# Familles de courbes adaptées à la factorisation des entiers

Razvan Barbulescu

▶ **To cite this version:**

Razvan Barbulescu. Familles de courbes adaptées à la factorisation des entiers. 2009. inria-00419218v1

**HAL Id: inria-00419218**

**https://inria.hal.science/inria-00419218v1**

Preprint submitted on 23 Sep 2009 (v1), last revised 29 Sep 2009 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Familles de courbes elliptiques adaptées à la factorisation des entiers

Răzvan Bărbulescu

ENS Lyon, LORIA – EPI CACAO

Septembre 2009

**Résumé**

Dans la méthode des courbes elliptiques pour factoriser des entiers, on utilise en général des familles de courbes particulières qui permettent d'accélérer les calculs. La famille de Suyama est une de ces familles. Son efficacité est due à la présence d'un grand groupe de torsion. Nous proposons une démarche pour construire de nouvelles familles. En particulier, nous avons trouvé deux familles de courbes, chacune paramétrée par une courbe elliptique de rang 1. Il s'agit de sous-familles de la famille de Suyama qui offrent de meilleures performances.

# Table des matières

# Remerciements

Ce mémoire a été rédigé lors de mon stage de Master 1, effectué durant l'été 2009 au LORIA, sous la direction de Pierrick Gaudry. Lors de ce stage, j'ai eu le soutien des membres de CACAO que je voudrais remercier :

- Alexander Kruppa pour les explications données sur le sujet du stage ;
- Emmanuel Thomé pour l'aide sur l'étude de $Aut(R \times R)$ utilisé dans la section 6 ;
- Gaëtan Bisson pour des conseils concernant l'utilisation de l'ordinateur et du logiciel Latex ;
- Guillaume Hanrot, Jérémie Detrey et Nicolas Brisebarre pour m'avoir enseigné les rudiments de la cryptographie et recommandé ce stage ;
- Iram Chelli pour avoir testé les nouvelles familles *Suyama* 11 et *Suyama* 9/4 ainsi que pour les questions qu'on a échangées ;
- Paul Zimmermann pour m'avoir transmis les valeurs de $\sigma$ qui m'ont permis de trouver la famille *Suyama* 9/4 ;
- Romain Cosset pour les réponses concernant aussi bien les courbes elliptiques que l'utilisation des logiciels : MAGMA, Sage et Maple9.5 ;
- Tamas Birkner pour les détails culturels qu'il m'a donnés lors de nos excursions en Lorraine, Alsace et Luxembourg.

# Introduction

Un des problèmes qui ont fasciné Gauss a été le suivant : *Étant donné $N$ entier, trouver effectivement sa décomposition en facteurs premiers.*. Il a même exprimé son souhait que ses efforts soient continués par les générations à venir par une phrase qu'il a écrite dans Disquitiones Arithmeticae : *En outre, la dignité de la science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre.*[1] Avec l'invention de l'ordinateur le voeu de Gauss est en partie réalisé, mais les mathématiciens continuent à factoriser des nombres toujours plus grands lorsqu'ils étudient une équation diophantienne particulière ou un corps de nombres explicite. Par exemple, pour calculer l'anneau des entiers d'un corps de nombres, on commence par factoriser le discriminant du polynôme qui définit le corps en question.

En plus de cela, l'invention de RSA en 1976 a déterminé les informaticiens à s'intéresser à la factorisation. En effet, en cryptographie on utilise des fonctions à sens unique i.e. intuitivement des fonctions $f : \mathbb{N}^m \to \mathbb{N}^n$ bijectives telles que $f$ se calcule par un algorithme rapide alors que $f^{-1}$ est difficilement calculable. Un tel exemple est le problème : *Étant donnés deux nombres premiers $p$ et $q$, calculer $pq$.*, dont l'inverse est : *Étant donné $pq$, trouver $p$ et $q$.* On remarque que la factorisation est encore plus difficile car on ne connaît pas d'avance le nombre de facteurs à trouver. Ainsi, une préoccupation des cryptographes est de trouver le meilleur algorithme de factorisation et de démontrer son optimalité.

# 1 La méthode de factorisation par courbes elliptiques, ECM

## 1.1 Présentation

### 1.1.1 Utilisation de ECM

La méthode de factorisation par courbes elliptiques, abrégée ECM, a été inventée en 1985 par H.W.Lenstra, voir [Len87]. La brique de base de la méthode est un algorithme qui, étant donné un nombre naturel $N$, trouve un facteur premier de $N$ avec une probabilité de succès $Prob(B_1)$ où $B_1$ est un paramètre choisi par l'utilisateur. Heuristiquement, les probabilités de succès de deux exécutions successives de l'algorithme sont indépendantes, exactement comme les jets de dés. Alors la méthode consiste à répéter l'algorithme jusqu'à ce qu'on trouve un facteur premier du nombre à factoriser. On verra dans 1.1.4 comment choisir le meilleur $B_1$ pour optimiser le temps qu'on passe en moyenne jusqu'à ce qu'on trouve. On verra également que la complexité de la méthode ECM est $c(|N|) \cdot e^{(\sqrt{2}+o(1))\sqrt{n}\sqrt{\log n}}$ où $n = \log(p)$ est la taille du nombre premier $p$ à trouver et $C(|N|)$ est un polynôme dans la taille $|N| = \log N$ de $N$. Cela rend ECM la meilleure méthode pour extraire des facteurs premiers $p$ de taille modérée i.e. $p < 10^{60}$. Il est donc utilisé par les logiciels de calcul numérique, comme Maple, Sage et MAGMA.
Par contre, pour attaquer le cryptosystème RSA, il faut factoriser des nombres $N = pq$ tels que $p$ et $q$ sont de taille au delà de la portée de ECM. On utilise alors la méthode NFS, dont la complexité est $\mathcal{O}(e^{1.93n^{1/3}(\log n)^{1/3}})$. Toutefois $NFS$ utilise $ECM$ en tant que sous-routine, en conséquence de quoi tout développement de $ECM$ a des effets en cryptographie.

[1] Recherches Arithmétiques, traduction de A.-C.-M Poullet-Delisle.1807

### 1.1.2 Définitions

**Définition 1.** *Soient $B_1$ et $B_2 \in \mathbb{N}$. On dit qu'un nombre $g \in \mathbb{N}$ est* $(B_1, B_2)$–friable *si $g = p_1^{e_1} p_2^{e_2} ... p_k^{e_k} \pi_0$ pour un $k \in \mathbb{N}$, avec $p_i^{e_i} \leq B_1$ et $\pi_0 = 1$ ou $B_1 \leq \pi_0 \leq B_2$.*

**Définition 2.** *Soit $K$ un corps. On appelle $\mathbb{P}^2(K)$ l'ensemble $(K^3 - \{(0,0,0)\})/\simeq$ où $(X,Y,Z) \simeq (X',Y',Z') \iff \exists \lambda \in K^* \ (X',Y',Z') = (\lambda X, \lambda Y, \lambda Z)$. Soient $A, B \in K$ et $f = Y^2Z - X^3 - AXZ^2 - BZ^3$. On pose $E(A,B) = \{(X:Y:Z) \in \mathbb{P}^2(K) / f(X:Y:Z) = 0\}$. On dit que $E(A,B)$ est une* courbe elliptique *si elle n'a pas de point tel que $\frac{\partial f}{\partial X}$, $\frac{\partial f}{\partial Y}$ et $\frac{\partial f}{\partial Z}$ s'annulent simultanément.*

**Remarque 1.** *Soient $A, B \in K$ et $E(A,B)$ l'ensemble de plus haut. On pose $\Delta(E(A,B)) = -(4A^3 + 27B^2)$. Alors $E(A,B)$ est une courbe elliptique si et seulement si $\Delta \neq 0$.*

**Définition 3.** *Soit $r = \frac{r_1}{r_2} \in \mathbb{Q}$ et $N \in \mathbb{N}$. Si $pgcd(N, r_2) = 1$ on dit que $r$* se réduit *modulo $N$. Dans ce cas on note $\tilde{r} = \tilde{r_1}\tilde{r_2}^{-1} \in \frac{\mathbb{Z}}{N\mathbb{Z}}$ où $\tilde{r_i}$ désigne le reste de $r_i$ modulo $N$.*

**Définition 4.** *Soient $A$, $B \in \mathbb{Q}$ et $E(A,B)$ la courbe elliptique associée. Soit $p$ un nombre premier tel que $A$ et $B$ se réduisent modulo $p$. On dit que $E(A,B)$* a une bonne réduction *modulo $p$ si $E(\tilde{A}, \tilde{B})$ est une courbe elliptique sur $\mathbb{F}_p$. Dans ce cas on écrit $E(A,B)/\mathbb{F}_p$ au lieu de $E(\tilde{A}, \tilde{B})$.*

**Remarque 2.** *$E(A,B)$ a une bonne réduction modulo tous les nombres premiers sauf un ensemble fini : les diviseurs des dénominateurs de $A$ et $B$ ainsi que du numérateur et du dénominateur de $\Delta(E(A,B))$. En effet, pour $p$ premier $\Delta(E(\tilde{A}, \tilde{B}))$ est égal à la réduction de $\Delta(E(A,B))$ modulo $p$.*

**Définition 5.** *Soient $A$, $B \in \mathbb{Q}$ et $E(A,B)$ la courbe elliptique associée. Soit $N \in \mathbb{N}$, $N \geq 2$. On dit que $E(A,B)$ se réduit modulo $N$ si $E(A,B)$ se réduit modulo $p$ pour tout diviseur premier $p$ de $N$.*

**Remarque 3.** *Pour vérifier que $E(A,B)$ a une bonne réduction modulo $N$ on n'a pas besoin de connaître la factorisation de $N$.*

*Justification* On note $A = \frac{A_n}{A_d}$, $B = \frac{B_n}{B_d}$ et $\Delta(E(A,B)) = \frac{\Delta_n}{\Delta_d}$. Alors $E(A,B)$ se réduit *modulo $N$* si aucun diviseur premier de $N$ ne divise $A_d \cdot B_d \cdot \Delta_n \cdot \Delta_d$. Or cela équivaut à $pgcd(A_d B_d \Delta_d \Delta_n, N) = 1$.

**Proposition 1.** *Il existe une loi de groupe abélien sur $E(A,B)$, notée additivement, telle que :*

1. *les coordonnées de $P_3(X_3 : Y_3 : Z_3) = P_1(X_1 : Y_1 : Z_1) + P_2(X_2 : Y_2 : Z_2)$ sont des polynômes dans les coefficients de $P_1$ et $P_2$ ;*
2. *$-P(x:y:z) = P'(x:-y:z)$ ;*
3. *le seul point de la droite $\{Z = 0\}$ sur la courbe est l'élément neutre, $(0:1:0)$.*

*Démonstration.* Voir l'annexe pour les formules de la loi de groupe. Les axiomes du groupe abélien se vérifient facilement sauf l'associativité, pour laquelle on renvoie à [Sil86]. □

**Remarque 4.** *Mis à part l'élément neutre qu'on note $\mathcal{O}$, tous les points d'une courbe elliptique ont un représentant du type $(x,y,1)$. Ces points sont dits affines, noté abusivement $P(x,y) \in E$ et caractérisés par $y^2 = x^3 + Ax + B$.*

**Corollaire 1.** *Soient $N \in \mathbb{N}$ et $A, B \in \mathbb{Q}$ tels que $pgcd(N, \Delta(E(A,B))) = 1$. Soient $0 \leq a, b, c < N$ tels que $a^3 + Aac^2 + Bc^3 - b^2c = 0$ modulo $N$. Alors :*

$$\{p \text{ premier diviseur de } pgcd(c,N)\} = \{p \text{ premier diviseur de } N / (\tilde{a}, \tilde{b}, \tilde{c}) = \mathcal{O} \in E(A,B)/\mathbb{F}_p\}.$$

*Démonstration.* Soit $p$ premier tel que $p \mid pgcd(c, N)$. Comme $p \mid N$ et $N \mid (a^3 + Aac^2 + Bc^3 - b^2c)$, on a $(\tilde{a}, \tilde{b}, \tilde{c}) \in E(A, B)/\mathbb{F}_p$. Comme $p \mid c$, $(\tilde{a} : \tilde{b} : \tilde{c}) \in \{(x : y : z) \in \mathbb{P}_2(\mathbb{F}_p)/z = 0\}$. Par $(iii)$ de la proposition 1, $(\tilde{a} : \tilde{b} : \tilde{c}) = \mathcal{O}$.
Réciproquement, soit $p$ premier diviseur de $N$ tel que $(\tilde{a} : \tilde{b} : \tilde{c}) = \mathcal{O} \in E(A, B)/\mathbb{F}_p$. Alors $\tilde{c} = 0$, donc $p \mid c$. Or $p \mid N$, donc $p \in \{p \text{ premier } /p \mid pgcd(c, N)\}$. □

**Application 1.** *Soit $E(A, B)$ une courbe elliptique sur $\mathbb{Q}$. On suppose connu $N \in \mathbb{N}$ tel que $E(A, B)$ se réduit modulo $N$. On note $p$ un diviseur premier de $N$ qu'on veut trouver. Alors on peut calculer dans le groupe $E(A, B)/\mathbb{F}_p$ sans connaître $p$.*

*Justification*

[étape 1] On représente les points de $E(A, B)/\mathbb{F}_p$ par des éléments de $\mathbb{Z}^3$. Ainsi $(a, b, c) \in \mathbb{Z}^3$ représente $(\tilde{a} : \tilde{b} : \tilde{c}) \in E(A, B)/\mathbb{F}_p$. Soient $P_1$ et $P_2 \in E(A, B)/\mathbb{F}_p$ représentés respectivement par $(x_1, y_1, z_1)$ et $(x_2, y_2, z_2) \in \mathbb{Z}^3$. On applique à $(x_1, y_1, z_1)$ et $(x_2, y_2, z_2)$ les formules de la loi de groupe, qui dépendent de $A$ et $B$, mais pas de $p$. Quand on doit comparer $P_1$ et $P_2$ on le fait *modulo* $N$, mais on teste si $pgcd((x_1 - x_2)(y_1 - y_2)(x_3 - y_3), N)$ vaut 1. On obtient un représentant de $P_1 + P_2$ dans $\mathbb{Z}^3$ car les formules sont polynomiales, donc les entiers qu'on calcule ont les bons restes modulo $p$.

