Courbes elliptiques avec des applications en cryptographie

Gerhard Frey

Université de Duisburg-Essen
Frey@exp-math.uni-essen.de

Théorie des Nombres et leur Applications
Université Mohammed I
Oujda

Mai 2015

Références

Les notions et les résultats usés dans la conférance suivante sont expliqués dans

J. Silverman *The Arithmetic of Elliptic Curves, GTM 106,* Springer 1986.

Pour tous les faits et méthodes concernants les applications à la cryptographie clés publique, y compris la théorie des courbes elliptiques d'un point de vue algorithmique (et théorique), voir

H. Cohen & G. Frey (eds.): *Handbook of Elliptic et Hyperelliptique Curve Cryptography*, CRC 2005

Dans ce livre, on trouvera une liste longue de références (40 pp) des articles originaux.

Au cours de la conférence nous donnerons plus de citations précise.

Dans l'entier article on suppose que K est un corps de caractéristique $p \geq 0$ qui est parfait, i.e. la clôture séparable de K est égale à son clôture algébrique $\overline{K}$. L est un sur-corps de K, i.e. un corps contenant K.
Le groupe de Galois absolu de K est

$$G_K := \mathrm{Aut}_K(\overline{K}).$$

Ce groupe a la structure d'un groupe topologique compact, une base pour les environs ouverts de l'unitie sont les sous-groupes de G_K à l'index fini.

1 Cubiques

1.1 Définitions

1.1.1 Le plan affine et le plan projectif

Le plan affine $\mathbb{A}^2_K$ est l'espace affine de dimension 2 défini sur K.

Soit L un corps contenant K.
L'ensemble des points L-rationels de $\mathbb{A}^2_K$ est

$$\mathbb{A}^2_K(L) := \{(x_1, x_2) \in L \times L\}.$$

Nous pouvons choisir des fonctions coordonnées affines X_1, X_2 et obtenons $\mathbb{A}^2_K(L)$ comme l'ensemble des valeurs L -rationelles de la paire des fonctions (X_1, X_2).
Les quotients des polynômes

$$f(X_1, X_2), g(X_1, X_2) \neq 0 \text{ dans } K[X_1, X_2]$$

sont les fonctions rationelles sur $\mathbb{A}^2_K$ définies sur K.

Ces fonctions forment le corps $K(X_1, X_2)$.
Le plan projectif $\mathbb{P}^2_K$ est l'espace projectif de dimension 2 défini sur K.

L'ensemble des points L-rationels de $\mathbb{P}^2_K$ est

$$\mathbb{P}^2_K(L) = \{(y_0, y_1, y_2) \in L^3 \setminus \{(0,0,0)\}/\sim\}$$

avec la relation $\sim$ définie par

$$(y_0, y_1, y_2) \sim (y_0', y_1', y_2')$$

si et seulement si $\exists \lambda \in L^*$ with

$$(y_0, y_1, y_2) = \lambda \cdot (y_0', y_1', y_2').$$

La classe d'équivalence de (y_0, y_1, y_2) est denotée par $(y_0 : y_1 : y_2)$.
Nous choisissons les fonctions coordonnées projectives Y_0, Y_1, Y_2 et obtenons $\mathbb{P}^2_K(L)$ comme classes d'équivalence des valeurs L-rationelles du triple des fonctions (Y_0, Y_1, Y_2).

Les polynômes homogènes de degré $d \geq 0$ sont denotés par $K[Y_0, Y_1, Y_2]_d$.

Les fonctions rationelles sur $\mathbb{P}^2_K$ sont les quotients des polynômes

$$g, h \in K[Y_0, Y_1, Y_2]_d; d \in \mathbb{N}.$$

Il y a beaucoup de possibilités d'identifier $\mathbb{A}^2_K$ à un part affine de $\mathbb{P}^2_K$. Nous choisissons l'injection suivante:

$$\pi : \mathbb{A}^2_K \to \mathbb{P}^2_K$$

$$(x_1, x_2) \mapsto \pi(x_1, x_2)) := ((1 : x_1 : x_2)$$

avec $x_1, x_2 \in \overline{K}$.

Nous observons que

$$\mathbb{P}^2_K(L) \setminus \pi(\mathbb{A}^2_K(L)$$
$$= \{(0 : y_1 : y_2);\, y_i \in L) =: H_\infty(L)$$

où H_∞ est la "droite a l'infinité " (dépendant de la choix de π) qui est isomorphe à l'espace projectif a dimension 1.
L'inverse de π est

$$\xi : \mathbb{P}^2_K \setminus H_\infty : (y_0 : y_1 : y_2) \mapsto (y_1/y_0, y_2/y_0).$$

En termes des fonctions coordonnées la relation entre $\mathbb{A}^2_K$ et $\mathbb{P}^2_K$ est donné par la relation

$$X_i = Y_i/Y_0 \text{ pour } i = 1, 2.$$

Par conséquence nous pouvons homogéniser des fonctions rationelles $r(X_1, X_2)$ sur $\mathbb{A}^2_K$ de sorte que le résultat $r^h(Y_0, Y_1, Y_2)$ est une fonction rationelle sur $\mathbb{P}^2_K$ avec

$$r^h(Y_0, Y_1, Y_2)_{|\mathbb{P}^2_K \setminus H_\infty} = r(X_1, X_2) \circ \pi^{-1} \ :$$

Nous commençons avec $r(X_1, X_2) \in K[X_1, X_2]$ avant le degré total d et posons

$$f^h(Y_0, Y_1, Y_2) := Y_0^d f(Y_1/Y_0, Y_2/Y_0).$$

Evidemment $f^h \in K[Y_0, Y_1, Y_2]_d$. Pour $r(X_1, X_2) = f(X_1, X_2)/g(X_1, X_2)$ avec f, g polynômes de degré d_1 et d_2 on définе

$$r^h(Y_0, Y_1, Y_2) := Y_0^{d_2 - d_1} \frac{f^h(Y_0, Y_1, Y_2)}{g^h(Y_0, Y_1, Y_2)}.$$

Inversement on dé-homogénise
$F \in K[Y_0, Y_1, Y_2]_d$ respectivement $R = F/G$ avec $F, G \in K[Y_0, Y_1, Y_2]_d$
par la transformation

$$Y_0 = 1, Y_1 = X_1, Y_2 = X_2.$$

On remarque que le corps de fonctions $K(X_1, X_2)$ de $\mathbb{A}^2_K$ est isomorphe à le corps des fonctions rationelles sur $\mathbb{P}^2_K$.

1.1.2 Courbes planes projectives

Définition 1.1

- *Pour $F(Y_0, Y_1, Y_2) \in K[Y_0, Y_1, Y_2]_d$ avec $d > 0$ on définе*

$$C_F(L) :=$$

$$\{(y_0 : y_1 : y_2) \in \mathbb{P}^2_K(L);\ F(y_0, y_1, y_2) = 0\},$$

  l'ensemble des points L-rationels de la courbe projective avec l'équation F.

- *Le foncteur $L \mapsto C_F(L)$ est représenté par un objet géométrique C, un sous-schéma de dimension 1, fermé dans la topologie de Zariski, de $\mathbb{P}^2_K$ et est denoté par courbe plane projective reliée à l' équation*

$$F(Y_0, Y_1, Y_2) = 0.$$

- *La courbe C est (absolument) irréductible si et seulement si F est irréductible dans $K[Y_0, Y_1, Y_2]$ ($\overline{K}[Y_0, Y_1, Y_2]$).*

- *Le degré de C est égal au degré de F.*

- *Un point $P = (y_0, y_1, y_2) \in C(\overline{K})$ est régulier si et seulement si le vecteur tangentiel à P de C est non-zéro, i.e.*

$$(\frac{\partial F}{\partial Y_0}(P), \frac{\partial F}{\partial Y_1}(P), \frac{\partial F}{\partial Y_2}(P)) \neq (0, 0, 0).$$

- *La courbe C est régulière si et seulement si tous les points de $C(\overline{K})$ sont réguliers.*

1.1.3 Courbes planes affines

Définition 1.2

Pour $f(X_1, X_2) \in K[X_1, X_2] \setminus K$ on définе

$$C_f(L) :=$$

$$\{(P = (x_1, y_1) \in \mathbb{A}^2_K(L);\ f(x_1, x_2) = 0\},$$

l'ensemble des points L-rationels de la courbe avec l'équation f.

- *Le foncteur $L \mapsto C_f(L)$ est représenté par un objet géométrique C, un sous-schéma de dimension 1, fermé dans la topologie de Zariski, de $\mathbb{A}^2_K$ et est denoté par courbe plane affine reliée à l' équation $f(X_1, X_2) = 0$.*

- *Un point $P = (x_1, x_2) \in C(\overline{K})$ est régulier si et seulement si le vecteur tangentiel à P de C est non-zéro, i.e.*

$$(\frac{\partial f}{\partial X_1}(P), \frac{\partial f}{\partial X_2}(P)) \neq (0, 0).$$

- *La courbe C est régulière si et seulement si tous les points de $C(\overline{K})$ sont réguliers.*

- *La courbe C est irréductible si et seulement si le polynôme $f(X_1, X_2)$ est irréductible.*

1.1.4 Clôture projective et réstriction affine

Nous supposons que C_f soit une courbe plane affine avec l' équation

$$f(X_1, X_2) = 0.$$

Soit $F(Y_0, Y_1, Y_2) := f^h(Y_0, Y_1, Y_2)$ le polynôme homogénisé de f.
La courbe $C_F \subset \mathbb{P}^2_K$ est la clôture (dans la topologie de Zariski) projective de C_f.
Inversement, soit C_F la courbe plane avec l'équation $F(Y_0, Y_1, Y_2) = 0$, et soit $f(X_1, X_2)$ la dé-homogénisation de F. La courbe $C_f \subset \mathbb{A}^2_K$ est (une) partie affine de C.
Notation: $C_F(L) \setminus C_f(L) =: C_\infty(L)$ sont les "points à l'infini " de C_F qui sont L-rationels.

Evidemment, $C_\infty(L) = C_F(L) \cap \mathbb{A}^2_K(L)$, et cet ensemble est fini si et seulements si H_∞ n'est pas un sous-schéma de C_F, i.e. Y_0 ne divise pas F.

Nous continuons de supposer que f est la dé-homogénisation de F.
Il est une exercice simple de vérifier que $P \in C_f(L)$ est regulier si et seulement si $P \in C_F$ est regulier, et que C_F est irréductible si et seulement si $f(X_1, X_2)$ est irréductible de degré totale égale au degré de F .

1.1.5 Corps de fonctions

Supposons que C_f (respectivement C_F) est irréductible.
La réstriction des fonctions rationelles de $\mathbb{A}^2_K$ (respectivement $\mathbb{P}^2_K$) à C_f (respectivement C_F) sont les fonctions rationelles de C_f(respectivement C_F).

En tout cas, ces fonctions forment un corps dénoté comme corps de fonctions F_{C_f} de C_f (respectivement F_{C_F} de C_F).

On observe que F_{C_f} est canoniquement isomorphe à F_{C_F}, et l'on identifiera ces deux corps.

1.1.6 Fonctions holomorphes

Soit C une courbe (affine ou projective) et soit $P \in C(\overline{K})$.

Définition 1.3

La function $f \in F_C$ est holomorphe à P si et seulement si f, comme fonction sur $\mathbb{P}^2_K$, n'a pas un pôle à P, i.e. f a un valeur bien défini $f(P) \in \overline{K}$.

Soit C' un sous-schéma de C. f est holomorphe sur C' si et seulement si f est holomorphe à chaque point de $C'(\overline{K})$.

