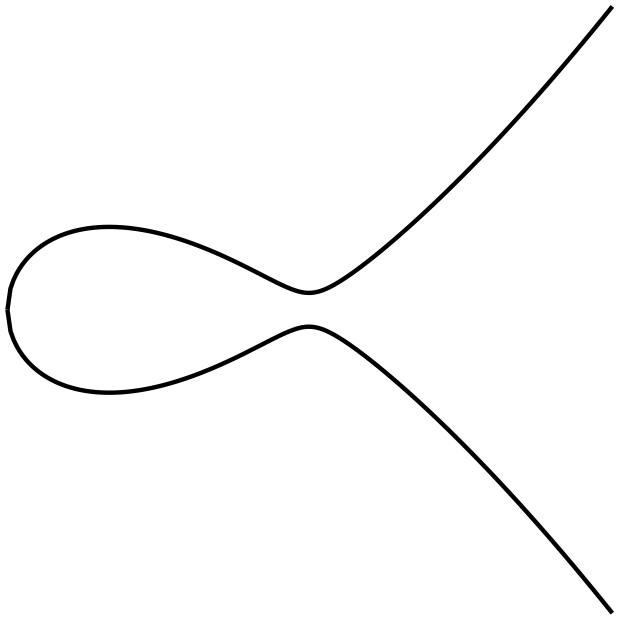
(plus etc...).

- D’autres modèles possibles, eg.

$$y^2 = x^3 + Ax^2 + Bx.$$

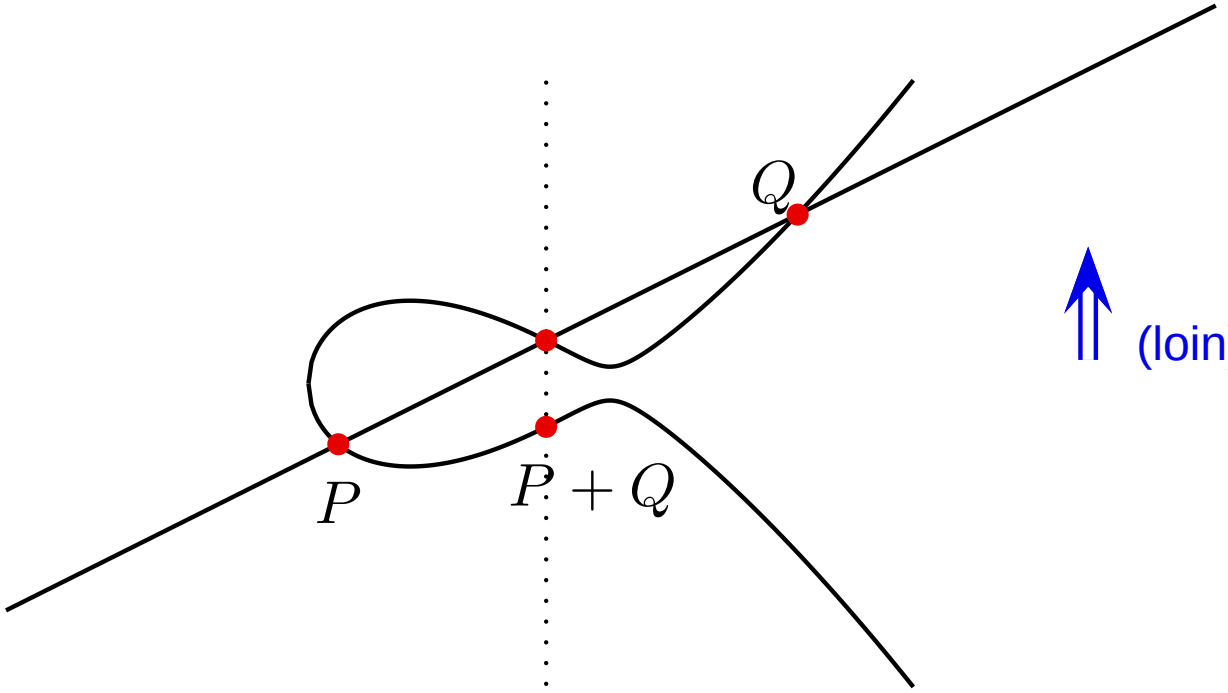
Courbes elliptiques - de quoi ça a l'air ?

Sur $\mathbb{R}$:



Courbes elliptiques – loi de groupe

Point de vue géométrique : trois points alignés se somment à 0.