[étape 2] Pour des raisons d'implémentation on remplace $\mathbb{Z}^3$ par $(\frac{\mathbb{Z}}{N\mathbb{Z}})^3$. En effet, cela ne change rien du point de vue mathématique car ($a$ mod $N$) mod p = $a$ mod $p$. Par contre cela améliore le temps de calcul car on travail toujours avec des nombres $\leq N$.

**Remarque 5.** *Si on remplace le corps $K$ de la définition 2 par $\frac{\mathbb{Z}}{N\mathbb{Z}}$ avec $N$ quelconque on obtient un ensemble, noté $E(\frac{\mathbb{Z}}{N\mathbb{Z}})$. Généralement $E(\frac{\mathbb{Z}}{N\mathbb{Z}})$ n'est pas un groupe car on peut avoir $P_1, P_2 \in E(\frac{\mathbb{Z}}{N\mathbb{Z}})$ et $P_1 + P_2 \in \frac{\mathbb{Z}}{N\mathbb{Z}}^3 - E(\frac{\mathbb{Z}}{N\mathbb{Z}})$, même si ce cas n'arrive que pour une proportion négligeable de couples $P_1, P_2 \in E(\frac{\mathbb{Z}}{N\mathbb{Z}})$. Dans la suite on n'utilise pas la structure de $E(\frac{\mathbb{Z}}{N\mathbb{Z}})$. Par contre on dit qu'on fait des calculs dans $E(\frac{\mathbb{Z}}{N\mathbb{Z}})$ comme raccourci pour dire qu'on travaille dans $E(\mathbb{F}_p)$ avec des représentants de $(\frac{\mathbb{Z}}{N\mathbb{Z}})^3$.*

**Remarque 6.** *On voit maintenant qu'en faisant des calculs sur $E(\mathbb{F}_p)$ sans connaître $p$ on peut espérer d'arriver sur $\mathcal{O}$, auquel cas on trouve un multiple de $p$ qui diffère généralement de $N$.*

**Notation 1.**

1. Soit $E/K$ une courbe elliptique et $P \in E$. On pose $m * P = P + ... + P$ pour la loi de groupe de $E/K$.
2. Pour $x$ réel, $[x]$ désigne la partie entière de $x$.
3. Soit $E/K$ une courbe elliptique. On pose $E[m] = \{P \in E(\overline{K})/m * P = \mathcal{O}\}$.
4. Soit $x > 2$. On pose $F(x) = \{\pi \text{ premier}/\pi \leq x\}$.

### 1.1.3 L'algorithme 1

[Données d'entrée] : $N$, $B_1$ et $B_2$ tels que $pgcd(N, 6) = 1$ et $\nexists p, k$ t.q. $N = p^k$.
[Données de sortie] : un facteur $q \neq 1$ de $N$ ou $FAIL$.

[précalcul ] Choisir une courbe elliptique $E(A, B)$ sur $\mathbb{Q}$ au hasard ainsi qu'un point $P_0 = (x_0 : y_0 : 1) \in E(\mathbb{Q})$ d'ordre infini de telle sorte que $E(A, B)$ et $P_0$ se réduisent *modulo* $N$ ;

[phase 1 ] Calculer $Q := m * P_0$ sur $E(\frac{Z}{NZ})$ où $m = \Pi_{\pi \in F(B_1)} \pi^{[log_\pi B_1]+1}$ ;

[phase 2 ] Pour chaque $\pi$ premier, $B_1 < \pi \leq B_2$ :

calculer $(x_\pi : y_\pi : z_\pi) = \pi * Q$ sur $E(\frac{Z}{NZ})$ ;

calculer $q \leftarrow pgcd(N, z_\pi)$ ;

si $q \neq 1$, afficher $q$ et arrêter ;

[postcalcul ]Afficher $FAIL$.

Il faut remarquer qu'on n'arrive au postcalcul que si les phases 1 et 2 ont échoué. Le précalcul prend un temps négligeable car on a des formules pour générer des courbes de rang non nul sur $\mathbb{Q}$. De plus, en pratique on ne doit essayer qu'une ou deux courbes car $Prob(pgcd(E(A,B),N) \neq 1 \mid A, B \in \mathbb{Q})$ est négligeable. En effet $Prob(pgcd(x,N) \neq 1 \mid x \in \mathbb{Q}) = \mathcal{O}(\frac{1}{p})$ où $p$ est le plus petit diviseur premier de $N$.

Pourquoi l'ECM marche ? Supposons que $N$ a un facteur premier $p$ tel que $g := \#E/\mathbb{F}_p$ est $(B_1, B_2)-$*friable*. Alors $g = p_1^{e_1}...p_k^{e_k}\pi_0$ avec $p_i^{e_i} \leq B_1$ et $\pi_0 = 1$ ou $B_1 \leq \pi_0 \leq B_2$. Par conséquent $m := \Pi_{\pi \in F(B_1)} \pi^{[log_\pi B_1]+1}$ est un multiple de $p_1^{e_1}...p_k^{e_k}$. On écrit $m = \lambda p_1^{e_1}...p_k^{e_k}$. Lors de la phase 2, pour $\pi = \pi_0$ on a $\pi * Q = (\pi \cdot m) * P_0 = (\pi \cdot \lambda \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k}) * P_0 = (\lambda \cdot g) * P_0 = (0:1:0)$ *mod* $p$. Par conséquent $p \mid z_\pi$ et alors $p \mid pgcd(N, z_\pi)$. Donc la sortie $q = pgcd(N, z_\pi)$ de ECM est un multiple de $p$.

Il se peut que $q$ soit un multiple strict de $p$, voir $N$. Si on veut trouver $p$ alors on teste la primalité de $q$, algorithme qui prend un temps polynomial, donc négligeable par rapport à ECM. Si $q$ n'est pas premier, on recommence ECM avec des bornes $B_1$ et $B_2$ plus petites pour différentier les facteurs premiers de $N$.

### 1.1.4 Complexité et choix de $B_1$

Comme l'algorithme plus haut n'est pas déterministe, il peut même arriver qu'on essaie à l'infini sans succès, donc on ne parle pas de complexité au pire de cas. Par contre on définit la complexité en moyenne par : temps(algorithme 1)$\cdot$(Nombre moyen d'itérations). Or d'après un exercice simple de la théorie des probabilités, (nombre moyen d'itérations) $= \frac{1}{Prob(\text{succès du algorithme 1})}$.

Voyons d'abord la complexité de l'algorithme de plus haut. D'après [SW93], le meilleur choix pour la borne $B_2$ est tel que la phase 2 prenne le même temps que la phase 1, donc la deuxième partie de l'algorithme ne change pas la complexité. Dans la phase 1 on utilise l'algorithme d'exponentiation rapide pour calculer $m * P_0$. Ainsi on a $\log(m)$ opérations dans $E(\frac{\mathbb{Z}}{N\mathbb{Z}})$. L'arithmétique dans $E(\frac{\mathbb{Z}}{N\mathbb{Z}})$ a une complexité $c(|N|)$ qui ne dépend pas de $p$. On a $\log(m) = \log(\Pi_{\pi \in F(B_1)} \pi^{[log_\pi B_1]+1})$ $= \Sigma_{\pi \in F(B_1)} \log(\pi) \cdot [\frac{\log(B_1)}{\log(\pi)}] \sim \Sigma_{\pi \in F(B_1)} \log(B_1) = \#F(B_1) \cdot \log(B_1)$. D'après le théorème des nombres premiers $\#F(B_1) \sim \frac{B_1}{\log(B_1)}$. Ainsi $\log(m) \sim \log(B_1) \cdot \frac{B_1}{\log(B_1)} = B_1$. On a donc

$$\text{temps}_{\text{algorithme 1}}(p, N) \sim c(N) \cdot B_1.$$

Pour calculer $Prob$(succès du algorithme 1), on a besoin de faire plusieures hypothèses qui sont vérifiées expérimentalement. Entre autres, $\#E/\mathbb{F}_p$ est un nombre arbitraire dans $]p - 2\sqrt{p}, p + 2\sqrt{p}[$ et $Prob(x \text{ est } B_1 - friable/\ x \in ]p - 2\sqrt{p}, p + 2\sqrt{p}[) = Prob(x \text{ est } B_1 - friable/\ x \in ]\frac{p}{2}, \frac{3p}{2}[)$. Donc on ne calcule qu'une valeur heuristique de la complexité. C'est ainsi qu'il est montré dans [CP00] que $Prob(\#E/\mathbb{F}_p \text{ est } B_1 - friable \mid E \text{ courbe sur } \mathbb{Q}) = u^{-u+o(u)}$ avec $u = \frac{\ln p}{\ln B_1}$. Le meilleur $B_1$ est celui qui minimise la complexité au cas moyen ce qui équivaut à minimiser $\frac{B_1}{Prob(B_1)}$. Tout calcul

fait, on trouve $B_1 = exp((\frac{\sqrt{2}}{2} + o(1))\sqrt{ln(p)lnln(p)})$ ce qui offre une bonne approximation de la valeur expérimentale de $B_1$. On remarque qu'on choisit $B_1$ en fonction de la taille anticipée du facteur premier à trouver. Avec cette valeur de $B_1$ on a :

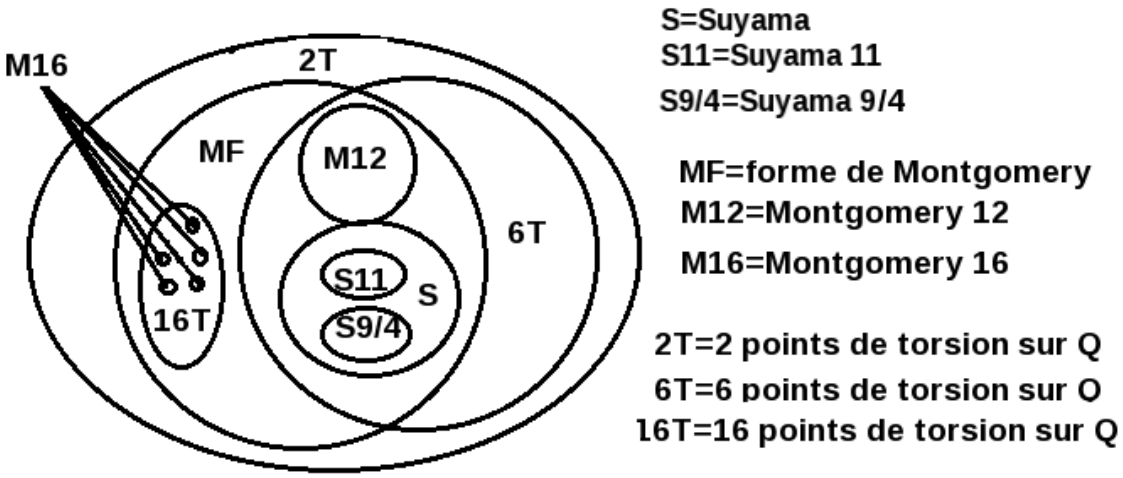
$$\text{Complexité heuristique}_{ECM}(p, N) = c(N) \cdot exp((\sqrt{2} + o(1))\sqrt{ln(p)lnln(p)}).$$

## 1.2 Comment améliorer ECM ?

On peut accélérer aussi bien la phase 1 que la phase 2. Pour améliorer la phase 1 on peut :

1. rendre les opérations dans l'anneau $\frac{\mathbb{Z}}{N\mathbb{Z}}$ plus rapides. Pour cela on utilise des méthodes comme celle de Karatsuba pour la multiplication des polynômes. Mais on peut aussi prendre une famille spéciale de courbes elliptiques où la loi de groupe a une expression simple. Par exemple, on utilise fréquemment les courbes de *Montgomery* : $by^2 = x^3 + ax^2 + x$ avec $b \neq 0$ et $a \neq \pm 2$.
2. choisir des courbes qui ont un grand sous-groupe de torsion $T$ sur $\mathbb{Q}$. En effet, le théorème 1 énoncé plus loin dans le rapport montre que pour tout $p$ premier sauf un ensemble fini $T \subset E/\mathbb{F}_p$, donc $\#E/\mathbb{F}_p$ est un multiple de $\#T$. De plus, on voit heuristiquement que $\#E/\mathbb{F}_p$ se comporte comme un entier aléatoire de $\#T$ dans l'intervalle $]p - 2\sqrt{p}, p + 2\sqrt{p}[$. Ainsi, $Prob(\#E/\mathbb{F}_p$ est $B_1$-friable$)$= Prob$(x \in ]\frac{p-2\sqrt{p}}{\#T}, \frac{p+2\sqrt{p}}{\#T}[$ est $B_1$-friable$)$. On augmente donc la probabilité de succès et diminue a fortiori le nombre moyen d'essais. Donc on accélère ECM.

Afin de créer des courbes à grande torsion, on a créé des familles infinies qui assurent une certaine torsion. Par exemple les courbes sous forme de *Montgomery* i.e. $by^2 = x^3 + ax^2 + x$ garantissent que $\#(E/\mathbb{F}_p)[4] \geq 4$ pour tout $p$ . Ensuite Peter Montgomery a donné dans sa thèse de doctorat deux familles infinies, avec 12, respectivement 16 points de torsion rationnels et un point rationnel d'ordre infini. Ces deux familles, qu'on va appeler *Montgomery* 12 et *Montgomery* 16 ont été peu utilisées à cause du fait qu'elles demandent un précalcul avant de lancer la phase 1 de ECM. À leur place on a utilisé la paramétrisation de *Suyama* qui assure 6 points de torsion rationnels, un point d'ordre infini et 12 points dans $\#(E/\mathbb{F}_p)[12]$ pour tout $p$. On obtient une courbe de la famille *Suyama* en suivant la recette : prendre $\sigma \in \mathbb{Q}$ arbitraire, puis calculer $u = \sigma^2 - 5$, $v = 4\sigma$, $x_0 = u^3$, $z_0 = v^3$, $a = \frac{(v-u)^3(3u+v)}{4u^3v} - 2$ et $b = u/z_0$. Voici plus bas un diagramme des familles connues à présent en précisant que *Suyama* 11 et *Suyama* 9/4 seront définies plus tard dans ce rapport.