Faits: Soit C une courbe plane *affine* avec équation $f(X_1, X_2) = 0$.

- Les fonctions holomorphes sur C sont des fonctions rationelles de C contenues dans la clôture intégrale de $O_C := K[X_1, X_2]/(f(X_1, X_2))$ dans F_C.
- Pour $P \in C(\overline{K})$ on appele m_P l'ideal formé des élélements $f \in O_C$ avec $f(P) = 0$.
  Les functions holomorphes dans P sont les éleménts de l'anneau locale

$$O_{C,P} := \{g(X_1, X_2)/h(X_1, X_2);$$

$$g \in O_C,\ h \in O_C \setminus m_P\}.$$

- $P \in C(\overline{K})$ est régulier si et seulement si $O_{C,P}$ est intégralement clos et est par conséquence un anneau de valuation.
  En particulier, on défine pour $f \in F_C$

$$v_P(f) = \max\{\mathrm{z} \in \mathbb{Z} \text{ avec } \mathrm{f} \in \mathrm{m_P^z}\},$$

  et pour P régulier la fonction v_P est une valuation discrète normalisée.
- La courbe C est régulière si es seulement O_C est intégralement clos. Dans ce cas O_C est un anneau de Dedekind.

1.2 Courbes planes de degré 3

Notation: Pour simplifier et parce que nous voulons user la notation commune dans les livres standards nous désignerons désormais les functions coordonnées projectives par $Z := Y_0, X := Y_1, Y := Y_2$ et les functions coordonnées affines par X, Y (avec l'identification

$$X \to X/Z, Y \to Y/Z, Z \to 1)$$

et nous ésperons que cet abus de langage ne produira des confusions.

Nous nous intéressons pour les courbes cubiques C reliées aux équations

$$F(X,Y,Z) = \sum_{0 \le i+j \le 3} a_{i,j} X^i Y^j Z^{3-(i+j)} = 0$$

avec $a_{i,j} \in K$, et nous supposerons que F soit irréductible sur $\overline{K}$.

Exercice 1 *Une courbe cubique C a au plus un point non-régulier (qui est nécessairement rationel sur K).*

Soit

$$g : aX + bY + cZ = 0$$

une droite définie sur K.
Il est bien connu et facilement vérifié que $(g \cap C)(\overline{K})$ n'est pas vide et contient au plus 3 points différents.
Génériquement l'intersection a exactement trois points.
Si $|(g \cap C)(\overline{K})| \le 2$ la droite g est une tangente à l'un des points dans $g \cap C(\overline{K})$.
Si $|(g \cap C)(\overline{K})| \le 1 = \{P\}$ ce point P est un point d'inflexion.

Exercice 2 *Si car(K)$\neq$ 3 une cubique a 9 points d'inflexion rationels sur $\overline{K}$.*

Ci-après nous ne regarderons que des cubiques satisfaisants la condition suivante:

$$\mathcal{I} : \; H_\infty \cap C(\overline{K}) = H_\infty \cap C(K)$$

$$= \{P_\infty = (0:1:0)\}$$

et P_∞ est un point régulier de C.
En particulier,

$$\mathbf{C}(\mathbf{K}) \neq \emptyset,$$

et P_∞ est un point d'inflexion de C.

Exercice 3 *Supposons que pour C la condition $\mathcal{I}$ est satisfaite. Alors C a une équation*

$$f_C : Y^2Z + a_1XYZ + a_3YZ^2 =$$

$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

1.2.1 Classification des singularités

Soit P un point singulier de la cubique C reliée à l'équation

$$f_C : Y^2Z + a_1XYZ + a_3YZ^2 =$$

$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Parce que $P \neq P_\infty$ nous pouvons choisir des coordonnées affines $P = (x, y)$ avec

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

Par un changement linéaire des coordonnées on peut supposer que $x = y = 0$ et par conséquence $a_6 = 0$.
De plus, on a $(2Y + a_1X + a_3)(0,0) = 0 = (a_1Y - 3X^2 - 2a_2X - a_4)(0,0)$.
Il suit que $a_3 = 0 = a_4$ et que l'équation affine pour C est

$$Y^2 + a_1XY = X^3 + a_2X^2.$$

Premier cas: $a_1^2 \neq 4a_2$.
Une calculation facile montre que dans ce cas il y a sur $\overline{K}$ exactement deux droites $Y = mX$ qui intersectent C seulement en $(0,0)$ (avec $m = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2}$ si la caractéristique de K est différente de 2).
On voit que C a deux "tangentes" dans $(0,0)$ qui sont rationelles après une

extension de K de degré ≤ 2. Supposons que $\sqrt{a_1^2 - 4a_2} \in K$. On peut changer les coordonnées tel que C a l'équation

$$Y^2Z + XYZ - X^3 = 0.$$

Par la paramétrisation

$$\varphi : u \mapsto (\frac{u}{(1-u)^2}, \frac{u^2}{(1-u)^3}, 1)$$

$$\text{si } u \neq 1; 1 \mapsto (0, 1, 0)$$

on obtient un isomorphisme de L^* à $C(L) \setminus \{(0, 0)\}$. On dit que C a *le type multiplicatif*.
Deuxième cas: $a_1^2 = 4a_2$
Dans ce cas chacune droite passant a travers $(0, 0)$ intersecte C avec multiplicité ≥ 2, et le type de la singularité est égal à la singularité de la parabole $Y^2 = X^3$ et P est un *point de rebroussement*.
Par la transformation

$$X \to X, Y \to Y - \frac{1}{2}\, a_1 X$$

on arrive à l'équation

$$Y^2Z = X^3.$$

La paramétrisation

$$\xi : t \mapsto (t^{-3}, t^{-2}, 1); t \neq 0;\ 0 \mapsto (0, 1, 0)$$

$$0 \mapsto (0, 1, 0)$$

est une bijection du groupe L^+ à
$C(L) \setminus \{P_\infty\}$ pour chaque sur-corps L de K.
On dit que C a *le type additif*.
Maintenant nous supposons que C est regulière. Nous expressons cette condition en usant l'équation

$$f_C : Y^2Z + a_1XYZ + a_3YZ^2 =$$

$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Pour simplifier la discussion nous assumerons pour le moment que car$(K)\neq 2$. Par la transformation

$$X \to X,\, Y \to Y - \frac{1}{2}\,(a_1\, X + a_3 Z), Z \to Z$$

on obtient une équation

$$Y^2 Z = X^3 + b_2 X^2 Z + b_4 X Z^2 + b_6 Z^3$$

pour C. Un calcul facile montre que C est regulière si et seulement si le discriminant du polynôme

$$f_3(X) := X^3 + b_2 X^2 + b_4 X + b_6$$

est non-zéro.

Exercice 4 *Calculez la condition pour la régularité pour car(K)= 2.*

1.3 Les lois d'addition

Nous continuons de supposer que C est une cubique qui satisfait la condition $\mathcal{I}$. Par C^{ns} nous dénotons le sous-schéma des points réguliers de C.
Une observation simple qui est fondamentale:
Soit g_{P_1,P_2} la droite projective passant par deux points différents $P_1, P_2 \in C(L)^{ns}(L)$. Alors

$$(g_{P_1,P_2} \cap C)(L) = \{P_1, P_2, P_3\}$$

avec $P_3 \in C(L)^{ns}$ (et possiblement égal à P_1 ou P_2. *Question*: Interprétation géométrique?).
Pour $P_1 = P_2 := P$ on remplace g_{P_1,P_2} par la tangente t_P de C dans P.

L'inversion ω L'application

$$\omega : C \to C$$

$$(X, Y, Z) \mapsto (X, -Y - a_1 X - a_3 Z, Z)$$

est un automorphisme de C (au sense de la géométrie algébrique) qui applique $C^{ns}(L)$ bijectivement sur $C^{ns}(L)$ pour chaque sur-corps L de K. Pour $P_1, P_2 \in C^{ns}(L)$ on dénote par P' le troisième point dans $(g_{P_1,P_2} \cap C)(L)$ (respectivement $(t_P \cap C)(L)$ si $P_1 = P_2$).

Définition 1.4

$$\oplus_L : C(L)^{ns} \times C(L)^{ns} \to C(L)^{ns}$$

est l'application définie par

$$P_1 \oplus_L P_2 := \omega(P').$$

Proposition 1.5 *Pour chaque L l'ensemble $C^{ns}(L)$ est un groupe abélien avec la composition $\oplus_L$.*
L'élément neutre est le point

$$P_\infty = (0 : 1 : 0),$$

et l'inverse de P est

$$\omega(P) =: \ominus(P).$$

La preuve de cette proposition est simple - **sauf** la vérification de l'associativité . Nous verrons une preuve "structurelle" ci-dessous.
Mais on a plus de propriétés: $\oplus_L$ est donné par une application polynomiale avec des polynômes à coefficients dans K et indépendent de L.
On calcule ces polynômes très simplement par usage du Théorème de Viète.
Nous donnons les **formules d'addition** pour le cas que

$$P_1 \neq P_2, \ominus P_2$$

et

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$$

différents de P_∞.
On a

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3) \text{ avec}$$

$$x_3 = -x_1 - x_2 - a_3 - a_1 \cdot \frac{(y_1 - y_2)}{(x_1 - x_2)} + (\frac{(y_1 - y_2)}{(x_1 - x_2)})^2$$

et y_3 choisie tellement que $(x_3, y_3) \in C$ n'est pas colinéaire avec $(x_1, y_1), (x_2, y_2)$.

Exercice 5

- *Prouvez la formule ci-dessus et calculez y_3.*
- *Donnez la formule pour les coordonnées de $P \oplus P =: [2]P$ (formule de duplication).*

- *Démontrez que les paramétrisations ξ et φ sont des homomorphismes de groupes.*

Par conséquence on a trouvé :

Théorème 1.6 *C^{ns} est un groupe algébrique commutatif et irréductible.*
Si C est de type multiplicatif ce groupe est isomorphe sur une extension K' de K ($K' : K] \leq 2$) avec G_m, le groupe multiplicatif, et ainsi C^{ns} est un tore.
Si C est de type additif C^{ns} est isomorphe avec G_a, le groupe additif.
Si C est une courbe régulière, le groupe algébrique est une variété abeliénne de dimension 1.
Les lois d'addition sont données par des fonctions rationelles explicites en coordonnées affines ou projectives.

Rappelons que la preuve de ce théorème a une lacune: Nous n'avons pas vérifiés l'associativité de $\oplus$ dans le cas que C est régulier. On peut faire ça par une calculation compliquée mais nous préférons une méthode plus structurelle.

2 Courbes elliptiques

Définition 2.1 *Les définitions suivantes sont équivalentes:*

1. *Une courbe elliptique E définie sur K est une courbe projective plane de degré* 3 *sans singularités et avec un $P_0 \in E(K)$.*

2. *E est donnée par une* ***équation de Weierstraß***

$$Y^2Z + a_1XYZ + a_3YZ^2 =$$

$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

et il n'y a aucun point de E pour lequel toutes les dérivés partielles disparaissent.

3. *E est une courbe projective non singulière absolument irréductible de genre* 1 *avec un point* K*- rationel.*

4. *E est une courbe projective qui est isomorphe à sa variété jacobienne, i.e.* (E, P_∞) *est une variété abélienne de dimension* 1 *avec l'origine* P_∞.

Dans les paragraphes suivantes nous expliquerons les notions usées dans la définition.