Courbes elliptiques – loi de groupe

Point de vue algébrique :

- $\mathbb{Z}[C(\mathbb{K})] = \sum_{P \in C(\mathbb{K})} n_P(P)$ le groupe libre engendré par $C(\mathbb{K})$;
- $\mathbb{Z}[C(\mathbb{K})]^0$ le sous-groupe tel que $\sum_P n_P = 0$.
- $L = \{(P) + (Q) + (R) - 3(\infty)\}$, avec P, Q, R alignés sur la courbe.

Th. Chaque classe de $\mathbb{Z}[C(\mathbb{K})]^0/L$ contient un et un seul élément de la forme $(P) - (\infty)$ ou 0.

Courbes elliptiques – loi de groupe

- bijection entre $\mathbb{Z}[C(\mathbb{K})]^0/L$ et $C(\mathbb{K})$.
- $\oplus$ sur $C(\mathbb{K}) \leftrightarrow +$ sur $\mathbb{Z}[C(\mathbb{K})]^0/L$.

Corollaire. $(C(\mathbb{K}), \oplus)$ est un groupe abélien.

Généralisations pour les curieux.

- $L \hookrightarrow$ intersections de courbes plus compliquées avec C ;
- $C(\mathbb{K}) \hookrightarrow$ (presque)$C(\mathbb{K})^g$
- **jacobienne** d'une courbe algébrique.

Bilan.

- Étant donné (presque tout) $(A, B) \in \mathbb{K}^2$ on sait construire une courbe $E_{A,B}(\mathbb{K})$, avec une loi de groupe ;
- Pourquoi faire un groupe ?
  - Pour faire de la crypto !
  - Si $G(\mathbb{Q})$ se “réduit modulo N”, pour factoriser N ou étudier la primalité de N !

Dans tous les cas, on a besoin de

- $P \mapsto -P$;
- $(P, Q) \mapsto P + Q$;
- $(n, P) \mapsto n \cdot P$.

très optimisé.

Courbes elliptiques - arithmétique

Courbes elliptiques – formules

Cas $c(\mathbb{K}) \neq 2, 3$, E : $y^2 = x^3 + Ax + B$.

Additionner $P = (x_1, y_1)$ et $Q = (x_2, y_2)$.

- Opposé de $(x, y) = (x, -y)$.
- Addition.
  - Cas $P = -Q$, $P + Q = \infty$.
  - Cas $P \neq \pm Q$, droite $(PQ) : y = \lambda x + \mu$, avec

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \mu = y_1 - \lambda x_1.$$

  - Cas $P = Q$, droite (PQ) :

$$\lambda = \frac{3x_1^2 + A}{2y_1}, \mu = y_1 - \lambda x_1.$$

Courbes elliptiques – formules (2)

On cherche l'intersection

$$\begin{cases} y^2 = x^3 + Ax + B, \\ y = \lambda x + \mu. \end{cases}$$

On reporte la deuxième dans la première :

$$(\lambda x + \mu)^2 = x^3 + Ax + B. \tag{1}$$

Il y a un truc !

$$x_1 + x_2 + x_3 = -\text{coeff. de } x^2$$

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda x_3 + \mu = y_1 + \lambda(x_3 - x_1).$$

Droite joignant (x_3, y_3) et le point à l'infini : $x = x_3$

$$P + Q = (x_3, -y_3).$$

$c(\mathbb{K}) = 2 \Rightarrow$ exercice (attention à la dernière étape).

Courbes elliptiques – formules (3)

Choisir d'autres représentations des points, eg.

- coordonnées projectives $(X : Y : Z)$ tq $(x, y) = (X/Z, Y/Z)$, $\infty \leftrightarrow (0 : 1 : 0)$
- coordonnées jacobiennes $(X : Y : Z)$ tq. $(x, y) = (X/Z^2, Y/Z^3)$. $\infty \leftrightarrow (1 : 1 : 0)$.

Avantage : pas de division. Inconvénient : plus de multiplications.

- Affine : $1I + 2M + 1C$ (addition), $1I + 2M + 2C$ (doublement) ;
- Projectif : $12M + 2C$ (addition), $7M + 5C$ (doublement) ;
- Jacobiennes : $12M + 4C$ (addition), $4M + 6C$ (doublement) ;

On peut mélanger tout ça, eg. $A + P \rightarrow J$, etc. Dépend :

- de l'application visée ;
- de la courbe ;
- de l'arithmétique sous-jacente.

Courbes elliptiques – exponentiation

Calculer $(n, P) \mapsto n \cdot P$.

On peut faire un peu mieux que G général, car $P \mapsto -P$ est peu coûteux :

- $g^{2n} = (g^2)^n$
- $g^{4n-1} = (g^2)^{2n} \cdot g^{-1}$
- $g^{4n+1} = (g^2)^{2n} \cdot g$.