# 2 Outils théoriques

## 2.1 Résultats généraux

**Théorème 1.** *Soit $E(A,B)$ une courbe elliptique sur $\mathbb{Q}$ et $p$ tel que $E(A,B)$ se réduit bien modulo $p$ et $m \in \mathbb{N}$ tel que $p \nmid m$. Alors les points de $\{P \in E(A,B)/\mathbb{Q} \mid \ ordre(P) = m\}$ ont des images distinctes dans $E/\mathbb{F}_p$.*

*Démonstration.* On utilise le lemme de Hensel. Pour une preuve détaillée et générale, voir le théorème C.1.4, page 263 de [HS00]. □

**Théorème 2.** *(Mazur) Soit $E/\mathbb{Q}$ une courbe elliptique. Alors le sous-groupe de torsion $E_{torsion}$ est isomorphe à un des groupes :*

$$\frac{\mathbb{Z}}{N\mathbb{Z}} \; ; \; 1 \leq N \leq 10 \text{ ou } N = 12,$$

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2N\mathbb{Z}} \; ; \; 1 \leq N \leq 4.$$

*Démonstration.* Voir [Maz77]. □

**Théorème 3.** *Soit $K$ un corps et $E/K$ une courbe elliptique. Soit $m \in \mathbb{N}$, $m \geq 2$ tel que $car(K) \nmid m$. Alors*

$$E[m] \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

*Démonstration.* Voir [HS00] ch 6.4. □

**Théorème 4.** *(Mordell-Weil) Soit $E/\mathbb{Q}$ une courbe elliptique. Alors il existe un entier naturel $k$, appelé rang de $E$, tel que*

$$E \simeq E_{torsion} \times \mathbb{Z}^k.$$

**Remarque 7.** *Il n'existe pas d'algorithme qui permette de calculer le rang de toute courbe elliptique. Toutefois, MAGMA offre une fonction qui donne le bon résultat dans la plupart des cas et annonce une minoration du rang en cas d'échec.*

## 2.2 Polynômes de division

Soit $P(x,y)$ un point sur la courbe elliptique sur un corps $K$, $E : Y^2 = X^3 + AX + B$ et $m \in \mathbb{N}$. On remarque que les coordonnées $x'$ et $y'$ de $m * P$ sont des fonctions rationnelles de $x$ et $y$. On peut montrer que $(x', y') = (\frac{\theta_m(x,y)}{\psi_m(x,y)}, \frac{\omega_m(x,y)}{\psi_m(x,y)})$ où $\theta_m$, $\omega_m$ et $\psi_m \in K[X,Y]$. Ce sont les polynômes $\psi_m$ qui vont se montrer utiles dans l'étude des points de torsion.

**Définition 6.** *Soit $E(A,B)$ une courbe elliptique sur un corps $K$. On appelle* polynômes $\psi_m$ *la suite ci-dessous d'éléments de $K[X,Y]$ :*

$$\begin{cases} \psi_0 = 0 \\ \psi_1 = 1 \\ \psi_2 = 2Y \\ \psi_3 = 3X^4 + 6AX^3 + 12BX - A^2 \\ \psi_4 = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3) \end{cases}$$

*Ensuite :*

$$\begin{cases}\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \ m \geq 2 \\ \psi_{2m} = \frac{1}{\psi_2}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \ m > 3\end{cases}$$

Vu qu'on n'évalue les polynômes $\psi_m$ que dans des points sur la courbe, on peut simplifier les polynômes. En effet, on montre par récurrence $\forall m \in \mathbb{N}\ \psi_{2m+1}(X,Y) \in K[X] \subset K[X,Y]$ et $\psi_{2m}(X,Y) \in YK[X] \subset K[X,Y]$.

**Définition 7.** *Soit $E : Y^2 = X^3 + AX + B$ une courbe elliptique. On appelle* polynômes de division *de $E$ les polynômes de $K[X]$ :* $\begin{cases}P_{2m+1} = \psi_{2m+1} \\ P_{2m} = (X^3 + AX + B) \cdot \psi_{2m}(X,Y)/(2Y).\end{cases}$

On peut maintenant énoncer un théorème qui se démontre par calcul direct :

**Théorème 5.** *Soit $P(x,y)$ un point non nul sur une courbe elliptique $E$ définie sur un corps quelconque. Alors on a pour tout $m \in \mathbb{N}$*

$$P_m(x) = 0 \iff \psi_m(x,y) = 0 \iff m * P = \mathcal{O}.$$

**Remarque 8.** *On peut calculer les polynômes de division à l'aide de la fonction* `DivisionPolynomial(E,m)` *de MAGMA.*

**Remarque 9.** *Les courbes sous forme de Montgomery ont des polynômes de division plus simples que les courbes génériques. On se place en coordonnées de Montgomery : $x = \frac{3bX-a}{3}$, $y = bY$. Grâce aux formules de passage de la forme de $by^2 = x^3 + ax^2 + x$ à la forme $Y^2 = X^3 + AX + B$ : $A = \frac{3-a^2}{3b^2}$ et $B = \frac{2/9a^3-a}{3b^3}$. On a alors*

$$\begin{aligned}P_2 &= x(x^2 + ax + 1) \\ P_3 &= x^4 + \tfrac{4}{3}ax^3 + 2x^2 - \tfrac{1}{3} \\ P_4 &= P_2(x-1)(x+1)(x^4 + 2ax^3 + 6x^2 + 2ax + 1) \\ P_8 &= P_4(x^4 - 4x^3 + (-4a-2)x^2 - 4x + 1)(x^4 + 4x^3 + (4a-2)x^2 + 4x + 1)P_{reste}\end{aligned}$$

*où $P_{reste}$ est un polynôme de degré* 16.

**Remarque 10.** *On peut montrer par récurrence que $deg(P_{2m+1}) = \frac{(2m+1)^2-1}{2}$. Cela corrobore avec le théorème ci-dessus car $\#E[2m+1] = (2m+1)^2$ et chaque racine de $P_{2m+1}$ est la coordonnée $X$ d'exactement deux points de $E[2m+1] - \mathcal{O}$ : $(X,Y)$ et $(X,-Y)$. De même, on a $deg(P_{2m}) = \frac{(2m)^2-4}{2} + 3$. En effet, $E[2m]$ contient $(2m)^2 - 4$ points autres que ceux de $E[2]$. Ces points forment des paires qui partages un même $X$. En tout $\frac{(2m)^2-4}{2}$ racines de $P_{2m}$ qui donnent des points de $E[2m] - E[2]$. Il reste* 3 *racines qui correspondent aux points de $E[2] - \mathcal{O}$.*

**Définition 8.** *Soit $K$ un corps et $P \in K[X]$. On regroupe par degré les facteurs irréductibles de $P$ et on note $n_i$ le nombre de facteurs de degré $d_i$. Alors on appelle* motif de factorisation *de $P$ l'ensemble $\{(d_1,n_1),(d_2,n_2),...,(d_k,n_k)\}$.*

**Remarque 11.** *Soit $K$ un corps. Soient $m,k \in \mathbb{N}$ tels que $carK \nmid m \cdot k$ et $E/K$ une courbe elliptique. On remarque que $E[m] \subset E[k \cdot m]$. Alors, grâce au théorème 5, toute racine de $P_m$ est racine de $P_{km}$. Comme, de plus les racines des polynômes de division sont simples, on a $P_m \mid P_{km}$. Par conséquent*

$$ppcm\{P_d/\ d \mid n,\ d \neq n\} \ \mid \ P_n.$$

**Notation 2.** *On pose* $P_n^{new} = \frac{P_n}{ppcm\{P_d/\ d|n,\ d\neq n\}} \in K[X]$.

**Remarque 12.** *Pour un $n$ naturel, $P_n$ peut ne pas avoir d'autre facteur irréductible que ceux qui sont évidents : $\{P_d^{new}/\ d$ divise $n\}$. On teste cela à l'aide de Sage pour $K = \mathbb{Q}$ et $E : Y^2 = X^3 + 11X + 13$. Voici dans le tableau suivant les motifs de factorisation des polynômes de division de $E$.*

| | | | |
|---|---|---|---|
| $P_2$ | $[(3,1)]$ | $P_2^{new}$ | $[(3,1)]$ |
| $P_3$ | $[(4,1)]$ | $P_3^{new}$ | $[(4,1)]$ |
| $P_4$ | $[(3,1),(6,1)]$ | $P_4^{new}$ | $[(6,1)]$ |
| $P_5$ | $[(12,1)]$ | $P_5^{new}$ | $[(12,1)]$ |
| $P_6$ | $[(3,1),(4,1),(12,1)]$ | $P_6^{new}$ | $[(12,1)]$ |
| $P_7$ | $[(24,1]$ | $P_7^{new}$ | $[(24,1]$ |
| $P_8$ | $[(3,1),(6,1),(24,1)]$ | $P_8^{new}$ | $[(24,1]$ |

# 3 Paramétrisation de Suyama

## 3.1 Comment la retrouver

Quelques mois après la publication de la forme de *Montgomery*, Hiromi Suyama a annoncé dans [Suy] sa paramétrisation décrite dans 1.2. Comme Suyama n'a jamais publié, sa méthode est restée inconnue ce qui a retardé l'amélioration de sa famille. C'est pour cette raison qu'on donne une méthode détaillée pour retrouver la paramétrisation de Suyama.

On cherche des courbes $E(a,b)$ sous la forme de Montgomery i.e. $by^2 = x^3 + ax^2 + x$ qui possèdent :

1. un point $M_3 = (x_3, y_3) \in \mathbb{Q} \times \mathbb{Q}$ d'ordre 3 ;
2. un point $M_\infty = (x_\infty, y_\infty) \in \mathbb{Q} \times \mathbb{Q}$ d'ordre $\infty$.

On a vu que $E(a,b)$ a exactement 8 points de 3-torsion non nuls sur la clôture algébrique de $\mathbb{Q}$. Ils sont caractérisés par les deux équations suivantes, où $P_3$ est le polynôme de 3-division de la courbe.

$$P_3(x_3) = x_3^4 + \frac{4}{3}ax_3^3 + 6x_3^2 - \frac{1}{3} = 0, \tag{1}$$

$$by_3^2 = x_3^3 + ax_3^2 + x_3. \tag{2}$$

Pour avoir $M_3 \in \mathbb{Q} \times \mathbb{Q}$ on impose que (1) et (2) aient des solutions rationnelles. Ensuite on impose à la courbe d'avoir un autre point rationnel $M_\infty(x_\infty, y_\infty)$ et on vérifie qu'il n'est pas de torsion. On impose donc que $by_\infty^2 = x_\infty^3 + ax_\infty^2 + x_\infty$ ait des solutions rationnelles. Une équation équivalente mais qui simplifie les calculs est obtenue avec la notation $k := y_3/y_\infty$ :

$$\exists k \in \mathbb{Q}.\ x_3^3 + ax_3^2 + x_3 = k^2(x_\infty^3 + ax_\infty^2 + x_\infty). \tag{3}$$

Pour s'assurer que $M_\infty$ n'est pas de torsion il suffit de vérifier qu'il n'est pas de $k-$torsion avec $k \leq 16$ grâce au théorème de Mazur. On va donc éliminer les solutions où $x_\infty$ annule le polynôme $P_2 \cdot P_3 \cdot ... \cdot P_{16}$.

On a ramené notre problème à la résolution d'un système polynomial, $\{(1),(2),(3)\}$. Avant tout calcul, on analyse le système. On remarque que les inconnues $b$ et $y_3$ n'apparaissent que dans

l'équation (2) où elle n'impose pas vraiment de condition. En effet on peut toujours poser la partie carrée de $x_3(x_3^2+ax_3+x_3)$ égale à $y_3^2$ et le reste égal à $b$. On renonce alors à l'équation (2). On a maintenant 2 équations, $\{(1),(3)\}$ et 4 inconnues, $a, x_3, x_\infty, k$. Mis à part des éventuels points de singularité, le système a une surface de solutions réelles. Il reste à voir combien d'entre elles sont rationnelles.

Pour résoudre le système on utilise (1) pour exprimer $a$ en fonction de $x_3$. On remplace $a = a(x_3)$ dans (3) pour obtenir $S(x_3, x_\infty, k) := x_3(x_3^2+ax_3+1) - k^2x_\infty(x_\infty^2+ax_\infty+1) = 0$. Il n'existe pas d'algorithme performant qui trouve les solutions rationnelles d'une telle équation. Par contre *MAGMA* calcule toutes les solutions rationnelles de certaines équations du type $C(x,y)=0$ avec $C$ un polynôme à coefficients rationnels. On doit donc ajouter une nouvelle équation quitte à restreindre la famille de solutions. Plusieurs choix sont possible, mais le meilleur choix semble :

$$x_\infty = x_3^3. \tag{4}$$

On peut maintenant résoudre le système $\{(1),(3),(4)\}$. On sort $a = a(x_3)$ de (1) et $x_\infty = x_\infty(x_3)$ de (4) et on les remplace dans (3). On obtient $C(x_3,k)=0$ avec $C = (x_3^6+ax_3^3+1)-k^2(x_3^2+ax_3+1) = (x_3-1)(x_3+1)(x_3^4+\frac{5}{4}x_3^2-\frac{1}{4}k^2)$. Pour $x_3 = \pm 1$ on a $x_\infty = x_3$ ce qui ne convient pas car $M_\infty$ serait un point de 3-torsion. Il reste donc l'équation

$$x_3^4+\frac{5}{4}x_3^2-\frac{1}{4}k^2 = 0. \tag{5}$$

*Maple*9.5 paramétrise les solution de cette équation par $x_3 = \frac{5-\sigma^2}{4\cdot\sigma}$ et $k = \frac{5}{8}(\frac{\sigma^2}{5}-\frac{5}{\sigma^2})$. On a retrouvé la famille de Suyama. Pour qu'elle soit utilisable on doit calculer $a$, $b$, $x_\infty$ et $y_\infty$ en fonction de $\sigma$. Pour cela on pose $u = \sigma^2-5$ et $v = 4\sigma$. Ainsi $x_3 = \frac{u}{v}$. De (1) on a $a = \frac{-3}{4}\frac{x_3^4+2x_3^2-1/3}{x_3^3} = \frac{-1}{4}\frac{(3u+v)\cdot(u-v)^3}{v\cdot u^3}$. De (4) on a $x_\infty = x_3^3 = \frac{u^3}{v^3}$. De (2) on trouve $b = b(x_3)$ à un facteur carré près, donc il faut faire un choix. Toutefois en changeant $b$ la courbe se transforme dans une courbe isomorphe, donc on peut faire le choix de Suyama sans rien perdre. On pose $b = \frac{u}{v^3}$ et on vérifie que $\frac{x_3^3+ax_3^2+x_3}{b}$ est un carré. On peut calculer $y_\infty$ pour donner le point rationnel d'ordre infini sur $\mathbb{Q}$ mais il n'est pas nécessaire pour l'implémentation actuelle de ECM.