2.0.1 Diviseurs des courbes

Soit C une courbe projective (non nécessairement plane) irréductible définie sur K et régulière (i.e. pour chaque point P sur C l'anneau locale des fonctions rationelles sur C qui sont holomorphe à P forment un anneau de valuation). La valuation discrète normée est dénotée par v_P.
Soit F_C le corps des fonctions rationelles de C.
Le groupe de Galois absolu G_K de K opère sur $C(\overline{K})$ via son opération sur des coordonnées des points.

Définition 2.2

- *Un diviseur premier* $\mathfrak{p}$ *de* C *est une orbite* $G_K \cdot P$ *ou* $P \in C(\overline{K})$.
  *(*Question*: Pourquoi est cette orbite finie?)*
  Le degré de $\mathfrak{p}$ *est*
  $\deg(\mathfrak{p}) :=$ *nombre des points dans l'orbite* $\mathfrak{p}$.
  L'ensemble des diviseurs premiers est appelez Σ_C.
  La valuation $v_\mathfrak{p}$ *est définie comme* v_P *pour* $P \in \mathfrak{p}$.

- *Le groupe des diviseurs de* C *est*

$$\mathcal{D}_C = \{\sum_{\mathfrak{p}\in\Sigma_C} z_\mathfrak{p} \cdot \mathfrak{p}; z_\mathfrak{p} \in \mathbb{Z}\}$$

  et presques tous les $z_\mathfrak{p} = 0$.
  L'addition est définie composante par composante.

- *Pour* $D = \sum_{\mathfrak{p}\in\Sigma_C} z_{\mathfrak{p}} \cdot \mathfrak{p}$ *le degré de* D *est* $\deg(D) = \sum z_{\mathfrak{p}} \cdot \deg(\mathfrak{p})$.
  Les diviseurs de degré 0 *forment un sous-groupe* $\mathcal{D}_C^0$ *de* $\mathcal{D}_C$.

- *Soit* $f \in F_C^*$ *une fonction rationelle non-nulle sur* C.

$$(f) := \sum_{\mathfrak{p}\in\Sigma_C} v_{\mathfrak{p}}(f) \cdot \mathfrak{p}$$

  est le diviseur principal de f.
  Les diviseurs principaux de C *forment un sous-groupe* $\mathcal{P}_C$ *de* $\mathcal{D}_C^0$.

- *Le groupe des classses de diviseurs de degré* 0 *est*

$$\mathrm{Pic}_C^0 := \mathcal{D}_C^0/\mathcal{P}_C.$$

  La classe d'un diviseur D *est dénotée par* $[D]$.

- *Pour chaque sur-corps* L *on peut considéré la courbe* C_L *obtenue par extension des scalaires de* C.
  Le foncteur de Picard de C *est le foncteur qui applique la catégorie des sur-corps* L *de* K *dans la catégorie des groupes abéliens par*

$$L \mapsto \mathrm{Pic}_{C_L}^0.$$

2.0.2 Le Théorème de Riemann-Roch

Le résultat fondamental dans la théorie des courbes algébriques est le Théorème de Riemann-Roch qui prédicte comment on peut interpoler les functions en F_C par la préscription des pôles et des zéros.

Définition 2.3
Soit $D \in \mathcal{D}_C$, $D = \sum_{\mathfrak{p}\in\Sigma_C} z_{\mathfrak{p}} \cdot \mathfrak{p}$.

$$L(D) := \{f \in F_C; v_{\mathfrak{p}}(f) \geq -z_{\mathfrak{p}}; \forall \mathfrak{p} \in \Sigma_C\}.$$

Fait: $L(D)$ est un espace vectoriel de dimension fini nommé $\ell(D)$.

Théorème 2.4 *Soit C une courbe projective absolument irréductible. Il y a un entier $g_C \geq 0$ tel que pour chaque $D \in \mathcal{D}_C$ on a*

$$\ell(D) \geq \deg(D) - g_C + 1.$$

Pour $\deg(D) > 2g - 2$ on peut remplacer $\geq$ par $=$.

Exemple 2.5 *Les courbes de genre 0 qui possèdent des points rationels sur K sont birationellement équivalent (i.e. les corps de fonctions sont isomorphes) à la droite projective.*
Les discussions ci-dessus montrent que les cubiques non-régulières sont des courbes de genre 0.

2.0.3 Applications aux courbes elliptiques

Démonstration des équivalences (1), (2) et (3) dans la Définition 2.1(équisse)
Nous commençons avec (2) et (3).
Supposons que C satisfait l'équation affine

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Nous appelons le diviseur premier relié à P_∞ par $\mathfrak{p}_\infty$. On vérifie que la fonction $v_{\mathfrak{p}_\infty}(X) = -2$, $v_{\mathfrak{p}_\infty}(Y) = -3$ et ainsi $\ell(2\mathfrak{p}_\infty) \geq 2$, $\ell(3\mathfrak{p}_\infty) \geq 3$. Par conséquence $g_C \leq 1$.
Si $g_C = 0$ on a une fonction non-constante $t \in \mathcal{L}(\mathfrak{p}_\infty)$. On vérifie que ce n'est pas possible parce que C est régulière. Supposons que C est une courbe de genre 1 avec un point $P_0 \in C(K)$. Soit $\mathfrak{p}_0$ le diviseur premier relié. Le Théorème de Riemann-Roch a pour conséquence qu'il y a une fonction non-constante X en $\mathcal{L}(2\mathfrak{p}_0)$ et une fonction non-constante Y en $\mathcal{L}(3\mathfrak{p}_0) \setminus \mathcal{L}(2\mathfrak{p}_0)$ et que la dimension de $\mathcal{L}(6\mathfrak{p}_0) = 6$. Mais on trouve 7 fonctions $1, X, Y, X^2, XY, Y^2, X^3$ dans $\mathcal{L}(6\mathfrak{p}_0)$, et de là il existe une rélation linéaire parmi ces fonctions. Maintenant, il est une exercice simple de prouver que (2) est satisfait (avec $P_\infty = P_0$). Pour prouver l'équivalence de (1) avec (3) on pourrait user les Formules de Plücker qui impliquent que le genre de C est ≤ 1, et qu'il est 1 si et seulement si C est régulière.
Ou, plus élémentaire on observe que le genre d'une courbe ne change pas si on change le corps de définition par une extension séparable (rappel: K est parfait) et ainsi on peut supposer que C satisfait la condition $\mathcal{I}$ et donc $g_C = g_{C \times \overline{K}} = 1$.

2.0.4 Courbes elliptiques comme variétés jacobiennes

Pour la discussion de (4) de la Définition 2.1 on a besoin de plus de théorie. Nous avons défini le foncteur Pic^0_C relié à la courbe C. Un théorème fondamental de la géométrie algébrique est que ce foncteur est représentable. Plus précisement, il y a une variété J_C projective absolument irréductible qui est un schéma de groupes avec $Pic^0_C(L) = J_C(L)$.
J_C est la variété jacobienne de C.
Encore on use le Théorème de Riemann-Roch qui a pour conséquence que *birationellement* J_C est équivalent au produit symmétrique de dimension g_C de C. En cas des courbes de genre 1 avec un diviseur premier $\mathfrak{p}_\infty$ à degré 1 nous décrirerons cette relation explicitement.
Soit $\mathfrak{p}$ un diviseur premier de $C \times L$ relié a $P \in C(L)$. Le diviseur

$$D_P := \mathfrak{p} - \mathfrak{p}_\infty$$

a degré 0.
Désignons par c_P la classe de D_P. L'application

$$\phi_L : C(L) \to \mathrm{Pic}^0_{C\times L}$$

avec

$$\Phi(P) = c_P$$

est injective parce que C a le genre 1 et par conséquence il n'y a pas des fonctions sur C avec une seule zéro à l'ordre 1. Inversement, soit

$$c \in \mathrm{Pic}^0_{C\times L} \text{ et } D \in c.$$

Le degré de

$$D + \mathfrak{p}_\infty$$

est 1, et par conséquence il y a une function $f \in F_{C\times L}$ tel que $(f) - D - \mathfrak{p}_\infty$ est un diviseur avec des coefficients ≥ 0. Le degré de $(f) - D + \mathfrak{p}_\infty$ est 1, et de là on a:

$$(f) - D + \mathfrak{p}_\infty = \mathfrak{p}$$

avec $\mathfrak{p}$ un diviseur premier de degré 1, et

$$c = [\mathfrak{p} - \mathfrak{p}_\infty].$$

Ça démontre que ϕ_L est surjective et que (4) de la définition 2.1 est satisfait pour les courbes de genre 1 avec un point rationel. **Conclusion:** Une courbe elliptique C est une variété abélienne et la structure de groupe algébrique est canonicalement déterminée après le choix d'un point rationel P_∞. La définition de l'addition sur les points rationels de C est comme suivante: Soient $P_1, P_2 \in C(K)$ et $\mathfrak{p}_1, \mathfrak{p}_2$ les diviseurs premiers reliés. Alors

$$P_3 = P_1 \oplus P_2 \text{ avec } \mathfrak{p}_3 \text{ relié à } P_3$$

si et seulement si

$$[\mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{p}_\infty] = [\mathfrak{p}_3 - \mathfrak{p}_\infty].$$

Exercice 6 *Prouvez que l'addition définie sur $C(L)$ avec Pic^0_C coïncide avec l'addition définie par l'intersection des droites avec C et que la lacune dans cette définition (l'associativité) est réparée.*

3 Les invariants et les isogénies des courbes elliptiques

Dans toutes les sections suivantes soit E une courbe elliptique, i.e. une courbe plane projective régulière de genre 1 avec $P_\infty \in E(K)$.
Pour simplifier quelques parts des discussions suivantes nous supposerons que $\mathrm{car}(K)$ ne divise pas 6. Pour la théorie ce n'est pas nécessaire, et les courbes elliptiques définies sur les corps de caractéristique 2 ou 3 sont importantes pour l'applications en cryptographie. Il est donc une
Exercice générique: Pour tous les résultats suivants étudiez les résultats analogues pour $\mathrm{car}(K) = 2, 3$.

3.1 Equation de Weierstraß courte (WNF) et les invariants

Nous savons que E peut être donnée par une équation

$$Y^2Z + a_1XYZ + a_3YZ^2 =$$
$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Par la transformation

$$X \to X, Y \to Y - \frac{1}{2}(a_1 X + a_3 Z), Z \to Z$$

on obtient l'équation (après de re-nommer les coordonnées par X, Y, Z)

$$Y^2 Z = X^3 + b_2 X^2 Z + b_4 X Z^2 + b_6 Z^3.$$

C'est l'équation de Weierstraß courte pour les corps avec caractéristique $\neq 2$.
Si $\mathrm{car}(K) \neq 3$ on peut simplifier encore plus.
Par la transformation

$$X \to X - \frac{1}{3} b_2 Z, Y \to Y, Z \to Z$$

on arrive à l'équation

$$\mathbf{WNF} : Y^2 Z = X^3 + a X Z^2 + b Z^3$$

avec $a, b \in K$ donnés par formules explicites en a_1, a_2, a_3, a_4, a_6.
L'équation de type **WNF** est nommée *l'équation de Weierstraß (courte)* de E pour les corps avec caractéistique premier à 6.
Notation:

- Nous re-nommerons
$$a_4 := a, \ a_6 := b.$$
- Dans la plupart des cas on travaillera avec l'équation de Weierstraß affine
$$Y^2 = X^3 + a_4 X + a_6$$
et on la dénote aussi par WNF.