Calcul de g^n, $\lceil \log_2 n \rceil = N$

	cas le pire	moyenne
binaire	N d + N a	N d + $N/2$ a
add/sub	N d + $N/2$ a	N d + $N/3$ a

Courbes elliptiques – exponentiation (2)

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 $By^2 = x^3 + Ax^2 + x$.

Applications : cf. exposé ET.

Exponentation 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.

Courbes elliptiques – objectifs

Comprendre la **structure** et la **cardinalité**. Pourquoi la cardinalité ?

- **Primalité**. Prouver N premier $\leftrightarrow$ construire $E/\mathbb{Q}$ tel que $\operatorname{card} E(\mathbb{Z}/N\mathbb{Z})$ factorisable ;
- **Factorisation**. Trouver un facteur p de $N \leftrightarrow$ trouver (en tirant au hasard) une courbe $E/\mathbb{Q}$ telle que $\operatorname{card} E(\mathbb{Z}/p\mathbb{Z})$ friable ;
- **Cryptologie**. Problème du log. discret difficile sur $E/\mathbb{K} \Rightarrow \operatorname{card} E(\mathbb{K})$ a un grand facteur premier q.

Une parenthèse – log discret

$DLP(g,h)$:

- Données : $G =< g >$ un groupe, $h = g^a$.
- Sortie : a.

Thm. Si $C = \mathrm{card}\, G = \prod_{i=1}^{r} p_i^{\alpha_i}$, il existe des groupes $(< g_{ij} >)_{1 \leq i \leq r, 1 \leq j \leq \alpha_i}$ tels que

- $\mathrm{card}\ < g_{ij} >= p_i$;
- $DLP(g,h)$ se réduit polynomialement à $(DLP(g_{ij}, h_{ij}))$.

Une parenthèse – log discret

Dém. Si $h = g^a$, $h^{C/p_1^{\alpha_1}} = g^{aC/p_1^{\alpha_1}}$. En particulier,

$$DLP(g^{C/p_1^{\alpha_1}}, h^{C/p_1^{\alpha_1}}) = DLP(g,h) \bmod p_1^{\alpha_1}.$$

$\Rightarrow$ théorème des restes chinois.

Cas $r = 1$.

$$DLP(g^{p_1^{\alpha_1 - 1}}, h^{p_1^{\alpha_1 - 1}}) = DLP(g,h) \bmod p_1 = \delta,$$

$$\delta + p_1 DLP(g^{p_1}, h \cdot g^{-\delta}) = DLP(g,h).$$

$$\text{card } < g^{p_1} >= p_1^{\alpha_1 - 1}.$$

Courbes elliptiques - cardinalité

Courbes elliptiques – cardinalité

Étant donné $E/\mathbb{F}_q$, que sait-on sur $\operatorname{card} E(\mathbb{F}_q)$?

- Point de vue théorique ;
- Point de vue algorithmique.

On verra deux types d'approches :

- Construire des courbes *ad hoc* ;
- Calculer la cardinalité de courbes aléatoires.

Courbes elliptiques – Thm. de Hasse-Weil

E courbe définie sur $\mathbb{F}_q$.

$$Z(E, \mathbb{F}_q) := \exp\left(\sum_{n \geq 0} \operatorname{card} E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Thm. (Hasse-Weil)

$$Z(E, \mathbb{F}_q) = \frac{1 - tT + qT^2}{(1-T)(1-qT)}$$

et $|t| \leq 2\sqrt{q}$.

Cor. $\operatorname{card} E(\mathbb{F}_q) = q + 1 - t \approx q$.

C'est moral : $y^2 = x^3 + Ax + B$, à peu près un x sur 2.

Courbes elliptiques – Thm. de Hasse-Weil (2)

Conséquences.

- un degré de liberté $\Rightarrow \operatorname{card} E(\mathbb{F}_q)$ détermine complètement $\operatorname{card} E(\mathbb{F}_{q^k})$ ($g = 1$) ; inversement,

$$\begin{aligned} \operatorname{card}(E, \mathbb{F}_q) &= \frac{Z'(E, \mathbb{F}_q)}{Z(E, \mathbb{F}_q)}(0) \\ &= q + 1 - t. \end{aligned}$$

- Si $1 - tT + qT^2 = (1 - \alpha T)(1 - \overline{\alpha} T)$,

$$\operatorname{card}(E, \mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \overline{\alpha^n}.$$

Courbes elliptiques – répartition de $\mathrm{card}\, E$

Pour l'application à la factorisation, comprendre si $E(\mathbb{F}_p) =$ entier aléatoire de $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.