Voyons de plus près les calculs de la paramétrisation de $C(x_3,k)$. On a :
$x_3^4+\frac{5}{4}x_3^2-(\frac{1}{2}k)^2 = 0 \iff (x_3^2+\frac{5}{8})^2 = \frac{k^2}{4}+\frac{25}{64} \iff (x_3^2+\frac{5}{8}-\frac{k}{2})(x_3^2+\frac{5}{8}+\frac{k}{2}) = \frac{25}{64}$
Cette dernière équation a les même solutions que le système suivant :
$$\begin{cases} x_3^2+\frac{5}{8}-\frac{k}{2} = \frac{5}{8}\lambda \\ x_3^2+\frac{5}{8}+\frac{k}{2} = \frac{5}{8}\lambda^{-1} \end{cases} \iff \begin{cases} k = \frac{5}{8}(\lambda^{-1}-\lambda) \\ x_3^2 = \frac{5}{16}(\lambda+\lambda^{-1}+2) = (\frac{\lambda-1}{4})^2\cdot\frac{5}{\lambda} \end{cases}$$
On remarque que $\frac{5}{\lambda} = (\frac{4x_3}{\lambda-1})^2$ est un carré rationnel. On pose donc $\frac{5}{\lambda} = \sigma^2$ avec $\sigma$ un paramètre rationnel. Alors $\lambda = \frac{5}{\sigma^2}$. Et aussi $\frac{4x_3}{\lambda-1} = \pm\sigma$, d'où $x_3 = \pm\frac{\sigma}{4}(\frac{5}{\sigma^2}-1)$. Comme les paires $(+,\sigma)$ et $(-,-\sigma)$ donnent la même valeur de $x_3$, on impose le signe $+$. On a donc $x_3 = \frac{\sigma}{4}(\frac{5}{\sigma^2}-1)$. D'où $k = \frac{5}{8}(\lambda^{-1}-\lambda) = \frac{\sigma^4-25}{8\sigma^2}$.

## 3.2 Performances

Ce qui rend une famille $\mathcal{F}$ meilleure que d'autres est la plus grande probabilité que $\#E/\mathbb{F}_p$ soit friable pour $E$ une courbe générique de $\mathcal{F}$. Toutefois on a besoin d'un indicateur indépendant de

l'implémentation et de la borne $B_1$. On va utiliser celui proposé par Montgomery dans [Mon92].

**Définition 9.** *Soit $E(A,B)$ une courbe elliptique sur $\mathbb{Q}$ et $\pi$ un nombre premier. Pour tout nombre premier $p$ tel que $E(A,B)$ ne se réduit pas modulo $p$, on pose par convention $valuation(\#E(A,B)/\mathbb{F}_p,\pi) = 0$. On appelle* valuation moyenne en $\pi$ *la quantité :*

$$\lim_{N\to\infty} moyenne\{valuation(\#E(A,B)/\mathbb{F}_p,\pi)/\ p\ premier \leq N\}.$$

**Remarque 13.**

1. *Les premiers pour lesquels $E(A,B)$ ne se réduit pas sont en nombre fini, donc ils n'interviennent pas dans la valuation moyenne.*
2. *On ne dispose pas d'une preuve de l'existence de cette limite, mais on observe en pratique une très grande vitesse de convergence. On verra dans 6 des raisons pour cette convergence.*
3. *La valuation moyenne a l'avantage d'être un indicateur facile d'approcher et ainsi utile pour identifier les meilleures courbes. Par contre il ne reste qu'un indicateur qualitatif i.e. des petites différences de la valuation moyenne peuvent cacher de grands écarts sur la probabilité du cardinal d'être $B_1$-friable.*

En suivant l'idée d'Alexander Kruppa, on cherche des meilleures courbes en mesurant la valuation moyenne pour des courbes $E(\sigma)$ de la famille de Suyama avec $\sigma$ entier et petit. Dans le tableau ci-dessus on calcule la valuation moyenne en 2 pour $10^5$ nombres premiers pris au hasard dans $[1, 2^{3\cdot 32}]$. Si on répète le test on trouve des valeurs égales à 0.01 près. On remarque qu'on obtient une précision de 0.05 avec seulement 100 nombres premiers choisis au hasard dans $[1, 2^{32}]$.

Famille de Suyama

| $\sigma$ | valuation moyenne en 2 |
|---|---|
| 10 | 3.33 |
| 11 | *3.66* |
| 12 | 3.33 |
| 13 | 3.33 |
| 14 | 3.33 |
| 15 | 3.33 |
| 16 | 3.33 |
| 17 | 3.33 |
| 18 | 3.33 |
| 19 | 3.33 |

Et aussi avec la famille Montgomery 12. On signale que $t$ est le paramètre décrit dans [Mon92] et qui vit sur une courbe elliptique.

Famille Montgomery 12

| $t$ | valuation moyenne en 2 |
|---|---|
| 1/2 | 3.66 |
| $-11/3$ | 3.66 |
| $-47/28$ | 3.66 |
| $-13/475$ | 3.66 |
| 7199/4026 | 3.66 |

On remarque que la courbe de *Suyama* de paramètre $\sigma = 11$ a les mêmes performances que des courbes génériques de la famille *Montgomery* 12 et que les autres courbes de *Suyama* ont des moindres performances. Comparons maintenant $\sigma = 11$ avec les autres $\sigma$ en distinguant les cas $p = 1\ mod\ 4$ et $p = 3\ mod\ 4$ :

| $\sigma$ | valuation $p = 1\ mod\ 4$ | valuation $p = 3\ mod\ 4$ |
|---|---|---|
| 10 | 3.16 | 3.50 |
| 11 | 3.82 | 3.50 |
| 12 | 3.16 | 3.50 |
| 13 | 3.16 | 3.50 |
| 14 | 3.16 | 3.50 |
| 15 | 3.16 | 3.50 |
| 16 | 3.16 | 3.50 |
| 17 | 3.16 | 3.50 |
| 18 | 3.16 | 3.50 |
| 19 | 3.16 | 3.50 |

On remarque que $\sigma = 11$ se comporte pour $p = 3\ mod\ 4$ comme les autres $\sigma$s. Par contre pour $p = 1\ mod\ 4$, $\sigma = 11$ est nettement meilleur. Alexander Kruppa a posé la question si on peut trouver d'autres valeurs de $\sigma$ avec la même valuation moyenne.

# 4 Améliorer la famille de Suyama

## 4.1 La famille Suyama 11

### 4.1.1 Construction

Afin de trouver une sous-famille de celle de Suyama avec les propriétés de $\sigma = 11$, on impose des nouvelles conditions. Je propose l'équation suivante

$$\exists c \in \mathbb{Q}.\ a + 2 = (-1)bc^2 \tag{6}$$

Avant de justifier ce choix, on va résoudre le système $\{(1), (2), (3), (4), (6)\}$. Cela revient à tester quelles solutions de $\{(1), (2), (3), (4)\}$ vérifient (6). On remplace $a(\sigma)$ et $b(\sigma)$ dans (6) : $(-1)(3\sigma - 5)(\sigma + 3)(\sigma - 5)(\sigma + 1)(\frac{\sigma(\sigma-5)(\sigma+1)}{\sigma^2-5})^2 = (-1)c^2$. Après avoir englobé le carré dans $c^2$ on a

$$3(\sigma - 5/3)(\sigma + 3)(\sigma - 5)(\sigma + 1) - c^2 = 0$$

Cette équation est équivalente à $c'^2 = 3(1+\frac{20}{3}\sigma')(1+8\sigma')(1+6\sigma')$ par la transformation birationnelle $\sigma' = \frac{1}{\sigma-5}$ et $c' = \frac{c}{(\sigma')^2}$. On remarque que cette transformation amène le point $(5, 0)$ de la courbe de départ au point à l'infini de la nouvelle courbe. Ensuite on met l'équation sous forme de *Weierstrass* courte par la transformation affine $\sigma' = 480x$ et $c' = 480^2 y$. On trouve l'équation :

$$y^2 = x^3 + \frac{71}{57600}x^2 + \frac{13}{27648000}x + \frac{1}{17694720000}.$$

*MAGMA* affirme que le rang de la courbe est 1 et nous donne trois générateurs : $P(-1/1600, 0)$, $Q(-1/2880, 0)$ et $M(-1/4800, 1/576000)$, d'ordres respectivement $2, 2$ et $\infty$. L'ensemble des solutions du système est :

$$\{n_P * P + n_Q * Q + n_M * M / n_P, n_Q \in \{0, 1\}, n_M \in \mathbb{Z}\}.$$

On remarque que $(n_P, 0, n_M)$ et $(n_P, 1, n_M)$ donnent des courbes isomorphes, donc on va éviter d'utiliser les deux courbes au même temps. Pour un calcul explicite des éléments de la famille, on utilise la fonction *MAGMA* suivante :

```
function CalculeSigma(nP,nQ,nM)
    F:=EllipticCurve([0,71/57600,0,13/27648000,1/17694720000]);
    P:=F![-1/1600, 0, 1]; Q:=F![-1/2880, 0, 1]; M:=F![-1/4800, 1/576000, 1];
    R:=nP*P+nQ*Q+nM*M;
    xR:=R[1];
    return 1/(480*xR)+5;
end function;
```

### 4.1.2 Justification mathématique

Voyons maintenant pourquoi choisir l'équation (6).

**Définition 10.** *On dit qu'un nombre rationnel $\sigma$ a la* propriété $\sigma_{11}$ *si, pour tout nombre premier $p$ tel que $(\frac{a(\sigma)^2-4}{p}) = 1$, 8 divise $\#E(\sigma)/\mathbb{F}_p$.*

**Notation 3.** *Soient $E/K$ une courbe elliptique, $S \in E$ et $m \in \mathbb{N}$ tel que $pgcd(m, carK) = 1$. On pose $\frac{1}{m}S = \{P \in E/\overline{K}/m * P = S\}$.*

**Lemme 1.** *Tout $\sigma$ qui vérifie (6) a la propriété $\sigma_{11}$.*

*Démonstration.* Soit $\sigma \in \mathbb{Q}$ tel que (6) soit vérifiée. On note $E$ la courbe de *Suyama* correspondant à $\sigma$. Soit $p$ un nombre premier tel que $(\frac{a^2-4}{p}) = 1$. Alors $a^2 - 4$ est un carré de $\mathbb{F}_p$ et le polynôme $x^2 + ax + 1$ a deux racines dans $\mathbb{F}_p$. Notons-les $\alpha_1$ et $\alpha_2$. On remarque que $R := (0, 0)$, $P := (\alpha_1, 0)$ et $Q := (\alpha_2, 0)$ sont tous des points de 2-torsion sur $E/\mathbb{F}_p$. Ainsi $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \subset E(\mathbb{F}_p)$. Donc $E(\mathbb{F}_p)$ a un sous-groupe d'ordre 8 exactement quand il existe un point $M$ de $E/\mathbb{F}_p$ tel que $M+M \in \{P, Q, R\}$.

On vérifie aisément que

$$\frac{1}{2}R = \{(1, \sqrt{\frac{a+2}{b}}), (1, -\sqrt{\frac{a+2}{b}}), (-1, \sqrt{\frac{a-2}{b}}), (-1, -\sqrt{\frac{a-2}{b}})\}.$$

Posons $f(x) = \frac{1}{b}(x^3 + ax^2 + x)$ et appelons $h_1, h_2, h_3, h_4$ les racines du polynôme $q := x^4 + 2ax^3 + 6x^2 + 2ax + 1 = \frac{P_4}{P_2(x-1)(x+1)}$ dans $\overline{\mathbb{F}_p}$. Alors on vérifie que

$$\frac{1}{2}P = \{(h_1, \sqrt{f(h_1)}), (h_2, \sqrt{f(h_2)}), (h_1, -\sqrt{f(h_1)}), (h_2, -\sqrt{f(h_2)})\}.$$

De manière analogue

$$\frac{1}{2}Q = \{(h_3, \sqrt{f(h_3)}), (h_4, \sqrt{f(h_4)}), (h_3, -\sqrt{f(h_3)}), (h_4, -\sqrt{f(h_4)})\}.$$

Afin de trouver des conditions équivalentes pour $h_i \in \mathbb{F}_p$ on analyse le polynôme $q$. Comme $(\frac{a^2-4}{p}) = 1$, il existe un $k \in \mathbb{F}_p$ tel que $k^2 = a^2 - 4$. On peut donc écrire $q$ comme $q = x^2(x + \frac{1}{x} + a - k)(x + \frac{1}{x} + a + k)$. On remarque que $h_1, h_2$ sont les racines de $x(x + \frac{1}{x} + a - k) = 0$ tandis que $h_3, h_4$ sont les racines de $x(x + \frac{1}{x} + a - k) = 0$. Les discriminants de ces deux polynômes sont $(a-k)^2 - 4$ et $(a+k)^2 - 4$ respectivement. Ainsi $q$ a des racines dans $\mathbb{F}_p$ si et seulement si $(\frac{(a-k)^2-4}{p}) = 1$ ou $(\frac{(a+k)^2-4}{p}) = 1$. Finalement, on remarque que $(a-k)^2-4 = a^2+k^2+2ak-4 = 2k^2-2ak = 2k(k-a)$. De manière analogue $(a+k)^2 - 4 = 2k(a+k)$.