Remarque: Dans la littérature classique on a souvent la notation $a_4 = -g_2$ et $a_6 = -g_3$ (sous-section 4.1), et parfois le terme X^3 a un facteur 4. La régularité de E est équivalente avec la condition que le discriminant

$$\Delta_E := -16(4a_4^3 + 27a_6^6) \neq 0.$$

Il n'est pas difficile à vérifier que (a_4, a_6) sont déterminés par la classe d'isomorphismes de E jusqu'aux transformations

$$X \to \mu^2 X, Y \to \mu^3 Y, Z \to Z$$

avec $\mu \in K^*$ et des changements résultants

$$(a_4, a_6) \to (\mu^4 a_4, \mu^6 a_6).$$

On voit qu'une transformation de ce type change Δ_E en $\mu^{12}\Delta_E$ et donc que Δ_E n'est pas un invariant de E. Mais

$$j_E = 12^3 \cdot \frac{-4 \cdot a_4^3}{\Delta_E}$$

ne dépend pas du choix des coordonnées et est nommé l'invariant absolu (ou j-invariant) de E. Le j–invariant j_E détermine E jusqu'aux "twists": Plus précisement:

1. Si $a_4 = 0$ (i.e $j_E = 0$) alors pour chaque $a_6 \in K^*$ la courbe E est isomorphe à

$$E' : Y^2 = X^3 + a_6' \text{ sur } K((a_6/a_6')^{1/6}).$$

2. Si $a_6 = 0$ (i.e. $j_E = 12^3$) alors pour chaque $a_4' \in K^*$ la courbe E est isomorphe à

$$E' : Y^2 = X^3 + a_4' X \text{ sur } K((a_4/a_4')^{1/4}).$$

3. Si $a_4 a_6 \neq 0$ alors pour chaque $d \in K^*$ la courbe E est isomorphe à

$$E^{(d)} : Y^2 = X^3 + a_4' X + a_6'$$

avec

$$a_4' = d^2 a_4 \text{ et } a_6' = d^3 a_6 \text{ sur } K(\sqrt{d}).$$

Donc sur $\overline{K}$ la classe d'isomorphisme de E est uniquement déterminée par j_E.
Si K n'est pas algébriquement clos E est déterminée par j_E seulement jusqu'aux **twists**.
Si $j_E \neq 0, 12^3$ les twists sont quadratiques comme dans (3) ci-dessus.
Une observation élementaire mais importante est que par tout $j \in K$ il y a une courbe elliptique E_j définie sur K avec $j-$invariant j, et cette courbe est uniquement déterminée jusqu'aux twists.

3.2 Isogénies

Définition 3.1

- *Deux courbes elliptiques E/K et E'/K sont isogène sur K s'il existe une application polynomiale (i.e. un morphisme projectif) du $\mathbb{P}^2_K$ sur lui-même qui, restreint à E, induit une application non-constante (i.e. un morphisme projectif surjectif)*

$$\psi : E \to E'$$

avec $\psi((0,1,0)) = (0,1,0)$.

- *En cas que $E = E'$ on dit que ψ est un endomorphisme de E.*

Théorème 3.2 *L'application ψ induit un homomorphisme de groupes de*

$$\psi_* : E(L) \to E'(L)$$

pour chaque sur-corps L de K:
ψ est un homomorphisme dans la catégorie des variétés abéliennes.
Le noyau de ψ est l'image inverse du sous-schéma réduit $\{(0,1,0)\}$, il est un sous-schéma $ker(\psi)$ de E qui est un schéma de groupe fini (mais pas réduit en général).

Définition 3.3 *L'ordre du* schéma *$ker(\psi)$ est le degré de ψ.*

Exemple 3.4 *Soit $m \in \mathbb{N}$ et E une courbe elliptique.*
$[m]$ est l'endomorphisme de E défini qu'on obtient par l'addition d'un point P à lui-même $m-1$-fois.
Pour $-m \in \mathbb{N}$ on définie $[m]$ par

$$[m] = \ominus \circ [-m].$$

Pour $m = 0$ on définie

$$[0] : P \mapsto (0,1,0)$$

pour chaque $P \in E(\overline{K})$.

m est une isogénie si $m \neq 0$.
Par $E[m]$ on défini le noyau de [m] (comme sous-schéma de E).

Exercice 7 *Déterminez $E[2]$ et $E[3]$.*

Par une manière évidente on donne l'ensemble des endomorphismes de E la structure d'un anneau: L'addition est induite par l'addition sur E, et la multiplication est la composition des endomorphismes.
Cet anneau est dénoté par $\mathrm{End}_K(E)$. Il est égal à l'ensemble des isogénies de E à E uni avec l'application [0].
Par l'exemple 3.4 on observe qu'on a un monomorphisme canonique

$$\mathbb{Z} \hookrightarrow End_K(E)$$

par

$$z \mapsto [z].$$

De plus, $\mathrm{End}_K(E)$ n'a pas des diviseurs de zéro.

Quelques propriétés des isogénies

Fait 3.5 *Pour chaque isogénie ψ de degré m il existe une isogénie unique $\hat{\psi} : E' \to E$, le dual de l'isogénie ψ, de sorte que*

$$\hat{\psi} \circ \psi = [m]_E \quad et \quad \psi \circ \hat{\psi} = [m]_{E'}.$$

Chaque isogénie ψ est factorisé par une isogénie séparable ψ_{sep} et une isogénie radicielle ψ_{ins}:

$$\psi = \psi_{sep} \circ \psi_{ins}.$$

Une isogénie ψ est séparable si et seulement si degré$(\psi) = |ker(\psi)(\overline{K})|$.
Les isogénies totalement inséparables ont un degré égale à une puissance de $\mathrm{car}(K)$.
Génériquement, on a $\mathrm{End}_K(E) = \mathbb{Z}$. Il est donc très intéressant d'étudier les courbes elliptiques pour lesquelles ce n'est pas vrai.

Définition 3.6 *Si* $\mathrm{End}(E)$ *est strictement plus grand que* $\mathbb{Z}$ *nous disons que E est une courbe avec "*multiplication complexe (CM)*".*

4 Courbes elliptiques sur des corps spéciaux

4.1 Courbes elliptiques sur $\mathbb{C}$

Soit $K = \mathbb{C}$ le corps des nombres complexes.
Dans la sous-section suivante nous décrirerons la théorie classique des courbes elliptiques sur $\mathbb{C}$ caracterisée par l'interaction de la géométrie analytique et algébrique.

4.1.1 Réseaux et courbes

Soit Λ un réseau de $\mathbb{C}$:

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \text{ avec } \mathrm{Im}(\omega_2/\omega_1) > 0.$$

Le groupe

$$T_\Lambda = \mathbb{C}/\Lambda$$

est muni d' une structure de variété analytique compacte: il est un groupe de Lie compact commutatif, en fait, il est un **tore de dimension** 1**.**
Il en résulte qu'il y a une structure sous-jacente d'une courbe algébrique projective E_Λ du genre 1 et que les fonction méromorphes sur T_Λ forment le corps des fonctions rationelles $F(E_\Lambda)$ de E_Λ.
Par des théorèmes standards (de Weierstraß et de Mittag-Leffler) on peut construire des fonctions méromorphes de $F(E_\Lambda)$, qui sont par définition des fonctions méromorphes sur $\mathbb{C}$ périodiques par rapport à Λ.
Un exemple explicit est la fonction de Weierstraß

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right),$$

une autre fonction dans F_E est sa dérivé $\wp'(z, \Lambda)$. Ces deux fonctions satisfont une équation différentielle

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 - 15G_4\wp - 35G_6$$

avec les séries d'Eisenstein $G_4(\Lambda)$ et $G_6(\Lambda)$ ou

$$G_n(\Lambda) := \sum_{\omega \ in \Lambda \setminus \{0\}} \omega^{-n}.$$

Définissons $g_2(\Lambda) = 15G_4$ et $g_3(\Lambda) = 35G_6$.

Il n'est pas difficile de voir que

$$F(E_\Lambda) = \mathbb{C}(\wp, \wp').$$

L'application

$$\phi : \mathbb{C}/\Lambda \to \mathbb{C}^2 \cup \infty$$
$$z \mapsto (\wp(z), \frac{1}{2}\wp'(z))$$

est une bijection holomorphe du tore T_Λ à la courbe elliptique

$$E_\Lambda : Y^2Z = X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3.$$

Le point $(0, 1, 0)$ correspond à $\bar{0} \in \mathbb{C}/\Lambda$, la classe des pôles de $\wp$ et $\wp'$.
Mais on a plus: ϕ est un homomorphisme de groupes (avec respect de l'addition $\oplus$ sur $E_\Lambda(\mathbb{C})$) et par conséquence les fonctions de Weierstraß satisfont *des formules d'addition.* Inversement une courbe elliptique définie sur $\mathbb{C}$ a une structure de groupe de Lie compact de dimension 1 et ainsi il y a un réseau Λ avec $E \simeq E_\Lambda$.

Théorème 4.1 *Deux courbes elliptiques E et E' avec réseau Λ et Λ' sont isomorphes si et seulement s'il y a un élément $\alpha \in \mathbb{C}$ avec $\alpha \cdot \Lambda = \Lambda'$.*

Identifiant les courbes elliptiques isomorphes nous pouvons supposer que

$$\Lambda_E = \mathbb{Z} + \tau_E \cdot \mathbb{Z} \text{ avec } Im(\tau_E) > 0.$$

τ_E est déterminée par E jusqu'aux transformations

$$\tau_E \mapsto \frac{a\tau_E + b}{c\tau_E + d}$$

avec $a, b, c, d \in \mathbb{Z}$ et $ad - bc = 1$.

Le j- invariant comme fonction méromorphe Soit $\mathbb{H}$ l'ensemble des nombres complexes z avec la partie imaginaire $Im(z)$ positive.
La fonction holomorphe

$$j : \mathbb{H} \to \mathbb{C}$$
$$\tau_E \mapsto j(\tau_E) = 1728\frac{g_2(\Lambda_\tau)^3}{4g_2(\Lambda_\tau)^3 - 27g_3(\Lambda_\tau)^2}$$

est surjective et détermine la classe d'isomorphie de E uniquement. En plus,

$$j_E = j(\tau_E).$$

4.1.2 Isogénies et endomorphismes

Nous déterminons les *classes d'isogénie* des courbes elliptiques sur $\mathbb{C}$ en utilisant la théorie de tores complexes:

Proposition 4.2 *Soient E, E' des courbes elliptiques définies sur $\mathbb{C}$ avec le réseau Λ respectivement Λ'.*
Ensuite E est isogène à E' si et seulement s'il existe sur $\alpha \in \mathbb{C}^*$ avec $\alpha\Lambda \subset \Lambda'$.
En ce cas nous désignons par η_α l'isogénie de E à E' induite par l'application

$$\mathbb{C}/\alpha\Lambda \to \mathbb{C}/\Lambda'.$$

Le noyau de η_α est canoniquement isomorphe à $\alpha^{-1}\Lambda'/\Lambda$.

Corollaire 4.3 *Supposons que E est une courbe elliptique sur $\mathbb{C}$ avec $j_E = j(\tau_E)$.*
Puis

$$\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C};\ \alpha\Lambda_{\tau_E} \subset \Lambda_{\tau_E}\}.$$

En particulier, $\mathrm{End}_{\mathbb{C}}(E)$ est un anneau commutatif sans diviseurs de zéro.
Il y a une injection naturelle de $\mathrm{End}_{\mathbb{C}}(E)$ dans $GL_2(\mathbb{Q})$, et parce que l'image est commutative la dimension de $\mathrm{End}_{\mathbb{C}}(E) \otimes \mathbb{Q}$ sur $\mathbb{Q}$ est ≤ 2.