Thm. (Deuring) Pour tout $|t| \leq 2\sqrt{p}$, il existe $E/\mathbb{F}_p$ telle que $\mathrm{card}\, E = p+1-t$.

Les probabilités de chaque t suivent la loi de Sato-Tate :

$$\Pr\left(\frac{t}{2\sqrt{p}} \in [\tau, \tau']\right) \to_{p\to\infty} \int_\tau^{\tau'} \sqrt{1-u^2}du.$$

En gros, t est "presque uniforme", sauf que

- Les petits t sont plus probables ;
- Les grands t sont peu probables.

Courbes elliptiques – courbes de Koblitz

Une première idée pour contrôler la cardinalité (Koblitz) :

- Construire $E/\mathbb{F}_q$ avec q petit ;
- $\mathrm{card}\, E(\mathbb{F}_q)$ par énumération ;
- En déduire $Z(E, \mathbb{F}_q)$;
- Utiliser $E/\mathbb{F}_{q^n}$, dont le cardinal est facile à calculer.

Avantage :

- Très facile.

Inconvénient en crypto :

- $\mathrm{Aut}\,(E)$ est gros, d'ordre au moins n ;
- $DLP(E, .)$ se réduit à $DLP(E/\mathrm{Aut}\,(E), .)$...

Pas possible pour la primalité où on veut $q = p$ grand.

Courbes elliptiques – courbes de Koblitz – ex.

- $E : y^2 + xy = x^3 + x$ sur $\mathbb{F}_2$;
- $E(\mathbb{F}_2) = \{\infty, (0,0), (1,0), (1,1)\}$;
- $t = \alpha + \overline{\alpha} = -1, \alpha\overline{\alpha} = 2$;
- $\alpha = (-1 \pm \sqrt{-7})/2$;
- $\operatorname{card} E(\mathbb{F}_{2^{192}}) = 2^{192} + 1 - 2\Re(\alpha^n) =$

$$6277101735386680763835789423054843517195581229679741356800$$

Courbes elliptiques – torsion

Déf :n-torsion : points $P \in E(\mathbb{K})$ tels que $n.P = 0$. Noté $E[n]$.

- $E(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$, donc $E[n](\mathbb{C}) = \{(a + b\tau)/n, a, b \in \mathbb{Z}\}$;
- $E[n](\mathbb{C}) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$;
- Encore vrai si $\mathbb{K}$ alg. clos, $(c(\mathbb{K}), n) = 1$.
- Si de plus $n = \ell$ premier, $E[\ell]$ est un $\mathbb{Z}/\ell\mathbb{Z}$-ev de dimension 2 ;
- Il existe $\psi_\ell(X)$ de degré $(\ell^2 - 1)/2$ dont les racines sont les abscisses des points de ℓ-torsion.

Courbes elliptiques – Frobenius

Soit $E/\mathbb{F}_q$. Sur $E(\overline{\mathbb{F}}_q)$, on a l'endomorphisme :

$$\begin{array}{rcl} \phi_q : E(\overline{\mathbb{F}}_q) & \to & E(\overline{\mathbb{F}}_q) \\ (x, y) & \mapsto & (x^q, y^q) \end{array}$$

- ϕ_q est linéaire : $\phi_q(P+Q) = \phi_q(P) + \phi_q(Q)$;
- ϕ_q est un endomorphisme de $E[\ell]$: $\ell\phi_q(P) = \phi_q(\ell P) = 0$;

Thm. Le polynôme carac. de ϕ_q restreint à $E[\ell]$ est $T^2 - tT + q \bmod \ell$, ou encore $t \bmod \ell = \mathrm{Tr}\,(\phi_q)$.

Courbes elliptiques – algorithme de Schoof

Idée. Déterminer $t \bmod \ell$ pour suffisamment de ℓ, puis utiliser le thm. chinois.

- Pour déterminer $t \bmod \ell$, chercher t tel que $\phi_q^2(P) + t\phi_q(P) + qP = 0$ pour tout $P \in E(\overline{\mathbb{F}}_q)[l]$;
- ie. $(X^{q^2}, Y^{q^2}) + t(X^q, Y^q) + q(X, Y) = 0$ sur $E(\overline{\mathbb{F}}_q)[l]$;
- Représenter $E(\overline{\mathbb{F}}_q)[l]$: c'est

$$\{(X, Y), Y^2 = X^3 + AX + B \text{ et } \psi_\ell(X) = 0\} \cup \{0\}.$$

- ie. on travaille modulo l'idéal $(\psi_\ell(X), Y^2 - X^3 - AX - B)$.
- Inconvénient : degré élevé ;
- Avantage : polynomial, $O(\log^8 p)$;
- On sait améliorer, mais c'est plus compliqué $\longrightarrow$ SEA.