À son tour $\sqrt{f(h_i)} \in \mathbb{F}_p$ si et seulement si $(\frac{f(h_i)}{p}) = 1$. On remarque que $(\frac{f(h_i)}{p}) = (\frac{h_i^2(h_i + \frac{1}{h_i} + a)/b}{p})$. D'après le paragraphe précédent, $h_i + \frac{1}{h_i}$ vaut $k - a$ pour $i = 1, 2$ et $-k - a$ pour $i = 3, 4$. On se concentre sur le cas $i = 1$, les autres cas étant similaires. On a $(\frac{(h_1 + \frac{1}{h_1} + a)/b}{p}) = (\frac{k \cdot b}{p})$. D'après (6), on a $b = (a+2) \cdot (-1) \cdot$ carré. Ainsi $(\frac{k \cdot b}{p}) = (\frac{(-1) \cdot (a+2) \cdot k}{p})$. Finalement on remarque que $2(a-k) \cdot (a+2) = (a+1-k)^2$. Ainsi $(\frac{(-1) \cdot (a+2) \cdot k}{p}) = (\frac{2k(k-a)}{p})$. *Conclusion* : $(h_1, \sqrt{f(h_1)}) \in \mathbb{F}_p \times \mathbb{F}_p$ si et seulement si $(\frac{2k(k-a)}{p}) = 1$. De même pour $h_2$, tandis que $h_3$ et $h_4$ dépendent de $(\frac{2k(k+a)}{p})$. Autrement dit, ($\frac{1}{2}Q$ ou $\frac{1}{2}P$ ont des points dans $\mathbb{F}_p \times \mathbb{F}_p$) si et seulement si ( un des symboles $(\frac{2k(k-a)}{p})$ et $(\frac{2k(k+a)}{p})$ vaut 1).

On distingue deux cas :

[$1^{er}$ cas ] $(\frac{-1}{p}) = 1$. Alors $(-1)$ est un carré dans $\mathbb{F}_p$. Par (6), $\frac{a+2}{b} = (-1)c^2$. Alors $\frac{a+2}{b}$ est un carré de $\mathbb{F}_p$. Donc $M(1, \sqrt{\frac{a+2}{b}}) \in \frac{1}{2}R$ est à coordonnées dans $\mathbb{F}_p$.

[$2^e$ cas ] $(\frac{-1}{p}) = (-1)$. On a

$$(\frac{2k(k+a)}{p}) \cdot (\frac{2k(k-a)}{p}) = (\frac{2k}{p})^2 \cdot (\frac{k^2-a^2}{p}) = (\frac{-4}{p}) = (\frac{-1}{p}) = (-1)$$

Comme $(-1) \cdot (-1) = 1$, les deux symboles de Legendre ne peuvent pas être simultanément $(-1)$. Donc, un des points $\{P, Q\}$ a un point de 2-division dans $E(\mathbb{F}_p)$.

Dans tous les cas, 8 divise $\#E/\mathbb{F}_p$. Donc $\sigma$ a la propriété $\sigma 11$. □

### 4.1.3 Vérification expérimentale

Avant de donner une preuve théorique que la propriété $\sigma_{11}$ assure une *valuation moyenne* en 2 égale à celle de $\sigma = 11$ on donne un tableau de valuations. Je précise que certaine valeurs pour lesquelles $\sigma \leq 5$ peuvent donner des courbes singulières. Mais cela ne concerne qu'un nombre fini de $\sigma$s et elles ont été évitées dans le tableau suivant.

Valuation moyenne en 2

| expression | $\sigma$ | $p$ quelconque | $p = 1 \ mod \ 4$ | $p = 3 \ mod \ 4$ |
|---|---|---|---|---|
| $P + M$ | 5/11 | 3, 66 | 3.82 | 3.50 |
| $P + 2M$ | −15/47 | 3, 66 | 3.82 | 3.50 |
| $P + 3M$ | 3595/2171 | 3, 66 | 3.82 | 3.50 |
| $2M$ | −65/11 | 3, 66 | 3.82 | 3.50 |

## 4.2 La famille Suyama 9/4

On a vu qu'une seule courbe peut conduire à la découverte d'une famille infinie avec les mêmes propriétés. Paul Zimmermann a trouvé d'autres bonnes valeurs de $\sigma$ en mesurant la valuation moyenne de tous les $\sigma$ avec des petits dénominateurs et numérateurs. Parmi les valeurs trouvées on a $\{\frac{9}{4}, 11, \frac{5}{11}, \frac{11}{13}, \frac{20}{9}, \frac{47}{3}, \frac{15}{47}, \frac{65}{11}, \frac{121}{169}, \frac{239}{241}, \frac{845}{121}\}$. Elles ont toutes la même valuation moyenne en 2, approximativement 3.66. En éliminant les valeurs de la famille *Suyama* 11 on reste avec $\{\frac{9}{4}, \frac{20}{9}, \frac{121}{169}, \frac{845}{121}\}$. On va trouver une famille infinie qui contient $\frac{9}{4}$ et remarquer qu'elle contient les autres valeurs.

### 4.2.1 Construction

On impose la condition

$$\exists k \in \mathbb{Q},\ b = k^2 \tag{7}$$

Comme pour la famille *Suyama* 11, le système $\{(1), (2), (3), (4), (7)\}$ se ramène à l'équation $\sigma^2 - 5 - \sigma k^2 = 0$. En posant $k_1 = k\sigma$ on obtient une courbe elliptique sous forme de *Weierstrass* courte :

$$\sigma^3 - 5\sigma = k_1^2.$$

Cette courbe est isomorphe à $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}$. Un point de 2 torsion est $P = [0, 0, 1]$ et un point d'ordre infini est $Q = [-1, 2, 1]$. On remarque que $P + nQ$ et $nQ$ donnent des courbes isomorphes, donc on n'utilise que les points $\{P + n * Q \mid\ n \in \mathbb{Z}\}$. Voici une fonction MAGMA qui calcule des valeurs de sigma de cette famille :

```
calcule_sigma9sur4(n)
    F:=EllipticCurve([0,0,0,-5,0]);
    Q:=F![-1,-2,1];
    P:=F![0,0,1];
    return (P+n*Q)[1];
end function;
```

### 4.2.2 Justification mathématique

On rappelle que dans la remarque 9 on a vu que $P_8^{new} = p_1 \cdot p_2 \cdot P_{reste}$ avec :

$$p_1 = x^4 - 4x^3 + (-4a - 2)x^2 - 4x + 1$$

$$p_2 = x^4 + 4x^3 + (4a - 2)x^2 + 4x + 1$$

**Lemme 2.** *Soit $\sigma \in \mathbb{Q}$ qui vérifie (7) et $E$ la courbe de Suyama correspondant à $\sigma$. Soit $p$ un premier tel que $p = 1$ mod 4 et $(\frac{a^2-4}{p}) = -1$. Alors $E/\mathbb{F}_p$ a un point rationnel d'ordre 8.*

*Démonstration.* Les polynômes $p_1$ et $p_2$ sont réciproques et en posant $X = x + \frac{1}{x}$, on trouve :

$$p_1 = X^2 - 4X + (-4a - 4)$$

$$p_2 = X^2 - 4X + (4a - 4)$$

Leurs discriminants respectifs sont $\Delta_1 = 4^2(2 + a)$ et $\Delta_2 = 4^2(2 - a)$.
Comme $(\frac{a^2-4}{p}) = -1$, exactement un des $(\frac{(a+2)/b}{p})$ et $(\frac{(a-2)/b}{p})$ vaut 1. Quitte à remplacer $a$ par

$-a$ i.e. à prendre une courbe isomorphe, on peut supposer que $(\frac{(a+2)/b}{p}) = 1$. On a alors $R_1 := (1, \sqrt{\frac{a+2}{b}}) \in \mathbb{F}_p \times \mathbb{F}_p$ point de 4-torsion sur $\mathbb{F}_p$. Comme $b = k^2$, on a $(\frac{a+2}{p}) = (\frac{(a+2)/b}{p}) = 1$. Donc, $\Delta_1$ est un carré et alors $P_1$ a deux racines $2 \pm \sqrt{a+2}$. Ainsi :

$$p_1 \text{ a des racines } \iff \begin{cases} x + \frac{1}{x} = 2 + \sqrt{a+2} \\ ou \\ x + \frac{1}{x} = 2 - \sqrt{a+2} \end{cases} \text{ a des racines.}$$

Or ce système a des racines exactement quand un des $\delta_1^+$ et $\delta_1^-$ est un carré, où $\delta_1^+ = 4\sqrt{a+2}(\sqrt{a+2}+2)$ et $\delta_1^- = 4\sqrt{a+2}(\sqrt{a+2}-2)$. On remarque que $(\frac{\delta_1^+}{p})(\frac{\delta_1^-}{p}) = (\frac{\sqrt{a+2}^2-4}{p}) = (\frac{2-a}{p}) = -(\frac{2+a}{p}) = -1$. Donc au moins un des $\delta_1^\pm$ est un carré. Donc $E(\mathbb{F}_p)$ a un point rationnel d'ordre 8. □

# 5 Autres pistes de construction

## 5.1 Stratégie

Toutes les paramétrisations qu'on connaît à présent s'exprime comme l'ensemble des solutions d'un système polynomial. De plus, la section 6 suggère que toute autre paramétrisation sera du même type. La brique de base de ma méthode est la proposition ci-dessous. On remarque que l'énoncé fait intervenir une notion nouvelle, le *genre* d'une courbe algébrique. Mais au lieu de le définir on précise qu'on dispose d'un algorithme capable de calculer le genre.

**Proposition 2.** *Soit $\mathcal{C} : C(x, y) = 0$ une courbe telle que $C \in \mathbb{Q}[X, Y]$ est irréductible sur $\overline{\mathbb{Q}}$. On note $g$ =genre($\mathcal{C}$). On suppose que $\mathcal{C}$ possède au moins un point rationnel. Alors on a :*

1. *Si $g = 0$, alors $\mathcal{C}$ est une conique. Dans ce cas il existe $p_x$ et $p_y \in \mathbb{Q}(X)$, deux fractions rationnelles telles que $\mathcal{C} = \{(p_x(\sigma), p_y(\sigma))/\sigma \in \mathbb{Q}\}$.*
2. *Si $g = 1$, alors $\mathcal{C}$ est une courbe elliptique. Dans ce cas, $\mathcal{C}$ est infinie si et seulement si $rang(\mathcal{C}) > 0$.*
3. *Si $g \geq 2$, alors $\mathcal{C}$ est finie.*

*Démonstration.* Voir [HS00] pour le lien entre $g$ et la nature de la courbe. Voyons le reste des affirmations.

1. C'est un corollaire du théorème de Legendre. Voir [IR82], ch 12.
2. D'après le théorème de Mordell-Weil on a $\mathcal{C} \simeq \mathcal{C}_{torsion} \times \mathbb{Z}^k$ avec $k$ fini. D'après le théorème de Mazur, $\mathcal{C}_{torsion}$ est fini. Ainsi $k = 0$ si et seulement si $\mathcal{C}$ est fini.
3. C'est le théorème de Faltings. Voir [HS00].

□

On peut maintenant donner les étapes de la recherche de nouvelles paramétrisations :

1. Trouver des équations polynomiales qui traduisent les bonnes propriétés des courbes.
2. Ajouter des équations ad-hoc jusqu'à ce qu'on ait une inconnue de plus que d'équations.
3. Transformer le système polynomial en un système formé d'une seule équation du type $C(x, y) = 0$ avec $C \in \mathbb{Q}[X, Y]$.

4. Décomposer $C$ en facteurs irréductibles sur $\mathbb{Q}[X,Y]$ : $C = C_1 \cdot ... \cdot C_k$.
5. Pour chaque $1 \leq i \leq k$, calculer le genre $g_i$ de $C_i$.
6. Si $g_i = 0$ alors paramétrer la conique $C_i$.
7. Si $g_i = 1$ alors trouver un système de générateurs $\mathcal{G}$ de $C_i$. On a $C_i = \Sigma_{P \in \mathcal{G}} \mathbb{Z}P$.

**Remarque 14.** *Dans les cas concrets qu'on traite dans ce rapport, toutes les courbes satisfont les hypothèse de la proposition ci-dessus.*

## 5.2 Les détails de chaque étape

[Étape 1.] C'est l'étape la plus importante. On distingue deux cas :

$1^{er}$ cas On ne connaît aucune courbe de la famille qu'on cherche. Dans ce cas les équations traduisent l'existence de quelques points de torsion ainsi qu'un point d'ordre infini. Pour cela on cherche des $m \in \mathbb{N}$ et des facteurs $F_m$ de $P_m^{new}$ qui sont irréductibles dans le cas générique et on impose qu'ils aient des racines rationnelles : $F_m(x_m) = 0$.

Mis à part certains facteurs de $P_m^{new}$ avec $m \leq 12$, on a $deg(F_m) \approx deg(P_m^{new}) \approx deg(P_m) \approx \frac{m^2}{2}$. Or une équation de degré $\frac{m^2}{2}$ avec $m \geq 12$ a peu de chances d'avoir des solutions rationnelles. On va donc se limiter à $m \leq 12$.

On remarque que, si $m = m_1 \cdot m_2$ et $pgcd(m_1, m_2) = 1$, alors $E$ a des points rationnels d'ordre $m_1 m_2$ si et seulement si $E$ a des points rationnels d'ordre $m_1$ *et* d'ordre $m_2$. Or les points d'ordre $m_1$ correspondent aux racines de $P_{m_1}^{new}$. Ainsi $P_{m_1 m_2}^{new}$ a des racines si et seulement si $P_{m_1}^{new}$ *et* $P_{m_2}^{new}$ ont des racines. On préfère donc de remplacer $P_{m_1 m_2}^{new}(x) = 0$ par $P_{m_1}^{new}(x') = 0$ et $P_{m_2}^{new}(x") = 0$ car on travaille avec des équations de moindre degré. Par conséquent on ne regarde que les polynômes $P_{\pi^k}$ avec $\pi$ et $k$ petits.

$2^e$ cas On connaît une courbe $E/\mathbb{Q}$ de la famille qu'on cherche. Alors on peut utiliser des équations plus élaborées. Pour cela on cherche $n_1 \leq n_2 \in \mathbb{N}$ tels que $Prob(\frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_2}\mathbb{Z}} \subset E/\mathbb{F}_p \mid \frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_2-1}\mathbb{Z}} \subset E/\mathbb{F}_p)$ est différente pour $E$ par rapport aux courbes génériques. Comme on le verra dans la section 6, cette probabilité dépend du groupe $Gal(\mathbb{Q}(E[\pi^{n_2+1}])/\mathbb{Q}(E[\pi^{n_1}]))$ où on a noté $\mathbb{Q}(E[m])$ l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de $E[m]$. Or ce groupe dépend des polynômes minimaux sur $\mathbb{Q}$ des coordonnées de $E[\pi^{n_2+1}]$.