Remarque 4.4 *Un principe général, le **principe de Hurwitz**, implique que le collaire reste vrai si on remplace $\mathbb{C}$ par un corps de caractéristique 0 quelconque.*

4.1.3 Points de torsion

Nous rappelons que, pour $n \in \mathbb{N}$, $E[n]$ est le noyau de l'endomorphisme relié à la multiplication scalaire par n. Donc $E[n](\mathbb{C})$ est le "*groupe des points de torsion d'ordre (divisant) n de la courbe E*".
Il est très simple de déterminer $E[n](\mathbb{C})$ pour E associée au réseau Λ_E:

$$E[n](\mathbb{C}) = \frac{1}{n}\Lambda_E/\Lambda_E \cong \mathbb{Z}/n \times \mathbb{Z}/n.$$

Une version du principe de Hurwitz implique:

Théorème 4.5 *Soient E une courbe elliptique définie sur un corps K et $n \in \mathbb{N}$ premier à car(K).*
Alors

$$E[n](\overline{K}) \cong \mathbb{Z}/n \times \mathbb{Z}/n.$$

Comme noyau d'un morphisme $E[n](\overline{K})$ est l'ensemble des zéros de certains polynômes en $K[X, Y, Z]$.
Pour

$$E : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

on vérifie facilement que ces polynômes ont des coefficients dans $\mathbb{Z}[a_4, a_6]$.
Evidemment $P_\infty \in E[n]$, et tous les points dans $E[n](\overline{K}) \setminus \{P_\infty\}$ sont des points affines sur E.
En coordonnées affines on obtient:

Corollaire 4.6 *Nous supposons que n est impair. Soit*

$$P = (x, y) \in E[n](\overline{K}) \setminus \{P_\infty\}.$$

Alors x est le zéro d'un polynôme

$$\Psi_n(X) \in \mathbb{Z}[X, a_4, a_6] \text{ de degré } \frac{(n-1)}{2}.$$

4.1.4 Représentations galoisiennes

Dans cette sous-section le corps K est un corps de caractéristique premier au nombre naturel n, et E est une courbe elliptique sur K.
Rappelons que G_K est le groupe de Galois absolu de K.
Parce que $E[n](\overline{K})$ est l'ensemble des zéros des polynômes à coefficients dans K il suit que G_K opère sur $E[n]$.
Cette opération induit une représentation continue

$$\rho_{E,n} : G_K \to Gl(2, \mathbb{Z}/n),$$

nommée "la représentation galoisienne reliée aux points d'ordre n de E".
Les représentations $\rho_{E,n}$ et leur limites projectives $\tilde{\rho}_{E,\ell}$ (pour $n = \ell^k$ et $k \to \infty$) sont fondamentales pour l'arithmétique des courbes elliptiques **et**

des corps K. En plusieurs exemples importants ces représentations sont semi-simples et donc déterminée par leur polynômes caractéristiques $\chi_{\rho_{E,n}}(T)$ resp. $\chi_{\tilde{\rho}_{E,\ell}}(T)$.

Nous remarquons que les résultats obtenues dans les sub-sections d'au-dessus forment la base pour la théorie des
courbes modulaires, par exemple des courbes $\mathbf{X_0(n)}$ qui paramétrisent les isogénies avec noyau $\cong \mathbb{Z}/n$, et les
formes modulaires reliées avec cettes courbes.

4.2 Multiplication complexe et théorie des nombres

Nous continuons d'assumer que E est une courbe elliptique sur $\mathbb{C}$.

Définition 4.7 *La courbe elliptique E est une courbe avec multiplication complexe (CM) si et seulement si* $\mathrm{End}_{\mathbb{C}}(E)$ *n'est pas égal à $\mathbb{Z}$, i.e. il y a*

$$\alpha \in \mathbb{C}^* \setminus \mathbb{R} \text{ avec } \alpha\Lambda_E \subset \Lambda_E.$$

Soit E une courbe avec CM et $\Lambda_E = \mathbb{Z} + \tau\mathbb{Z}$ le réseau de E.
Une calculation facile montre:

Fait 4.8 *τ est un entier dans le corps quadratique imaginaire $\mathbb{Q}(\tau)$ et $\mathrm{End}_{\mathbb{C}}(E)$ est un **ordre** en $\mathbb{Q}(\tau)$.*

Inversement:

Proposition 4.9 *Soit K un corps quadratique imaginaire, soit $\mathcal{O}$ un ordre de K, et soit A un idéal de $\mathcal{O}$.*
Ensuite

$$A \subset \mathbb{C}$$

est un réseau, la courbe elliptique

$$E_A := \mathbb{C}/A$$

est une courbe elliptique avec multiplication complexe et

$$\mathrm{End}_{\mathbb{C}}(E_A) = \mathcal{O}.$$

Pour deux idéaux A, A' de $\mathcal{O}$ on obtient: E_A est isomorphe à $E_{A'}$ sur $\mathbb{C}$ si et seulement si A et A' sont dans la même classe d'idéaux de $\mathcal{O}$.

En particulier on a vue que les courbes avec multiplication complexe ont des périodes τ qui sont des nombres *algébriques*. Mais on a plus d'informations: L'invariant absolu $j(\tau)$ est un entier algébrique très spéciale. La déscription précise est le résultat–clé de la théorie du corps de classes des corps quadratiques imaginaires:

Théorème 4.10 *Supposons que E est définie sur $\mathbb{C}$ et a CM avec réseau Λ_E. Soit τ sa période.*
Ensuite $\mathbb{Q}(\tau)$ est un corps quadratique imaginaire, $\mathrm{End}_{\mathbb{Q}(\tau)}(E) = \mathrm{End}_{\mathbb{C}}(E)$ est un ordre $\mathcal{O}_E$ en $\mathbb{Q}(\tau)$ et l'invariant absolu $j(\tau)$ est contenu dans le corps de classes de $\mathcal{O}$.
L'invariant $j(\tau)$ est la fonction j évaluée à l'ideal de $\mathcal{O}_E$ qui est isomorphe à Λ_E.

Corollaire 4.11 *Soit E une courbe elliptique sur $\mathbb{C}$ avec CM.*
Alors il y a une courbe E_0 définie sur un corps de nombres (plus précisement, un corps de classe d'un ordre dans un corps quadratique imaginaire) tel que $C \times \mathbb{C}$ est isomorphe à E.

4.3 Courbes elliptiques sur des corps finis

4.3.1 Corps finis et l'endomorphisme de Frobenius

Soit p un nombre premier, $k \in \mathbb{N}$ et $q = p^k$.
$\mathbb{F}_q$ est le corps avec q éléments.
L'automorphisme de *Frobenius* π_q est l'automorphisme de $\overline{\mathbb{F}_q}$ définie par

$$\pi_q(x) = x^q;\ x \in \overline{\mathbb{F}_q}.$$

On a

$$\pi_q(x) = x \text{ si et seulement si } x \in \mathbb{F}_q,$$

d'où

$$\pi_q \in G_{\mathbb{F}_q}.$$

De plus, π_q est un générateur topologique de $G_{\mathbb{F}_q}$ et toute application φ continue de $G_{\mathbb{F}_q}$ dans un éspace topologique est uniquement déterminée par $\varphi(\pi_q)$.

L'opération de π_q sur le plan projective est obtenue en appliquant π_q aux fonctions coordonnées homogènes:

$$(X, Y, Z) \mapsto (X^q, Y^q, Z^q).$$

Soit E une courbe elliptique définie sur $\mathbb{F}_q$ et donnée par une équation cubique

$$E : Y^2Z + a_1XYZ + a_3YZ^2 =$$

$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Alors $\pi_q(E)$ a l'équation

$$(Y^2Z)^q + a_1(XYZ)^q + a_3(YZ^2)^q =$$

$$= (X^3)^q + a_2(X^2Z)^q + a_4(XZ^2)^q + a_6(Z^3)^q.$$

Parce que $a_i^q = a_i$ on a

$$((Y^2Z) + a_1(XYZ) + a_3(YZ^2))^q =$$

$$(X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)^q$$

et ainsi: $\pi_q(E)$ est isomorphe à E et $\pi_{q|E}$ est un endomorphisme de E, aussi appelé π_q. De plus,

$$\pi_q : E(\overline{\mathbb{F}_q})) \to E(\overline{\mathbb{F}_q})$$

est un ismorphisme de groupes. Mais π_q n'est pas un isomorphisme de E!
Regardons la situation au niveau des fonctions:
Soit $\mathbb{F}_q(X, Y) = F_E$ le corps des fonctions de E. π_q applique X to X^q et Y

to Y^q et ainsi π_q induit une injection du corps de functions de $\pi_q(E)$ into $\mathbb{F}_q(X,Y)$:

$$\pi_q^* : \mathbb{F}_q(X^q, Y^q) \hookrightarrow \mathbb{F}_q(X,Y).$$

L'extension $\mathbb{F}_q(X,Y)/\mathbb{F}_q(X^q,Y^q)$ est purement inséparable de degré q, et par consequence π_q est un endomorphisme purement inséparable, le noyau de π_q est un schéma de groupe radiciel.
L'endomorphisme dual de π_q est nommé v_q, le "Verschiebung".
On a

$$\pi_q \circ v_q = [q].$$

Définition 4.12 *E est supersingulière si v_q est inséparable, ou équivalent, si*

$$E[p](\overline{\mathbb{F}_q}) = \{P_\infty\}.$$

E est ordinaire si E n'est pas supersingulière.

4.3.2 Structure de l'anneau $\mathrm{End}_{\mathbb{F}_q}(E)$

Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$.
π_q est un endomorphisme de degré q et par suite $\neq [z]$ pour chaque $z \in \mathbb{Z}$.
Il en résulte que E est une courbe avec CM. Le résultat fondamental de **Deuring** est:

Théorème 4.13 *Soit E une courbe elliptique sur $\mathbb{F}_q$ qui est ordinaire.*

1. *(**Lifting**): Il y a un corps de nombres K avec l'anneau des entiers O_K, un idéal premier $\mathfrak{P} \subset O_K$ avec le corps résiduel $\mathbb{F}_q$ et une courbe elliptique $\tilde{E}$ définie sur K par une équation de Weierstraß avec des coefficients dans O_K tel que la réduction des coefficients de l'équation modulo $\mathfrak{P}$ est une équation de Weierstraß pour E et tel que*

$$\mathrm{End}_K(\tilde{E}) = \mathrm{End}_{\mathbb{F}_q}(E).$$

2. *$\tilde{E} \times \mathbb{C}$ est uniquement déterminée par E et est appelée le **Deuring Lift** (ou lift canonique) de la courbe E.*

3. *Par conséquence* $\mathrm{End}_{\mathbb{F}_q}(E)$ *est un ordre dans le corps quadratique imaginaire* $\mathbb{Q}(\pi_q)$.
En particulier, π_q *peut être identifier avec un entier algébrique de degré* 2.

4. *La norme de* π_q *est* q.

Corollaire 4.14 *La trace* $tr(\pi_q)$ *de* π_q *satisfait l'inégalité*

$$|tr(\pi_q) - q - 1| \leq 2\sqrt{q}.$$

Pour prouver ce corollaire on observe que le discriminant de

$$X^2 - tr(\pi_q)X + q$$

est négatif.
Une conséquence du Théorème 4.13 est que $\mathrm{End}_{\mathbb{F}_q}(E)$ est commutatif. Ce n'est pas vrai pour les courbes supersingulières. C'est encore Deuring qui a prouvé:

Théorème 4.15 1. *Il y a un polynôme* $\phi_p(T) \in \mathbb{Z}[T]$ *de degré dépendant de* $p \mod 12$ *et* $\sim p$ *tel que* E *est supersingulière si et seulement si* $\phi_p(j_E) = 0$.

2. *Dans ce cas* $j_E \in \mathbb{F}_{p^2}$.