Courbes elliptiques – algorithme de Schoof

Un exemple en Magma :

```
Magma V2.13-9 Sun Mar 18 2007 22 :34 :50 on macaron
Type? for help. Type <Ctrl>-D to quit.
> K := FiniteField(p); // 192 bits
> E := EllipticCurve([K!17, K!42]);
> time #E;
20456663862227867266175929616281812839497O...
Time : 6.320
```

Pentium 4 3.2 GHz.

Courbes elliptiques – petite caractéristique

$q = 2^n$.

- Algorithmes très efficaces (beaucoup plus que Schoof !) ;
- Principe assez différent, mais ϕ_p reste au centre ;
- Un exemple :

```
> K := FiniteField(2^192);
> E := EllipticCurve([K!1,0,K.1^42+K.1^17,0,K.1]);
> time #E;
Using canonical lift algorithm for characteristic 2
Computing trace via canonical lift.
Working with Cyclotomic basis.
Total trace time : 0.250
6277101735386680763835789423892604277850286237438465956 96
Time : 0.250
```

Courbes elliptiques – endomorphismes sur $\mathbb{C}$

- $[n]$: $P \mapsto n.P$ est un endomorphisme ; on dit que $\mathbb{Z} \subset \mathrm{End}\,(E)$;
- Si $\mathbb{K} = \mathbb{C}$, $E \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$;
- Les endomorphismes $\varphi \in \mathrm{End}\,(E)$ sont de la forme forme $x \mapsto \alpha x$ avec $\alpha(\mathbb{Z} + \tau\mathbb{Z}) \subset \mathbb{Z} + \tau\mathbb{Z}$;
- ie. $\alpha = a\tau + b$, $\alpha\tau = c\tau + d$.
- ou encore $a\tau^2 + (b - c)\tau - d = 0$.
- Si τ est racine d'un pol. de degré 2 à coefs. entiers, $\mathrm{End}\,(E) = \mathbb{Z}[a\tau + b]$ (multiplication complexe). Sinon, $\mathrm{End}\,(E) = \mathbb{Z}$.

Endomorphismes sur $\mathbb{F}_q$

- On a toujours $\mathrm{End}\,(E)$ strictement plus grand que $\mathbb{Z}$: $\phi_p \in \mathrm{End}\,(E)$.
- Ici encore, ϕ_p vérifie une équation de degré 2 : $\phi_p^2 - t\phi_p + p = 0$

Thm. Si $\mathrm{End}\,(E/\mathbb{Q}) = \mathbb{Z}[\tau]$, et si $\omega \in \mathbb{Z}[\tau]$ est tel que $\omega\overline{\omega} = p$, alors $t = \pm(\omega + \overline{\omega})$ (sauf peut-être si $\mathbb{Q}(\tau) = \mathbb{Q}(i)$ ou $\mathbb{Q}(j)$).

Pratique. Si $p = U^2 + DV^2$, on prend $\tau = \sqrt{-D}$, $\omega = U + \tau V$, et on *construit* une courbe telle que $\mathrm{End}\,(E/\mathbb{Q}) = \mathbb{Z}[\tau]$. Et alors, $\mathrm{card}\, E(\mathbb{F}_p) = p + 1 \pm 2U$.

Csq. Construire simultanément E et $\mathrm{card}\, E$. Applications : primalité !

Bilan global

- Courbes elliptiques : $y^2 = x^3 + Ax + B$
- Arithmétique : une addition = une dizaine de multiplications dans $\mathbb{K}$;
- Cardinalité : problème mathématiquement et algorithmiquement sophistiqué...
- mais essentiellement résolu.
- Applications en crypto, factorisation, primalité : cf. la suite.

Courte bibliographie

- I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, London Math. Soc. Lecture Notes Series **265** (1999). *Livre traitant l'ensemble des sujets abordés dans la session.*
- J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag Graduate Texts in Mathematics (1986). *L'un des cours de références sur les courbes elliptiques. Très complet, beaucoup plus large et orienté "théorie" que la session*
- J. W. S. Cassels, Lectures on Elliptic Curves, London Math. Soc. Student Texts **24**. *Le point de vue théorique, de façon plus élémentaire que le précédent.*
- H. Cohen, G. Frey (Eds.), Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Mathematics and Its Applications, Chapman & Hall. *Un manuel de référence plus qu'un livre dans lequel apprendre la théorie, très dense mais exhaustif.*