Par exemple, pour $\sigma = 11$, $\pi = 2$ et le couple $(n_1, n_2) = (1, 2)$ on a une probabilité de 100% au lieu de 75%. On regarde donc les polynômes minimaux des coordonnées de $E[2^2] - E[2]$ i.e. $y^2 - \frac{a+2}{b}$, $y^2 - \frac{a-2}{b}$ et $x^4 + 2ax^3 + 6x^2 + 6ax + 1$. On conclut que $\sigma = 11$ vérifie une équation qui oblige pour tout $p$ qu'au moins un des polynômes ci-dessus ait des racines sur $\mathbb{F}_p$. D'après 4.1.2, cette équation est (6). A l'aide de cette équation on trouve la famille *Suyama* 11.

[Étape 2.] C'est l'étape la plus difficile. On pourrait même dire que l'art de trouver des paramétrisations consiste à choisir des équations qui rendent le système une courbe de rang 0 ou du moins 1. Par exemple Suyama a trouvé une courbe de genre 0, alors que Montgomery a trouvé plusieures familles de genre 1 qui ont été moins utilisées pour cette raison.

[Étape 3.] Si on a bien choisi les équations, alors cette étape va de soi. Sinon, il faudrait utiliser les bases de Gröbner.

[Étape 4.] On peut toujours décomposer $C$ car $\mathbb{Q}[X,Y]$ est un anneau factoriel. La fonction `Factorization` de MAGMA fait ce travail pour nous.

[Étape 5.] La fonction `Genus` de MAGMA calcule cet invariant.

[Étape 6.] Le code `with(algcurves) ; parametrisation(C(x,y),x,y,s) ;` de *Maple*9.5 calcule l'ensemble de solutions d'une conique.

[Étape 7.] La fonction `Generators` de MAGMA calcule un base du $\mathbb{Z} - module\ libre$ formé des points d'une courbe elliptique $\mathcal{C}$. Toutefois, elle peut se contenter de donner une base d'un sous-$\mathbb{Z}$-module de $\mathcal{C}$.

## 5.3 Liste des polynômes de division

On donne une liste des polynômes de division en coordonnées de *Montgomery*.

$\tilde{p}_2(x)=x\cdot(x^2+ax+1)$

$\tilde{p}_4^{new}=(x-1)\cdot(x+1)\cdot(x^4+2ax^3+6x^2+2ax+1)$

$\tilde{p}_8^{new}=(x^4-4x^3+(-4a-2)x^2-4x+1)\cdot(x^4+4x^3+(4a-2)x^2+4x+1)\cdot P_{reste}$

$\tilde{p}_3=x^4+\frac{4}{3}ax^3+2x^2-\frac{1}{3}$

$$\begin{aligned}\tilde{p}_5(x)=&5x^{12}+20ax^{11}+(16a^2+62)x^{10}+80ax^9-105x^8-360ax^7+\\&(-240a^2-300)x^6+(-64a^3-368a)x^5+(-160a^2-125)x^4-140ax^3-50x^2+1\end{aligned}$$

$$\begin{aligned}\tilde{p}_7(x)=&7x^{24}+56ax^{23}+(112a^2+308)x^{22}+(64a^3+944a)x^{21}+\\&(672a^2-2954)x^{20}-19656ax^{19}+(-47040a^2-19852)x^{18}+(-60928a^3-88256a)x^{17}+\\&(-48384a^4-179200a^2-35231)x^{16}+(-21504a^5-204288a^3-177296a)x^{15}+\\&(-4096a^6-120320a^4-348000a^2-82264)x^{14}+(-28672a^5-291200a^3-329952a)x^{13}+\\&(-89600a^4-407232a^2-111916)x^{12}+(-164864a^3-244944a)*x^{11}+(-111552a^2-42168)x^{10}+\\&(35840a^3+1344a)x^9+(8960a^4+80640a^2+15673)x^8+(1024a^5+25088a^3+59736a)x^7+\\&(3584a^4+25200a^2+14756)x^6+(4928a^3+10416a)x^5+(3360a^2+1302)x^4+1176ax^3+196x^2-1\end{aligned}$$

Dans le cas de la famille de *Suyama*, $\tilde{p}_3$ se simplifie pour devenir :

$$\frac{1}{3x_3^3}\cdot(x-x_3)\cdot(3x_3^3x^3-6x_3^2x^2+x^2+x_3x+x_3^2).$$

Ensuite on identifie les points de la courbe correspondant à chaque facteur des polynômes de division qui est irréductible au cas générique.

Polynôme $p_2$ et notation des points

| motif de factorisation | $(1,1)$ | $(2,1)$ |
|---|---|---|
| points correspondants | $R$ | $P,Q$ |

Polynôme $p_4^{new}$

| motif | $(2,1)$ | $(4,1)$ |
|---|---|---|
| points | $\frac{1}{2}R:=\{R_1,-R_1,R_2,-R_2\}$ | $\frac{1}{2}P\bigcup\frac{1}{2}Q$ |

Polynôme $p_8^{new}$

| motif | $(4,1)$ | $(4,1)$ | $(16,1)$ |
|---|---|---|---|
| points | $\frac{1}{2}R_1$ | $\frac{1}{2}R_2$ | $\frac{1}{2}(\frac{1}{2}P\bigcup\frac{1}{2}Q)$ |

Dans le cas de la paramétrisation de Suyama, $p_3$ a un motif de division spécial :

Polynôme $P_3$

| motif | $(1,1)$ | $(3,1)$ |
|---|---|---|
| points | $M_3, (-1)M_3$ | $E[3] - \{M_3, (-1)M_3\}$ |

## 5.4 Nouvelles équations

Voici une liste d'équations qui ont été essayées lors du stage.

d1 $a^2 - 4 = c^2$
On impose que $E[2]$ ait 4 points rationnels i.e. les points $P$ et $Q$ ci-dessus sont rationnels.
Le système $\{(1), (2), (3), (4), (d1)\}$ est une courbe de genre 7, donc une famille finie.

d2 $a - 2 = (-1)bc^2$
C'est une équation duale de celle qu'on utilise pour la famille *Suyama* 11.
Le système $\{(1), (2), (3), (4), (d2)\}$ est une courbe de genre 1, donc une courbe elliptique. Son rang vaut 1, donc on a une famille infinie. Il se trouve que chaque courbe de cette famille est isomorphe à une courbe de la famille *Suyama* 11.

d3 $a + 2 = bc^2$
On impose que le point $R_1$ ci-dessus soit rationnel.
Le système $\{(1), (2), (3), (d3)\}$ est une courbe de genre 1. Son rang vaut 0, donc elle est finie. Grâce à MAGMA on a la liste complète des valeurs de $\sigma$ : $\{-3, 5, -1, \frac{5}{3}\}$. Or toutes ces valeurs donnes des courbes singulières. Donc cette famille est vide.

d4 $a - 2 = bc^2$
On impose que le point $R_2$ ci-dessus soit rationnel.
On trouve une famille isomorphe courbe par courbe avec celle de $d3$.

d5 $\tilde{p}_5(x_5) = 0$
On impose un point de 5-torsion rationnel. Une telle courbe aurait 10 points de torsion sur $\mathbb{Q}$ et $20 \mid \#E/\mathbb{F}_p$ pour tout $p$ premier.
L'équation $d5$ seule est une courbe de genre 1. Comme elle possède le point $(x_5 = 2, a = -1)$, il s'agit d'une courbe elliptique. A l'aide de MAGMA on apprend que la courbe a rang 0, donc elle est fini. Finalement elle a 6 points, y compris $\mathcal{O}$ donc 5 ponts affine qui donnent chacun une courbe possiblement singulière.

d6 $\tilde{p}_7(x_7) = 0$
L'équation $d6$ seule donne une courbe de genre 4. On a donc une famille finie, voir vide. On retrouve le résultat grâce au théorème de Mazur. En effet les courbes de cette famille auraient un point d'ordre 14 sur $\mathbb{Q}$.

d7 $x_\infty = \frac{3x_3^2+1}{4x_3}$
Le système $\{(1), (2), (3), (d6), (d1)\}$ retrouve la famille *Montgomery* 12.

d8 $p_3(x_3^{deux}) = 0$
On impose une deuxième racine de $P_3$ sur $\mathbb{Q}$. Autrement dit, on impose que $E[3]$ ait 9 points rationnels.
Le système $\{(3), (d8)\}$ a comme solutions une courbe elliptique de rang 0. Tous ses points donnent des courbes singulières. On retrouve le résultat par le théorème de Mazur car aucun groupe de torsion possible ne peut contenir $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$.

d9 $(x_\infty^{deux})^3 + a(x_\infty^{deux})^2 + x_\infty^{deux} = c^2(x_3^3 + ax_3 + x_3)$
On impose à la courbe d'avoir rang $\geq 2$ sur $\mathbb{Q}$. En effet on peut espérer augmenter la probabilité que l'ordre soit $B_1 - friable$ en augmentant le rang sur $\mathbb{Q}$.
On trouve une famille infinie de solutions du système $\{(1), (2), (3), (4), (d8)\}$
On remarque expérimentalement que les courbes d'un rang plus grand se comportent de manière identique que les courbes d'un rang plus petit. Cela s'explique par le fait qu'on peut changer le rang sans changer les polynômes de division. Or seuls les polynômes de division déterminent la probabilité d'être $B_1 - friable$.

d10 $p_1(x_8) = 0$ et où $p_1$ est le facteur de $\tilde{p}_8^{new}$.
Le système $\{(d1), (d10)\}$ traduit que la courbe contient toute la $2 - torsion$ et un point de $8 - torsion$. On retrouve la famille des courbes à 16 points de torsion sur $\mathbb{Q}$, que l'on détaille dans la sous-section suivante.

## 5.5 Application : la famille *Montgomery* 16

Résolvons le système $\{(d1), (d10)\}$. On teste que si $x_8$ vérifie $(d10)$, alors l'équation $by_8^2 = x_8^3 + ax_8^2 + x_8$ admet une racine rationnelle $y_8$. Donc $\{(d1), (d10)\}$ caractérise les courbes sous forme de Montgomery avec 16 points de torsion sur $\mathbb{Q}$, notée $16T$. Dans [Mon92] il est montré que toute courbe avec 16 points de torsion sur $\mathbb{Q}$ se met sous forme de Montgomery. Les solutions du système sont : $\begin{cases} x_8 = \frac{1-t^2}{6+2t} \\ a = \frac{x_8^4 - 4x_8^3 - 2x_8^2 - 4x8 + 1}{4x8^2} \\ b = (x_8^2 - 1)^2 \end{cases} \quad t \in \mathbb{Q}$
Remarquons que cette paramétrisation $16T$ coïncide avec celle donnée dans [Mon92]. En effet, dans [Mon92], $16T$ est paramétrée par $\begin{cases} b = 1 \\ a = r^2 + \frac{1}{r^2} \end{cases}$ $r$ tel que $r^2 + 1 = k^2$ avec $k, r \in \mathbb{Q}$.
Pour passer d'une paramétrisation à l'autre on fait $y' = y(x_8^2 - 1)$ pour changer $b$. On retrouve les mêmes valeurs de $a$ par les deux paramétrisations grâce à

$$r = \frac{t^2 + 2t - 3}{4(t+1)}$$

$$\text{respectivement } x_8 = \frac{k^2 + r + k(r+1)}{r} \text{ où } k^2 = r^2 + 1.$$

Afin de trouver des sous-familles de $16T$ de rang positif, Montgomery prend dans [Mon92] un ensemble $F$ d'équations ad-hoc et résout le système $\{(d1), (d10), (f)\}$ pour chaque $f \in F$. La plupart de ces systèmes sont équivalents à des courbes de genre 1 et leur rang en tant que courbe elliptique est non nul. Ainsi, Montgomery donne une collection de familles infinies ayant 16 points de torsion et un autre point possiblement d'ordre infini. Kruppa a remarqué que le point $x_\infty$ peut être de torsion. Il faut donc vérifier, pour chaque courbe de *Montgomery* 16 que son $x_\infty$ n'annule pas $P_2 \cdot P_3 \cdot ... \cdot P_{16}$. Voir la discussion de 3.1.
Pour continuer les calculs, on préfère faire des notations en suivant [Mon92]. Ainsi une courbe générique à 16 points de torsion est du type $E : y^2 = x^3 + (\frac{\alpha^2}{\beta^2} + \frac{\beta^2}{\alpha^2})x^2 + x$ où $\alpha := 2\tau$ et $\beta := \tau^2 - 1$ avec $\tau \in \mathbb{Q}$. On prend l'équation $f : x_\infty = \frac{\alpha}{\beta}$ et on résout $\{(d1), (d10), (f), (3'')\}$ où $(3'')$ désigne $y_\infty^2 = x_\infty^3 + (\frac{\alpha^2}{\beta^2} + \frac{\beta^2}{\alpha^2})x_\infty^2 + x_\infty$.

En remplaçant $x_\infty$, $\alpha$ et $\beta$ en fonction de $\tau$, l'équation (3") devient $(\tau^2+2\tau-1)^2(\tau^2-1)^{-4}(\tau^4-2\tau^3+2\tau^2+2\tau+1) = y_\infty^2$. En englobant le carré à $y_\infty^2$ on trouve l'équation équivelante : $\tau^4-2\tau^3+2\tau^2+2\tau+1 = k^2$ où $k = (\tau^2-1)^2\frac{y_\infty}{\tau^2-2\tau-1}$. Il s'agit d'une courbe elliptique grâce à laquelle on calcule $\tau$ pour qu'ensuite on calcule toutes les autres inconnues.

Pour amener cette courbe sur une forme canonique on pose : $\begin{cases}\tau := \frac{w}{2u},\\ k := \frac{-2u^3+2u^2-2uw+u^2}{2u^2}.\end{cases}$

On trouve alors la courbe elliptique $F : w^2-2uw+6w = u^3-2u^2-3u$. MAGMA calcule les générateurs de $F$ : $P(-3,-6)$, $Q(1,-2)$ et $M(5,-6)$. En conclusion, on calcule $u$ et $v$ comme coordonnées d'un point $n_P*P+n_Q*Q+n_M*M$ sur $F$. On retrouve $\tau$ et $k$ grâce au formules plus haut. Finalement on remplace pour trouver $\alpha$, $\beta$ et $x_\infty$. Avec ces valeurs on peut lancer ECM.