3. *L'anneau des endomorphismes d'une courbe elliptique supersingulière est un ordre maximal d'une algèbre de quaternions.*

Parce que les courbes supersingulières ne jouent qu'un rôle mineur dans la cryptographie nous nous concentrerons désormais sur le cas que la courbe E est ordinaire.

4.3.3 Le polynôme caractéristique de π_q

Soit E une courbe elliptique ordinaire sur $\mathbb{F}_q$.
Soit n un nombre premier à p et $\rho_{E,n}$ la répresentation induite par l'action de $G_{\mathbb{F}_q}$ sur $E[n]$.

$\rho_{E,n}$ est déterminée par $\rho_{E,n}(\pi_q)$.
Soit $\chi_{E,n}(T)$ le polynôme caractéristique de $\rho_{E,n}(\pi_q)$ dans $\mathbb{Z}/n[T]$.
Une conséquence du Théorème 4.13 est que pour chaque n on a:

$$\chi_{E,n}(T) \equiv \chi_{\pi_q}(T) \mod n$$

où $\chi_{\pi_q}(T)$ est le polynôme minimal de π_q interprété comme élément dans un corps quadratique imaginaire. Il suit que $\chi_{\pi_q}(\pi_q) = 0$, et donc $\chi_{\pi_q}(T)$ est le polynôme caractéristique de
l'*endomorphisme* π_q.

Théorème 4.16 ***(Tate)***
E est isogène à E' sur $\mathbb{F}_q$ si et seulement si les polynômes caractéristiques des endomorphismes de Frobenius sont égaux.

Pour des applications il est très important que l'on peut utiliser $\chi_{\pi_q}(T)$ pour calculer $|E(\mathbb{F}_q)|$.
Une première observation est que

$$E(\mathbb{F}_q) = E(\overline{\mathbb{F}_q})^{\pi_q},$$

l'ensemble des points fixés par π_q, et donc

$$E(\mathbb{F}_q) = ker(\pi_q - id_E).$$

Parce que π_q est inséparable on vérifie que $\pi_q - id_E$ est séparable et donc

$$|E(\mathbb{F}_q)| = |ker(\pi_q - id_E)| = \text{degré de } (\pi_q - id_E).$$

L'algèbra linéaire montre que le degré de $\pi_q - id_E$ est la norme de l'élément

$$\pi_q - 1 \in \mathbb{Q}(\pi_q)$$

et par conséquence on a:

Théorème 4.17

$$|E(\mathbb{F}_q)| = \chi_{\pi_q}(1)$$

Par usage du corollaire 4.14 on obtient

Corollaire 4.18 *On a*

$$||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}.$$

Ce corollaire est un résultat de Hasse et il est l'analogue de la conjecture de Riemann pour le cas des courbes elliptiques sur des corps finis.

4.4 Courbes elliptiques sur des corps de nombres

Par définition, un corps de nombres K est une extension de degré fini de $\mathbb{Q}$. Si l'on veut étudier des courbes elliptiques sur K on peut utiliser l'arithmétique de K, et inversement, on obtient des résultats qui concernent l'arithméthique de K par la théorie des courbes elliptiques.
Un exemple fameux pour ça est la preuve de FLT par A. Wiles.

4.4.1 Le groupe de Mordell-Weil

Soit E une courbe elliptique sur le corps de nombres K.

Fait 4.19

1. *$E(K)$ est un groupe abélien de type fini (Mordell–Weil).*
2. *Il y a des algorithmes efficaces pour calculer $E(K)_{tor}$ (Nagell–Lutz).*
3. *Il y a une borne N dépendent seulement de $[K : \mathbb{Q}]$ tel que*

   $$|E(K)_{tor}| \leq N$$

   (Merel, Parent).
4. *La dimension de $E(K) \bigotimes \mathbb{Q}$ est le rang de E/K, et on n' a pas des algorithmes pour calculer ce nombre pour toutes les courbes E jusqu'aujourd'hui.*

5. *$E(K)\bigotimes\mathbb{R}$ est un espace euclidien avec une métrique induite par la hauteur de Néron-Tate.*

La conjecture fameuse de Birch et Swinnerton-Dyer prédicte qu'on peut calculer le rang de $E(K)$, la torsion de $E(K)$ et des autres invariants par des valeurs spéciales d'une fonction analytique, la série L de la courbe E. Cette série est fortement liée avec les répresentation galoisiennes de E.

4.4.2 Représentations galoisiennes de dimension 2 sur des corps de nombres

Nous supposons que R est un anneau topologique et que $\rho : G_K \to Gl(2, R)$ est une représentation continue.
Pour $\sigma \in G_K$ on dénote par

$$\chi_{\rho(\sigma)}(T)$$

le polynôme caractéristique de $\rho(\sigma)$.

Définition 4.20 *ρ est semi-simple si et seulement si ρ est déterminée par $\{\chi_{\rho(\sigma)}(T); \sigma \in G_K\}$.*

Les automorphismes de Frobenius
Soit ℓ un nombre premier.

Définition 4.21 *Soit $\mathfrak{l}$ un idéal premier de K avec $\ell \in \mathfrak{l}$.*
$\sigma_\mathfrak{l} \in G_K$ est un automorphisme de Frobenius pour $\mathfrak{l}$ s'il y a un idéal premier $\mathfrak{l}'$ de $\bar{\mathbb{Z}}$ avec $\mathfrak{l} \cdot \bar{\mathbb{Z}} \subset \mathfrak{l}'$ tel que pour chaque $x \in \bar{\mathbb{Z}}$ on a: $\sigma_\mathfrak{l}(x) - x^l \in \mathfrak{l}'$.

Théorème 4.22 Čebotarev
Les représentations ρ semi-simples sont déterminées par

$$\{\chi_{\rho(\sigma_\mathfrak{l})}(T); \mathfrak{l} \text{ ideal premier de } K\}.$$

Le resultat suivant dû à Serre est fondamental pour l'arithmétique des courbes elliptiques:

Théorème 4.23 *Soit E une courbe elliptique sans CM.*
Pour presque tous les nombres premiers ℓ la représentation $\rho_{E,\ell}$ est irréductible et donc semi-simple.

Remarque 4.24
Faltings *a preuvé le résultat beaucoup plus général:*
Pour tous les nombres premier ℓ et pour toutes les variétés abéliennes définies sur K les représentations ℓ-adiques reliées sont semi-simple.
Ce résultat est l'ingrédient majeur pour la preuve de la conjecture de Mordell.

4.4.3 Courbes elliptiques sur $\mathbb{Q}$

Maintenant nous supposons que

$$K = \mathbb{Q}.$$

Soit E une courbe elliptique avec une équation de Weierstraß avec des coefficients dans $\mathbb{Z}$ et telle que la valeur absolue du discriminant est minimal.
Soit p un nombre premier et $E^{(p)}$ la cubique obtenue par réduction des coefficients de E modulo p.
Nous savons que $E^{(p)}$ est de type additif ou de type multiplicatif (cas de *réduction mauvaise*) ou une courbe elliptique sur $\mathbb{F}_p$ (cas de *bonne réduction*).
Si E a bonne réduction modulo p nous dénotons par a_p le nombre des points dans $E^{(p)}(\mathbb{F}_p)$.

La série L de la courbe E
Il n'y a qu'un nombre fini de premiers p tel que E a mauvaise réduction modulo p (pourquoi?). Soit S_E l'ensemble de ces nombres premiers. On défini

$$L_E(s) := f^*(s) \cdot \prod_{\ell \notin S_E} (1 - (l + 1 - a_l)l^{-s} + l^{1-s})^{-1}$$

où

$$f^*(s) = \prod_{\ell \in S_E} (1 - t_\ell l^{-s})^{-1}$$

avec $t_\ell = 0$ en cas de type additif,
$t_\ell = 1$ en cas où $E^{(p)ns} = G_m$ et

$t_\ell = -1$ si $E^{(p)ns}$ est un tore non-décomposé . Parce que $K = \mathbb{Q}$ nous avons un objet beaucoup plus fort reliant E et sa série L:
$L_E(s)$ est le produit Eulerien d'une **forme modulaire**.
Ce résultat est une conséquence de la **Conjecture de Serre** qui prédicte qu'une représentation irréductible impaire de dimension 2 dans $Gl(2, \overline{\mathbb{F}_p})$ est modulaire d'un poids et d'un niveau précise.
Et cette conjecture est maintenant un **théorème de Kisin, Khare et Wintenberger**! **Conséquences**
Les résultats suivants sont excitants (du moins pour les *specialists* en géometrie arithmétique):

- La conjecture d'Artin est vrai pour les représentations impaires de dimension 2.
- Les variétés abéliennes de type $Gl(2)$ sont modulaires.
- En particulier, les courbes elliptiques sur $\mathbb{Q}$ sont modulaires.
- La conjecture A-B-C sur $\mathbb{Q}$ est fortement reliée à des congruences parmi les formes modulaires.

Nous finissons cette section par une preuve de 6 lignes mais précise du **dernier Théorème de Fermat**:
Pour $A^p - B^p = C^p$ nous définissons $E : Y^2 = X(X - A^p)(X - B^p)$.
La forme modulaire reliée à $\rho_{E,p}$ a le poids 2 et le niveau 2.
La courbe modulaire $X_0(2)$ a le genre 0 et donc une telle forme n'existe pas.

5 Applications cryptographiques

Dans cette section nous voulons appliquer certaines parties de la théorie profonde des courbes elliptiques sur des corps finis et sur des corps de nombres que nous avons discutés dans les sections précédentes.

Le centre de nos considérations sera le sujet de la cryptographie à clés publiques qui a besoin des outils comme des fonctions hashages, des générateurs aléatoires, et des méthodes pour échanger des clés, signer des messages et d'authentifier.

Au-dessus nous avons vu que deux éleménts $a_2, a_6 \in \mathbb{Z}$ définissent une courbe elliptique sur $\mathbb{Q}$ et donc une série L. Il est intéressant qu'il y a des suggestions d'user (a_4, a_6) comme clé secrète et les coefficients de la série pour construiere des fonctions de hachage (Anshel-Goldfeld, Omar et al.), et de manipuler ces coefficients pour la génération des séries " comportant comme séries aléatoires".
Dans cette leçon nous nous concentrerons à l'échange des clés de type Diffie-Hellman.

5.1 L'échange de clé

Assumons que $A \subset \mathbb{N}$ et $B \subset \mathrm{End}_{set}(A)$ et que la composition de deux éléments de B est encore en B.
En plus, nous assumons qu'il y a un élément $a_0 \in A$ tel que les éléments de B commuent si l'on les restreint à $B\{a_0\}$:

$$b_1(b_2(a_0)) = b_2(b_1(a_0));\ b_i \in B.$$

$$(A, a_0, B)$$

est usé pour l'échange de clé dans une manière évidente: Les partenaires P_i (i=1,2) font un choix pour b_i and publient $b_i(a_0)$.
Alors

$$b_1(b_2(a_0)) = b_2(b_1(a_0))$$

est le secret partagé .

5.2 Exemple: Le système de Couveignes- Stolbunov

Soit E une courbe elliptique ordinaire sur $\mathbb{F}_q$.
Soit S_E l'ensemble des classes d'isomorphisme des courbes elliptiques $E'/\mathbb{F}_q$ avec

$$\mathrm{End}(E') = \mathrm{End}(E) = O \subset \mathbb{Q}(\sqrt{-d}).$$

Nous usons la correspondence 1-1 entre S_E et le groupe des classes d'ideaux $Cl(O)$ de O pour donner S_E la structure d'un espace principal homogène

avec le groupe des translations $Cl(O)$.
Soit $\tilde{E}$ le Deuring lift (théorème 4.13) de E.
Sans perte de généralité on peut assumer que le réseau de $\tilde{E}$ est O.
Soit A un idéal de O et c sa classe d'idéal. Alors $c \cdot [E]$ est la classe d'isomorphie de la courbe elliptique E' qui a le Deuring lift C/A.