Voici plus bas une implémentation possible :

```
function calcule_courbe_sur_M16(nP,nQ,nM)
   F:=EllipticCurve([-2,-2,6,-3,0]);//F courbe sur laquelle habitent les paramètres
   P:=F![-3,-6,1];  Q:=F![1,-2,1];  M:=F![5,-6,1];
   R:=nP*P+nQ*Q+nM*M;
   u:=R[1]; w:=R[2];
   tau:=w/(2*u);
   k:=(-2*u^3 + 2*u^2 - 2*u*w + w^2)/(2*u)^2;
   alpha:=2*tau;   beta:=tau^2-1;
   a:=alpha^2/beta^2+beta^2/alpha^2;    b:=1;
   A:=(3-a^2)/(3*b^2);    B:=(2*a^3/9-a)/(3*b^3);
   E:=EllipticCurve([A,B]);// courbe définie par (nP,nQ,nM)
   x_infty:=alpha/beta;// en coordonnees de Montgomery
// y_infty:=k*(tau^2+2*tau-1)/(tau^2-1)^2;
// Y:=b*y_infty;
// X:=(3*x_infty+a)/(3*b);// en coordonnees de Weierstrass
// P_infty:=E![X,Y,1];
   return a,b,x_infty;
end function;
```

On remarque que pour tout $n \in \mathbb{Z}$ les courbes définies par $(0,0,n)$, $(1,0,n)$, $(0,1,n)$ et $(1,1,n)$ ont le même $j$-invariant, donc sont isomorphes. On utilise alors seulement la branche $\{(0,0,n)/n \in \mathbb{Z}\}$.

Un autre problème est de s'assurer que le point $P_\infty(X_\infty, Y_\infty)$ qu'on ajoute sur la courbe est effectivement d'ordre infini. Des expérimentations montre que $ordre(P_\infty) = \infty$ pour $(nP, nQ, nM) \in \{(0,0,n)/1 \leq n \leq 128\}$. Toutefois, si on estime que le cas où $ordre(P_\infty) < \infty$ est trop fréquent, alors on peut tester que $P_\infty$ n'est pas de torsion avant de lancer ECM. D'après le théorème de Mazur, une courbe ne peut pas avoir plus de 16 points de torsion sur $\mathbb{Q}$. Or les courbes de la familles *Montgomery* 16 en ont déjà 16. Pour que le point en plus soit de torsion il faut qu'il coïncide avec un des points de torsion, donc que son ordre divise 8. Il suffit donc de tester si $8 * P_\infty = \mathcal{O}$.

# 6 Vers une estimation précise de la valuation

## 6.1 Théorème de Chebotarëv

On ne dispose pas de formule capable de donner pour une courbe $E(a,b)$ la valuation moyenne en un premier $\pi$. Par contre on va l'estimer à l'aide de l'hypothèse que $E$ est une courbe générique d'une certaine famille.

Dans cette section on va utiliser la théorie de la mesure pour donner un sens à la *valuation moyenne*. On munit donc l'ensemble des premiers d'une tribu et d'une mesure.

**Définition 11.** *Soit $S$ un ensemble de nombres premiers. On dit que $S$ a une densité $\delta$ si*

$$\frac{\#\{p \leq x; p \in S\}}{\#\{p \leq x; p \text{ premier}\}} \to \delta \text{ pour } x \to \infty.$$

**Définition 12.** *On note $\mathcal{P}$ l'ensemble des premiers. On dit qu'une partie $S$ de $\mathcal{P}$ est $\mu$* mesurable *si et seulement si elle a une densité. Dans ce cas on pose $\mu(S)$ égale à la densité de $S$.*

**Remarque 15.** *On a $\mu(\mathcal{P}) = 1$, donc $\mu$ est une mesure de probabilités. De plus pour tout $F \subset \mathcal{P}$ fini on a $\mu(F) = 0$.*

Voyons maintenant comment peut se décomposer un polynôme $f \in \mathbb{Q}[X]$ quand on le plonge dans $\mathbb{F}_p$.

**Définition 13.** *Soit $f = a_n X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Q}[X]$ et $d = dnominateur(a_0 \cdot a_1 \cdot ... \cdot a_n)$ et $p$ un nombre premier tel que $p \nmid \Delta(f) \cdot d$. Alors on dit que $f$ se réduit modulo $p$.*

**Notation 4.** *Soit $f \in \mathbb{Q}[X]$ et $p$ premier tel que $f$ se réduit modulo $p$.*

1. *On note $\alpha_1, ..., \alpha_n$ ses racines complexes et $Dec(f) = \mathbb{Q}(\alpha_1, ..., \alpha_n)$ son corps de décomposition.*
2. *On note $G = Gal(Dec(f)/\mathbb{Q})$.*
3. *Soit $p \cdot \mathcal{O}_{Dec(f)} = \mathfrak{p}_1 ... \mathfrak{p}_k$ la décomposition en idéaux premiers de $p$ dans $Dec(f)$. Comme $f$ se réduit modulo $p$, il existe exactement un $\tau_i \in G$ pour chaque $\mathfrak{p}_i$ tel que $\forall x \in Dec(f). x^p - \tau_i(x) \in \mathfrak{p}_i$. On appelle* Frobenius de $f$ sur $p$ *l'ensemble $Frob(p) := \{\tau_1, ..., \tau_k\}$.*

**Remarque 16.** *Les éléments de $\{\tau|_{\{\alpha_1,...,\alpha_n\}} \mid \tau \in Frob(p)\}$ se décomposent en cycles de la même manière. Pour cela on pose pour tout $\tau \in G$, $\tilde{\tau} = \tau|_{\{\alpha_1,...,\alpha_n\}}$. Soient $\tau$ et $\tau'$ dans $Frob(p)$. On peut vérifier que $Frob(p)$ est une classe de conjugaison de $G$, donc il existe $g \in G$ tel que $\tau' = g\tau g^{-1}$. Par conséquent, $\tilde{\tau'} = \tilde{g}\tilde{\tau}\tilde{g}^{-1}$. Donc les permutations $\tilde{\tau}$ et $\tilde{\tau'}$ sont conjuguées. Ainsi elles ont le même motif de décomposition en cycles disjoints.*

**Définition 14.** *Soit $p$ comme dans la notation précédente et $Frob(p)$ définit plus haut. On appelle* motif de cycles de $f$ sur $p$ *le motif commun de décomposition en cycles des éléments de $Frob(p)$.*

**Théorème 6.** *Soit $f \in \mathbb{Q}[X]$ et $p$ premier tel que $f$ se réduit modulo $p$. Alors les trois quantités suivantes sont égales :*

*(i) le motif de décomposition en cycles de $f$ sur $p$ ;*

*(ii) le motif des cycles de $fr|_{\{racines\ de\ f\}}$ où $fr : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$, $x \mapsto x^p$ ;*

*(iii) le motif de factorisation de $f$ sur $p$.*

*Démonstration.* $(i) = (ii)$ Comme $p \nmid \Delta(f)$, $f$ a des racines simples sur $\mathbb{Q}$ et sur $\mathbb{F}_p$. Soit $\mathfrak{p}$ un idéal au-dessus de $p$ et $\tau \in G$ son automorphisme associé comme plus haut. Soit $k$ le degré d'inertie de $\mathfrak{p}$. On définit $\psi_\tau : Dec(f) \to \overline{\mathbb{F}_p}$, $x \mapsto x + \mathfrak{p} \in Dec(f)/\mathfrak{p} = F_{p^k} \subset \overline{\mathbb{F}_p}$. On a alors $fr \circ \psi_\tau = \psi_\tau \circ \tau$.

Soit $\alpha_i$ une racine complexes de $f$. Comme $\psi_\tau$ est un homomorphisme d'anneaux et $f$ est un polynôme, $f(\psi_\tau(\alpha_i)) = \psi_\tau(f(\alpha_i)) = 0$. Donc $\psi_\tau(\alpha_i)$ est racine de $f$. Comme $\#\{\psi_\tau(\alpha_i)/1 \leq i \leq n\} = n = deg(f)$, ce sont toutes les racines de $f$ dans $\overline{\mathbb{F}_p}$.
On note $\sigma \in \mathcal{S}_n$ l'action de $fr$ sur les indices des racines de $f$ dans $\overline{\mathbb{F}_p}$ i.e. $\{\psi_\tau(\alpha_i)/1 \leq i \leq n\}$ : $fr(\psi_\tau(\alpha_i)) = \psi_\tau(\alpha_{\sigma(i)})$. De même on note $\sigma' \in \mathcal{S}_n$ l'action de $\tau$ sur les indices des racines de $f$ dans $\mathbb{C}$ : $\tau(\alpha_i) = \alpha_{\sigma'(i)}$. On a alors $\psi_\tau(\alpha_{\sigma'(i)}) = \psi_\tau(\tau(\alpha_i)) = fr(\psi_\tau(\alpha_i)) = \psi_\tau(\alpha_{\sigma(i)})$. Comme $\psi_\tau|_{\{\text{racines de } f\}}$ est injectif et les racines sont distinctes, $\sigma(i) = \sigma'(i)$. Donc $\sigma = \sigma'$.

$(ii) = (iii)$ Soit $\mathcal{O}$ le support d'un cycle de $fr$. On note $a_i = \psi_\tau(\alpha_i)$ et $A = \{a_i/1 \leq i \leq n\}$. Comme $H := Gal(\mathbb{F}_p(A)/\mathbb{F}_p)$ est engendré par $fr$, $\mathcal{O}$ est une orbite de $h|_A$ pour tout $h \in H$. Alors $f_\mathcal{O} := \Pi_{\beta \in \mathcal{O}}(X - \beta)$ est stable par $H$, donc $f_\mathcal{O} \in \mathbb{F}_p[X]$. Comme $f$ et $\Pi_{orbites} f_\mathcal{O}$ ont les mêmes racines avec les mêmes multiplicités, $f = \Pi_{orbites} f_\mathcal{O}$.
Supposons par l'absurde que $f_\mathcal{O}$ n'est pas irréductible. Alors $f = gh$ pour certains $g, h \in \mathbb{F}_p[X]$. On note $\mathcal{O}_g$ et $\mathcal{O}_h$ les ensembles respectifs de racines. Comme $g \in \mathbb{F}_p[X]$, $\mathcal{O}_g$ est stable par tout automorphisme de $\overline{\mathbb{F}_p}$, en particulier par $H$. Or $fr$ agit transitivement sur ses orbites, donc $\mathcal{O}_g$ est une orbite de $fr$. Or $\mathcal{O}_g = \{\text{racines de } g\} \subset \{\text{racines de } f_\mathcal{O}\} = \mathcal{O}$, donc $\mathcal{O}_g = \mathcal{O}$. Ainsi $deg(h) = 0$, soit $f_\mathcal{O}$ est irréductible. Ainsi le motif de factorisation de $f$ sur $p$ est égal à $\{(\#\mathcal{O}, 1)/\mathcal{O} \text{ orbite de } fr\}$ i.e. motif de cycles de $fr$.

□

**Théorème 7.** *(de Chebotarëv) Soit $f$ un polynôme unitaire de $\mathbb{Z}[X]$, de degré $n$, pas forcément irréductible. Soit $C$ une classe de conjugaison de $Gal(Dec(f)/\mathbb{Q})$. Alors $E_C = \{p \text{ premier}/Frob(p) = C\}$ a une densité et elle vaut $\frac{\#C}{\#Gal(f,\mathbb{Q})}$.*

*Démonstration.* Lire [SL06]. □

**Remarque 17.** *Le résultat reste vrai pour $f \in \mathbb{Q}[X]$.*

*Justification* Soit $f \in \mathbb{Q}[X]$, $f = \frac{a_n}{b_n}x^n + ... + \frac{a_0}{b_0}$. On pose $\lambda = ppcm\{b_0, ..., b_n\}$ et $f_1 := \lambda f$. Ensuite on pose $f_2(x) = \lambda^{n-1} f_1(\frac{x}{\lambda})$. On constate que $f_2 \in \mathbb{Z}[X]$ et qu'il est unitaire. Ainsi le théorème 7 s'applique à $f_2$. Or $f_2$ et $f$ ont le même groupe de Galois sur $\mathbb{Q}$ et pour les premier $p$ où ils se réduisent, ils donnent le même motif de factorisation. Finalement, $f_2$ se réduit pour tous les premiers car unitaire et entier, alors que $f$ se réduit pour tous sauf les diviseurs de $\lambda$, donc un ensemble fini, qui ne change pas les proportions.□

**Corollaire 2.** *Soient $p$ un premier et $f \in \mathbb{Q}[X]$ qui se réduit modulo $p$ et qui vérifie : $\frac{\mathbb{Q}[X]}{<f(X)>} \simeq Dec(f, \mathbb{Q})$. Alors $\delta\{p \mid f \text{ a une racine sur } \mathbb{F}_p\} = \delta\{p \mid f \text{ est scindé sur } \mathbb{F}_p\}$.*

*Démonstration.* D'après le théorème 7 il suffit de montrer qu'il n'existe pas de $\tau \in Gal(f, \mathbb{Q})$ qui fixe une racine de $f$ sans les fixer toutes. Supposons qu'il existe $\tau \in Gal(Dec(f), \mathbb{Q})$ et $\alpha \in \overline{\mathbb{Q}}$ tels que $f(\alpha) = 0$ et $\tau(\alpha) = \alpha$. Alors $\frac{\mathbb{Q}[X]}{<f(X)>} \simeq \mathbb{Q}(\alpha)$, d'où $\mathbb{Q}(\alpha) \simeq Dec(f)$. Or $\mathbb{Q}(\alpha) \subset Dec(f)$, donc $\mathbb{Q}(\alpha) = Dec(f)$. Comme $\tau(\alpha) = \alpha$, $\tau = id$. Donc $\tau$ fixe toutes les racines de $f$. □

**Corollaire 3.** *Soit $f \in \mathbb{Q}[X]$, $G$ son groupe de Galois sur $\mathbb{Q}$. Soient $C$ une classe de conjugaison de $G$ et $\mathcal{F}$ une propriété i.e. un sous ensemble de $G$, stable par conjugaison. Soit $p$ une variable aléatoire par rapport à $\mu$. Alors :*

1. $Prob(Frob(p) = C) = \frac{\#C}{\#G}$ ;
2. $Prob(Frob(p) \subset \mathcal{F}) = \frac{\#\mathcal{F}}{\#G}$.

*Démonstration.* 1. On a $Prob(Frob(p) = C) = Prob(p \in E_C) = \mu(E_C)$. D'après le théorème 7 $\mu(E_C) = \frac{\#C}{\#G}$.