Echange de clé : La clé secrète est c, la clé publique est le j-invariant de la courbe E'.

Pour avoir une exécution assez rapide de cet échange on exploit que dans chaque classe c on a un idéal A qui est le produit d'idéaux premiers avant une petite norme. Alors, on peut appliquer une chaine d'isogénies de degré modéré pour calculer le j-invariant de $c \cdot [E]$.

Remarque 5.1 *On ne peut pas appliquer un algorithme de "double et ajoute" parce qu'on n'a pas une multiplication scalaire a faire.*
On peut prouver que la sécurité du système ne dépend pas de la complexité du logarithme discret (voir ci-dessous) dans le groupe des classes d'idéaux de O et ainsi, une application directe de l'algorithme de Shor pour des ordinateurs quantum n'est pas possible.
Mais il existe un algorithme sur un tel ordinateur qui est subexponentiel (voir ci-dessous).

5.3 Les Systèmes de logarithmes discrets (LD)

Les systèmes de logarithmes discrets (LD) sont des outils maintenant "classiques" pour établir l'échange de clé à la manière de Diffie-Hellman.

Définition 5.2 *Un* système(LD) *est un groupe G de l'ordre premier ℓ avec les propriétés suivantes:*

- *Les éléments de G sont présentés compactement, e.g. par la donnée de $O(log(\ell))$ bits.*
- *La loi $\oplus$ de la composition du groupe est facilement implementée et est exécutée très rapidement, e.g. elle a la complexité $O(log(\ell))$.*

- *Le problème (LD) is difficile, i.e.*
  pour des éléments aléatoires

  $$g_1, g_2 \in G$$

  la calculation d'un nombre

  $$k \in \mathbb{Z} \text{ avec } [k]g_2 = g_1$$

  a la complexité

  $$O(exp(C \cdot log(\ell)^{\alpha} \cdot log(log(\ell))^{1-\alpha}))$$

  avec $0 \leq \alpha \leq 1$ *et* α *non loin de* 1.

Le cas idéal est que $\alpha = 1$:
la complexité est exponentielle.

Le pire cas est que $\alpha = 0$:
la complexité est polynomiale.

Le cas que $0 < \alpha < 1$ est appelé
"complexité subexponentielle".

Pour des systèmes usés souvent comme RSA ou le (LD) classique (voir ci-dessous) on a $\alpha = \frac{1}{2}$ (ce qui est tolérable) ou $\alpha = 1/3$ (assez insécure).

5.4 Attaques

Naturellement on peut user "la force brutale" pour computer le LD avec la complexité $O(\ell)$. Mais la structure "groupe" implique la possibilité des attaques plus efficaces.

5.4.1 Attaques génériques

La méthode de Shanks appelée "Baby-Step-Giant-Step" aussi bien que les méthodes de Pollard appelées ρ- et Λ-algorithmes travaillent dans chaque groupe fini et ils ont la complexité $O(\ell^{\frac{1}{2}})$.
Par conséquence elles sont exponentielles avec la constante $C = \frac{1}{2}$.
Le fait positif est que pour les "groupes génériques" nous ne pouvons pas faire mieux.
Mais ...

5.4.2 Le calcul d'indices

En théorie, l'ensemble des éléments d'un groupe est très homogène. En réalité nous avons à user une présentation concrète des éléments de G.
Il y a beaucoup d'exemples où il y a des éléments dans G pour lesquels la computation du (LD) est plus facile qu'en cas général. Basée sur ce fait la méthode de l'attaque par le calcul d'indices est établie. Typicalement, la complexité de cette attaque est subexponentielle.

Exemple 5.3 *1. $G = \mathbb{Z}/\ell$.*
Par usant l'algorithme d'Euclid on voit que le LD est computé avec complexité polynomiale (quadratique).

2. ***Le logarithme discret classique**: Soit $q = p^k$ tel que $\ell | q - 1$. Alors $\mathbb{F}_q^*$ contient le groupe $\mu_\ell =< \zeta_\ell >$ des racines de l'unité d'ordre ℓ (avec ζ_ℓ une racine primitive d'ordre ℓ) et on prend $G = \mu_\ell$.*

   ***Définition 5.4** Le logarithme discret de $\bar{x} \in \mu_\ell$ avec le point de base ζ_ℓ est (chaque) nombre z avec*

   $$\bar{x} = \zeta_\ell^z.$$

   On peut lifter facilement les éléments de $\mathbb{F}_q$ dans les corps de nombres ou dans les corps des fonctions et on peut appliquer les méthodes des cribles dans ses corps basées sur des éléments "lisses".
   Par des résultats nouveaux de Joux et.al. on a une complexité subexponentielle avec $\alpha = 1/3$ et plus petite dans les cas où $k \geq 4$.

5.5 Systèmes (LD) basésur les courbes elliptiques

On cherche des familles de groupes d'ordre premier pour lesquelles le problème (LD) est aussi difficile que pour des groupes génériques. L'idée fondamentale de Koblitz et Miller était d'user les groupes des points rationels sur $\mathbb{F}_q$ des groupes algébriques.
Dans la première section nous avons vus que les cubiques plane projective C produisent tel groupes.
Mais si l'on a des cubiques avec singularité les groupes reliés qu'on obtient sont les groupes additives G_a et multiplicatives G_m sur $\mathbb{F}_q$ et donc les exemples d'au-dessus.Koblitz et Miller ont proposés d'user des courbes elliptiques ou plus général, des varietés jacobiennes.
Un point important pour ce choix est le fait que le lifting des points de $E(\mathbb{F}_p)$ aux points rationels d'un lift $\tilde{E}$ est, contrairement au cas de G_m et G_a, extrêmement difficile, et ce fait est dû à l'existence de la hauteur de Néron-Tate.
La conséquence est qu'une attaque par le calcul d'indices comme dans le cas du (LD) classique n'est pas possible, et des variantes raffinées comme Xedni (Silverman) n'avaient pas eu du succès.
Mais attention: Ça ne signifie pas que pour des courbes elliptiques spéciaux on ne peut pas avoir une attaque dangereuse du calcul d'indices.

5.6 La construction des courbes elliptiques utilisables

Nous chercherons de courbes elliptiques sur $\mathbb{F}_q$ tel que $E(\mathbb{F}_q)$ contient un sous-groupe d'un ordre premier ℓ avec $\ell \approx |E(\mathbb{F}_q)| \approx q$, et un nombre réalistique pour la cryptographie est $q \approx 2^{512}$.
La stratégie est de choisir q et E par hazard et alors de calculer $|E(\mathbb{F}_q)|$.
Il est evident que la première nécessité est qu'on a des algorithmes très rapide pour calculer l'ordre des points sur E (comptage de points), et toutes les méthodes connues calculent le polynôme caractéristique $\chi_E(T)$ de l'endomorphisme de Frobenius sur E et exploitent le corollaire 4.17. On peut suivre deux stratégies:

1. Pour q fixe on choisit une courbe elliptique E par hazard sur $\mathbb{F}_q$ (peut-être un corps favorisé) , ou

2. pour E fixe (peut-être une courbe favorisée) (par example définie sur $\mathbb{Q}$) on varie q.

5.6.1 Structure de $E(\mathbb{F}_q)$

Les deux stratégies ont une bonne chance de succès. La raison est l'existence des théorèmes de densité . Pour simplifier nous supposons dans le premier cas que $p = q$ (ce qui est le cas le plus important pour des applications). Par Deuring, Hasse et Tate, nous savons que pour tout entier t dans l'intervalle

$$I_q = [-2\sqrt{q}, 2\sqrt{q}]$$

de longueur 4 $\sqrt{q}$ il y a une classe d'isogénie des courbes elliptiques E avec

$$\mid E(\mathbb{F}_q) \mid = q + 1 - t.$$

Le théorème des nombres premiers nous dit qu'asymptotiquement il y a $\sim \frac{4\sqrt{q}}{\log(q)}$ nombres premiers parmi ces ordres possibles, et (usant une distribution de probabilité connue pour des nombres de courbes elliptique dans les classes d'isogénie) la probabilité de succès de la première méthode s'en suit.

La probabilité de succès de la deuxième stratégie est donnée par des théorèmes / conjectures de type de Lang-Trotter qui prédisent la distribution des traces d'éléments de Frobenius pour les courbes elliptiques sur les corps de nombres.

5.6.2 La méthode CM

Historiquement, c'était la premiére méthode pour la construction des systèmes utilisables pour la cryptographie. Elle est très efficace et utile jusqu' aujourd'hui.
On constructe (en principe) une courbe avec CM sur un corps de nombre par le choix d'un ordre O dans un corps quadratique imaginaire et on use la description des j-invariants par la théorie des corps de classe et des endomorphismes de Frobenius comme éléments dans l'ordre O qui détermine le polynôme caractéristique de l'endomorphisme de Frobenius. La partie de l'algorithme la plus difficile est la computation du polynôme de classe $h_O(X) \in \mathbb{Z}[X]$ de l'anneau O usant la théorie des formes quadratiques de Gauß. C'est une pré–calculation, et après on a à factoriser $h_O(X)$ sur $\mathbb{F}_p$ pour des nombres premiers p variables ce qu'est très rapide.

5.6.3 L'algorithme de Schoof

Le premier algorithme qui a calculé, pour q et E choisis par hazard, l'ordre de $E(\mathbb{F}_q)$ en temps polynomial est dû à **Schoof**.
Rappelons: Le polynôme caractéristique de l'endomorphisme de Frobenius de E est un polynôme avec des coefficients entiers qui est, simultanément pour les nombres naturels n, le polynôme caractéristique de π_q opérant sur des points de torsion $E[n]$.
Etant donné que la valeur absolue des coefficients est délimitée par q il est suffisant de déterminer cette action pour les nombres $n \leq \log(q)$. C'est le point de départ de l'algorithme de Schoof.
Pour l'exécution de cette idée on doit décrire les points de l'ordre n par les polynôme de division $\psi_n(X)$ qui sont de degré $O(n^2)$ et qui satisfont une récurrence linéaire.

Théorème 5.5 (Schoof)
Pour les courbes elliptiques E la complexité pour calculer $\chi_E(T)$ est délimitée par une fonction polynomiale en $\log(q)$.

La variante d'Atkin-Elkies
Dans la version originale l'algorithme de Schoof est beaucoup trops lent pour l'utiliser pratiquement. La raison en est que le degré de $\psi_n(X)$ est assez grand.
La situation est devenue beaucoup mieux par des observations et des améliorations dues à **Atkin** et **Elkies**:
Au lieu d'utiliser le noyau de la multiplication par n on peut utiliser le noyau des *endomorphismes* de petite norme et déterminer $\chi_E(T)$ *modulo des idéaux* de $\mathrm{End}_{\mathbb{F}_p}(E)$.
Pour ce calcul on use le courbes modulaires $X_0(\ell)$ qui paramétrisent les isogénies de degré ℓ (et qui ont les formes modulaires décrit dans la section ci-dessus commes des differentielles holomorphes). Après des considérations non-triviaux (par exemple, on a à accepter la conjecture de Riemann généralisée pour le résultat optimal) on a:

Théorème 5.6 *Nous assumons que la conjecture de Riemann généralisée est vrai. Soit ϵ un nombre réel positif. Soit E une courbe elliptique définie sur $\mathbb{F}_q$.*

Alors l'ordre de $E(\mathbb{F}_q)$ peut être calculé avec la complexité (probabilistique) $O((\log(q))^\delta)$ avec $\delta \leq 5 + \epsilon$ et conjecturalement $\delta \leq 4 + \epsilon$.

Ce résultat suffit pour construire des courbes elliptiques choisies par hazard sur les corps premiers avec des ordres suffisants pour être utilisée pour des systèmes LD sécures.

5.7 Méthodes $\mathfrak{p}$-adiques

D'un point de vue élevé l'algorithme de Schoof utilise la cohomologie étale des varietés abéliennes.
Le contrepart est la cohomologie p-adique qui est beaucoup plus sophistiquée. Un mot–clé est la cohomologie de Monsky-Washnitzer, et Dwork a contribué des résultats fondamentaux pour cette théorie.
Il est une surprise qu'on peut transformer cette théorie en des algorithmes efficaces pour la calculation de $\chi_E(T)$, au moins dans le cas que p est assez petit et $q = p^k$ avec k assez grand.
Le principe est de lifter l'endomorphisme de Frobenius de $\mathbb{F}_q$ à un endomorphisme d'un schéma analytique rigide p-adique.
Le résultat est un algorithme d'approximation $\mathfrak{p}$-adique pour $\chi_E(T)$, et cela suffi pour déterminer $\chi_E(T)$. Nous mentions ici les travaux fondamentales de Kedlaya mais nous nous restreignons à une équisse de la méthode de Satoh qui fut le premier membre de cette famille d'algorithmes.

La méthode de Satoh
Nous supposons maintenant que E est ordinaire.
Ensuite, par le théorème de Deuring il y a un lift canonique avec le même anneau d'endomorphismes que E. Par l'utilisation de l'approximation de Newton appliquée à la courbe modulaire $X_0(p)$ Satoh a montré comment on peut calculer le j-invariant de ce lift par une approximation p-adique.
Il obtient le résultat:

Théorème 5.7 ***(Satoh)***
Soit p un nombre premier fixe.
Il existe un algorithme déterministique pour calculer le nombre des points rationels de la courbe elliptic E sur un corps fini $\mathbb{F}_q$ avec $q = p^k$ et $j(E) \notin \mathbb{F}_p^2$,

qui a asymptotiquement (pour $k \to \infty$) besoin de $O(k^{2\mu+1})$ opérations en bits. Voici μ est le coût de la multiplication dans $\mathbb{F}_q$.

Inspirée par la méthode de Satoh est la méthode *AGM (moyenne arithmético-géométrique) de Mestre* qui est l'algorithme le plus rapide pour $p = 2$ et $p = 3$ et qui a ses racines dans des travaux de Lagrange et Gauß.

5.7.1 Conclusion

En utilisant les résultats de ci-dessus et compte tenu des résultats de la subsection 5.6.1, nous pouvons construire rapidement un grand nombre de courbes elliptiques avec la propriété qu'un nombre premier ℓ divise $E(\mathbb{F}_q)$ avec ℓ si grand qu'on le désire pour les systèmes (LD).
Il reste de vérifié que la complexité du (LD) est d'une difficulté suffisammant grande.

6 Sécurité

Les bonnes nouvelles sont: Il n'y a pas d'algorithmes connus qui calculent **directement** dans $E(\mathbb{F}_q)$ le logarithme discret plus rapidement que les algorithmes génériques.
En particulier, il n'y a pas d'algorithmes du calcul d'indices connus qui marchent par construire des points sur des courbes elliptiques définies sur des corps de nombres à partir des points dans $E(\mathbb{F}_q)$.
Mais il y a, dans des situations spéciales, des transferts vers d'autres groupes qui sont vulnérables.

Le calcul d'indices dans les variétés jacobiennes Par des travaux d' Adleman, de Huang, Gaudry, Enge et d'autres, nous avons un résultat maintenant classic: Il y a un calcul d'indices subexponentiel pour le LD dans les groupes Pic_C^0 des courbes C avec g_C large.

Plus important pour des applications pratiques est le résultat de C. Diem, P. Gaudry, N. Thériault et E. Thomé suivant:

Théorème 6.1 *Il existe un algorithme (probabiliste) qui calcule le DL dans* Pic_C^0 *pour des courbes* C *de genre groupe* g*, jusqu'à un facteur logarithmique, avec la complexité* $O(q^{(2-2/g)})$.

Cela exclut $g \geq 4$ et, avec un autre résultat de Diem, les courbes du genre $g = 3$ sont en danger.

Pourquoi ces résultats sont-ils de rélevance pour les courbes elliptiques?

6.1 La Descente de Weil

Supposons que le corps de base utilisé est $\mathbb{F}_q$ avec $q = p^k$. En restreignant les scalaires nous trouvons une variété abélienne W_E définie sur $\mathbb{F}_p$ de dimension k donnée d'une façon explicite avec

$$W_E(\mathbb{F}_p) = E(\mathbb{F}_q).$$

Ainsi le LD dans $\mathbb{F}_q$ est équivalent au LD dans $W_E(\mathbb{F}_p)$, et il peut arriver que nous pouvons appliquer le calcul d'indices à W_E come décrit ci-dessus! L'auteur a proposé d'étudier cette situation dans un discours pendant la conférence ECC 1998.
En fait, cette suggestion a eu un nombre considérable de conséquences obtenues par Galbraith, Hess et Smart, de Diem, Gaudry et beaucoup d'autres.

Par exemple, nous savons maintenant que le corps très agréable $\mathbb{F}_{2^{155}}$ est un choix très mauvais pour le corps de base parce que $155 = 5 \cdot (32 - 1)$.

Mais la véritable force de la méthode de descente est démontrée pour k petit.

Théorème 6.2 *(**Diem** et **Gaudry**)*
Nous fixons $k > 2$.
Puis le LD en $E(\mathbb{F}_{q^k})$ *peut être calculé dans un temps* $\tilde{O}(q^{2-2/k})$.
En particulier, pour $k = 4$ *la complexité du LD est* $\tilde{O}(q)$.

Pour prouver ce théorème on utilise comme " base" les points sur E avec X-coordonnées dans $\mathbb{F}_q$. Plus précisément on utilise des sous-variétés définis

par la sommation des polynômes de Semaev. Comme un test d'être lisse on doit résoudre des systèmes d'équations polynomiales qui définent un schéma de dimension zéro. Le succès de la méthode est un exemple magnifique pour la puissance de la géométrie arithmétique algorithmique.

Au delà de ces résultats il y a des développements nouvelles remarquables dû à Diem qui peut construire des tours de corps d'une caractéristque p (fixée) tel que le LD dans cettes tours a une complexité asymptotique subexponentielle.
La conclusion est qu'il est un bon conseil d'user des corps premiers pour le corps de base pour les courbes elliptiques.

6.2 Structures bilinéaires

Définition 6.3 *Supposons qu'il y a des modules A, B, C sur $\mathbb{Z}$ et une applications $\mathbb{Z}$–bilinéaire*

$$Q : A \times B \to C$$

avec

- *Les lois de compositions de groupe dans A, B et C et la calculation de l'application Q est rapide (par exemple en temps polynomial).*
- *$Q(.,.)$ est non-dégénérée dans la première variable: Pour $b \in B$ choisi par hazard on a $Q(a_1, b) = Q(a_2, b)$ si et seulement si $a_1 = a_2$.*

Nous appelons (A, Q)un système LD avec structure bilinéaire.

6.2.1 Quelques applications des systèmes bilinéaires

L'application majeure des systèmes bilinéaires est déstructive parce qu' elle peut affaiblir le système DL par un transfert.

- Le système LD $(A, \circ)$ est au plus aussi sécure que le logarithme discret dans $(C, \circ)$.

Mais il y a aussi des aspects constructives, par exemples:

- On a un système pour échanger des clés parmi trois parténaires.
- On a des protocols basés à une identité publique.
- On a des signatures courtes.

Pour plus d'informations le lecteur intéressé est invité à visiter *Paulo Barreto's Crypto Lounge*. L'état d'art aujourd'hui est que dans tous les cas connus le groupe C est le groupe multiplicatif d'un corps fini, et par le progrès obténu par les travaux récentes (Joux, Diem, Gaudry et al.) pour le LD classique il est devenue douteux que la sécurité du LD en ce cas est suffisante pour les applications décrit ci-dessus.

6.2.2 L'accouplage de Tate–Lichtenbaum

Il est difficile de trouver des structures bilinéaires.
Une source principale est délivrée par les théorèmes de dualité des variétés abéliennes (sur $\mathbb{C}$ on peut prendre le réseau dual de la variété et le mot–clé est la forme de Riemann) et les théorèmes de dualité bien connues dans la théorie des nombres, le mot–clé est la théorie des corps de classes. Ici est une conséquence.
Soit ℓ un nombre premier différent de p et E une courbe elliptique définie sur $\mathbb{F}_q$.
Soit $E[\ell]^{(q)} \subset E[\ell](\overline{\mathbb{F}_q})$ défini par la condition que π_q opère comme $[q]$ sur $E[\ell]^{(q)}$.
Soit k le nombre minimal tel que

$$\ell | q^k - 1.$$

Ainsi $\mathbb{F}_{q^k}$ est la plus petite d'extension de $\mathbb{F}_q$ qui contient une ℓ–ème racine de l'unité.

Théorème 6.4 *Il existe une application bilinéaire non–dégénérée*

$$<,>_\ell \colon E(\mathbb{F}_q)/\ell \cdot E(\mathbb{F}_q) \times E[\ell]^{(q)} \to \mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*\ell}$$

donnée par la règle suivante:
Prenez $Q \in E[\ell]^{(q)}$ *et* f_Q *comme fonction avec diviseur* $\ell \cdot (Q - P_\infty)$.
Prenez $P \in E(\mathbb{F}_q)$ *et représentez la classe du diviseur* $P - P_\infty$ *par un diviseur* D *qui est premier au diviseur* $Q - P_\infty$.
Puis

$$< P + \ell \cdot E(\mathbb{F}_q), Q >= f_Q(D) \cdot \mathbb{F}_{q^k}^{*\ell}$$

.

La forme bilinéaire $<,>$ est appelée *l'accouplage de Tate–Lichtenbaum.* On calcule $<,>$ par une méthode de Miller (et raffinéments) assez rapidement (en temps polynomial) dans $\mathbb{F}_{q^k}$.
Conséquence:
Nous pouvons réduire le logarithme discret dans $E(\mathbb{F}_q))[\ell]$ au logarithme discret dans $\mathbb{F}_{q^k}^*$ avec le coût $O(\log(|\mathbb{F}_{q^k}|)$.
Pour des courbes choisi par hazard k est très grand ($\sim \ell$) et donc la forme bilinéaire $<,>$ ne peut être calculée dans un temps raisonable.
Mais pour les courbes spéciales k peut être assez petit.L'exemple le plus important est le cas où E est une courbe supersingulière. Dans ce cas $k \leq 2$ si $p > 3$ et ≤ 12 pour $p = 2, 3$. Les résultats mentionnés ci-dessus impliquent qu'on ne peut pas utiliser les courbes elliptiques supersingulières pour des systémes LD.

Il y a des travaux intéressants de Barreto, Nährig et. al. où on trouve des exemples des courbes ordinaires avec $k \sim 20$ et on peut espérer que ces courbes puissent être usées pour des applications décrit dans la subsection 6.2.1. En tous cas l'histoire finale du rôle des accouplages dans la cryptographie à clés publiques n'est pas encore écrit jusqu'aujourd'hui.