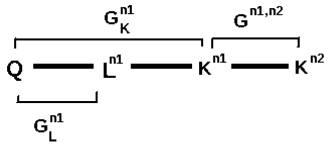
2. Comme $\mathcal{F}$ est stable par conjugaison, elle est la réunion disjointe de classes de conjugaison de $G$ : $\mathcal{F} = C_1 \bigcup ... \bigcup C_k$. On a alors $Prob(Frob(p) \subset \mathcal{F}) = \Sigma_{1 \leq i \leq k} Prob(Frob(p) = C_i) = \Sigma_{1 \leq i \leq k} \frac{\#C_i}{\#G} = \frac{\#\mathcal{F}}{\#G}$.

□

**Définition 15.** *Soient $E/\mathbb{Q}$ une courbe elliptique, $\pi$ un premier et $1 \leq n_1 < n_2$ dans $\mathbb{N}$. On note :*

1. $q_{n_1} = Prob(\frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \subset E/\mathbb{F}_p)$ ;
2. $p_{n_1,n_2} = Prob(\frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_2}\mathbb{Z}} \subset E/\mathbb{F}_p | \frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \subset E/\mathbb{F}_p)$ ;
3. $L^{n_1} = Dec(P^{new}_{\pi^{n_1}})$ ;
4. $G^{n_1}_L := Gal(L^{n_1}, \mathbb{Q})$ ;
5. $K^{n_1} := \mathbb{Q}(E[\pi^{n_1}])$ ; $K^{n_2} := \mathbb{Q}(E[\pi^{n_2}])$
6. $G^{n_1}_K := Gal(K^{n_1}/\mathbb{Q})$ ;
7. $G^{n_1,n_2} := Gal(K^{n_2}/K^{n_1}) = G^{n_2}_K / G^{n_1}_K$.
8. $s_{n_1,n_2} := \#\{\tau \in G^{n_1,n_2} / \tau$ *fixe un point de* $E[\pi^{n_2}] \setminus E[\pi^{n_2-1}]\}$.

*Justification.* $L^{n_1}/\mathbb{Q}$ est galoisienne car $L^{n_1}$ est un corps de décomposition. De plus $K^{n_1}$ s'obtient de $L^{n_1}$ par des extentions successives par les polynômes de $\{p_\alpha := X^2 - \frac{1}{b}(\alpha^3 + A\alpha + B)/\alpha$ racinde de $P_{\pi^{n_1}}\}$. Comme toute extention de corps de nombres, de degré 1 et 2 est galoisienne et comme une tour d'extensions galoisiennes est galoisienne, $K^{n_1}/\mathbb{Q}$ est galoisienne. De manière analogue $K^{n_2}/\mathbb{Q}$ est galoisienne, d'où $K^{n_2}/K^{n_1}$ est galoisienne.




**Proposition 3.** *Soit $n_1 \in \mathbb{N}$. Alors $q_{n_1} = \frac{1}{\#G^{n_1}_K}$.*

*Démonstration.* Par le théorème de l'élément primitif, il existe un polynôme irréductible $f \in \mathbb{Q}[X]$ tel que $K^{n_1} = \frac{\mathbb{Q}[X]}{<f(X)>}$. Comme $K^{n_1}/\mathbb{Q}$ est galoisienne, $\frac{\mathbb{Q}[X]}{<f(X)>} = Dec(f)$. Ainsi $G^{n_1}_K = Gal(f, \mathbb{Q})$.

On admet pour l'instant que $\mathbb{F}_p(E(\overline{\mathbb{F}_p})[\pi^{n_1}]) = \mathbb{F}_p$ exactement pour les $p$ pour lesquels $Dec(f, \mathbb{F}_p) = \mathbb{F}_p$. On a $\frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \subset E/\mathbb{F}_p$ exactement pour ces $p$ pour lesquels on a $\pi^{2n_1}$ points de $E(\overline{\mathbb{F}_p})[\pi^{n_1}]$ à coefficients dans $\mathbb{F}_p$. Or $E(\overline{\mathbb{F}_p})[\pi^{n_1}]$ contient $\pi^{2n_1}$ points en tout, donc exactement quand $\mathbb{F}_p(E(\overline{\mathbb{F}_p})[\pi^{n_1}]) = \mathbb{F}_p$. Grâce au fait qu'on a admis et on démontre par la suite, cela arrive exactement quand $Dec(f, \mathbb{F}_p) = \mathbb{F}_p$. Or $Dec(f, \mathbb{F}_p) = \mathbb{F}_p$ arrive ecxactement pour les $p$ pour lesquels $fr$ fixe toute racine de $f$, soit $Frob(p) = \{id\}$. Ainsi $q_{n_1} = Prob(Frob(p) = \{id\})$. Par le corollaire 3 on a $q_{n_1} = \frac{1}{\#Gal(f)} = \frac{1}{\#G_K^{n_1}}$.

Montrons maintenant que $\mathbb{F}_p(E(\overline{\mathbb{F}_p})[\pi^{n_1}]) = \mathbb{F}_p$ si et seullement si $Dec(f, \mathbb{F}_p) = \mathbb{F}_p$. Pour cela notons $\alpha_1, ..., \alpha_m$ les racines dans $\overline{\mathbb{Q}}$ de $f$. On remarque que $Dec(f) \supset \mathbb{Q}(\alpha_1) \simeq \frac{\mathbb{Q}[X]}{<f(X)>} \simeq Dec(f)$, donc $K^{n_1} = Dec(f) = \mathbb{Q}(\alpha_1)$. Notons $(x_i, ..., x_n)$ les racines dans $\overline{\mathbb{Q}}$ de $P_{\pi^{n_1}}$. Notons $y_1, ..., y_n$ les racines dans $\overline{\mathbb{Q}}$ de $\{p_\alpha := X^2 - \frac{1}{b}(\alpha^3 + A\alpha + B)/\alpha$ racine de $P_{\pi^{n_1}}\}$. D'après le théorème 5 on a $E[\pi^n] = \{\mathcal{O}\} \bigcup \{(x_i, \pm y_i)/1 \leq i \leq n\}$, donc $K^{n_1} = \mathbb{Q}(x_1, ..., x_n, y_1, ..., y_n)$. Comme $\mathbb{Q}(\alpha_1) = K^{n_1} = \mathbb{Q}(x_1, ..., x_n, y_1, ..., y_n)$, il existe des polynômes $P_{x_i}$ et $P_{y_i} \in \mathbb{Q}[X]$ respectivement $P_{\alpha_1} \in \mathbb{Q}[X_1, ..., X_n, Y_1, ..., Y_n]$ tels que $P_{x_i}(\alpha_1) = x_i$, $P_{y_i}(\alpha_1) = y_i$ et $P_{\alpha_1}(x_1, ..., x_n, y_1, ..., y_n) = \alpha_1$. Mis à part un nombre fini de premiers $p$, tous ces polynômes se réduisent *modulo* $p$. Or les ensembles finis n'interviennent pas dans le calcul des probabilités, donc on peut supposer que les polynômes se réduisent *modulo* tous les nombres premiers.

On remarque que dans $\mathbb{Q}(\alpha_1)[X]$ on a $\Pi_{i=1}^n (X - P_{x_i}(\alpha_1)) = P_{\pi^{n_1}}(X)$. Ainsi il existe $k \in \mathbb{Q}[X, T]$ tel que dans $\mathbb{Q}[X, T]$ on a

$$\Pi_{i=1}^n (X - P_{x_i}(T)) = P_{\pi^{n_1}}(X) + f(T) \cdot k(X, T)$$

et de manière analogue on a $P_{y_i}^2(T) - (P_{x_i}^3(T) + AP_{x_i}(T) + B) = f(T)k_i(X, T)$ pour tout $i$ et un certain $k_i$.

Soit $p$ premier tel que $Dec(f, \mathbb{F}_p) = \mathbb{F}_p$. Alors il existe $\tilde{\alpha_1} \in \mathbb{F}_p$ tel que $f(\tilde{\alpha_1}) = 0$. Dans l'identité plus haut on pose $T = \tilde{\alpha_1} \in \mathbb{F}_p$ et on plonge les coefficients modulo $p$. Alors on remarque que $P_{\pi^{n_1}}(X)$ est scindé modulo $p$. De plus $x_i^3 + Ax_i + B$ est un carré de $\mathbb{F}_p$ pour tout $i$. D'après le théorème 5, tout point de $E(\overline{\mathbb{F}_p})[\pi^{n_1}]$ a ses coordonnées dans $\mathbb{F}_p$. Donc $\mathbb{F}_p(E(\overline{\mathbb{F}_p})[\pi^{n_1}]) = \mathbb{F}_p$.

Réciproquement, soit $p$ tel que $P_{\pi^{n_1}}$ soit scindé sur $\mathbb{F}_p$ et il existe $y_i \in \mathbb{F}_p$ tel que $y_i^2 = x_i^3 + Ax_i + B$. On pose $\tilde{\alpha_1} := P_{\alpha_1}(x_1, ..., x_n, y_1, ..., y_n) \in \mathbb{F}_p$ et on vérifie que $f(\tilde{\alpha_1}) = 0$. D'après le corollaire 2, $f$ a toutes ses racines dans $\mathbb{F}_p$. Donc $Dec(f, \mathbb{F}_p) = \mathbb{F}_p$.

□

**Proposition 4.** *Soient $n_1 < n_2 \in \mathbb{N}$. Alors $p_{n_1,n_2} = \frac{s_{n_1,n_2}}{\#G^{n_1,n_2}}$.*

*Démonstration.* :

On a $Prob(\frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_2}\mathbb{Z}} \subset E/\mathbb{F}_p) = \frac{\#\{\tau \in G_K^{n_2} / \tau \text{ fixe un point de } E[\pi^{n_2}] \setminus E[\pi^{n_2-1}] \text{ et tous les points de } K^{n_1}\}}{\#G_K^{n_2}}$.
De même on a $Prob(\frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^{n_1}\mathbb{Z}} \subset E/\mathbb{F}_p) = \frac{\#\{\tau \in G_K^{n_2} / \tau \text{ fixe } K^{n_1}\}}{\#G_K^{n_2}}$.
Ainsi $p_{n_1,n_2} = \frac{\#\{\tau \in G_K^{n_2} / \tau \text{ fixe un point de } E[\pi^{n_2}] \setminus E[\pi^{n_2-1}] \text{ et tous les points de } K^{n_1}\}}{\#\{\tau \in G_K^{n_2} / \tau \text{ fixe } K^{n_1}\}}$.
D'une part, on a $\#\{\tau \in G_K^{n_2} / \tau \text{ fixe } K^{n_1}\} = \#Gal(K^{n_2}/K^{n_1}) = \#G^{n_1,n_2}$.
D'autre part, $\#\{\tau \in G_K^{n_2} / \tau$ fixe un point de $E[\pi^{n_2}] \setminus E[\pi^{n_2-1}]$ et tous les points de $K^{n_1}\} =$
$= \#\{\tau_1 \circ h / \tau_1 \in G_K^{n_1}, h \in G^{n_1,n_2}$ tels que $\tau_1 \circ h$ fixe un point de $E[\pi^{n_2}] \setminus E[\pi^{n_2-1}]$ et fixe $K^{n_1}\} =$
$= \#\{h \in G^{n_1,n_2} / h$ fixe un point de $E[\pi^{n_2}] \setminus E[\pi^{n_2-1}]\} = s_{n_1,n_2}$.
En conclusion $p_{n_1,n_2} = \frac{s_{n_1,n_2}}{\#G^{n_1,n_2}}$. □

## 6.2 Applications

Kruppa a remarqué un comportement étrange de la courbe de *Suyama* correspondant à $\sigma = 10$. D'une part $\sigma = 10$ est une courbe quelconque de la famille de *Suyama* car ses valuations moyennes en 2 et en 3 ne sont pas spéciales. D'autre part, $\sigma = 10$ a une propriété rare, présente chez les $\sigma' s$ de la famille *Suyama* 11 : le polynôme de 12 division est scindé *modulo p* pour une grande proportion de premiers $p$. Grâce à la théorie qui précède on va éclairer cette apparante contradiction.

À l'aide de MAGMA on peut calculer le groupe de Galois d'une extension galoisienne de $\mathbb{Q}$. Le tableau ci-dessous regroupe les informations pour trois courbes de la famille de *Suyama*. On précise que les notations sont celles de plus haut et que $\pi = 2$. On a également noté $Gal(P_{12})$ le polynôme de l'extension de $\mathbb{Q}$ qui contient toutes les racines de $P_{12}$, malgré le fait que $P_{12}$ ne soit pas irréductible. Finalement, $E(12)$ se comporte toujours comme la plupart des courbes de *Suyama*, donc on l'a pris comme représentant des courbes génériques.

| $\sigma$ | 10 | 11 | 12 |
|---|---|---|---|
| $G_L^1 = G_K^1$ | $\frac{\mathbb{Z}}{2\mathbb{Z}}$ | $\frac{\mathbb{Z}}{2\mathbb{Z}}$ | $\frac{\mathbb{Z}}{2\mathbb{Z}}$ |
| $G_L^2$ | $D_8$ | $D_8$ | $D_8$ |
| $G_K^2$ | $D_8 \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ | $D_8 \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ | $D_8 \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ |
| $G^{1,2}$ | $D_8 \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ | $D_8$ | $D_8 \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ |
| $\#Gal(P_{12})$ | 48 | 48 | 96 |

On remarque que $G_K^1 \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$. Par la proposition 3 on a $q_1 = \frac{1}{2}$ pour $E(10)$, $E(11)$ et $E(12)$. Des expériences sur 1000 nombres premiers ont montré : $q_1(\sigma = 10) = \frac{502}{1000}$, $q_1(\sigma = 11) = \frac{509}{1000}$ et $q_1(\sigma = 12) = \frac{511}{1000}$.

On voit que $G_L^2$ est isomorphe au groupe diédral à 8 éléments pour les trois courbes. Par le théorème 7 on peut calculer la proportion de nombres premiers pour lequel $P_4$ a chacun des motifs de factorisation possible. En tout cas, comme les $G_L^2$ respectifs coïncident, les proportions coïncident également pour les trois courbes.

On constate que $G^{1,2}$ a la même valeur pour $E(10)$ et $E(12)$ mais pas pour $E(11)$. Comme $p_{1,2}$ se calcule à partir de $G^{1,2}$, $E(10)$ et $E(12)$ ont le même $p_{1,2}$. Par contre $E(11)$ a un groupe $G^{1,2}$ différent, donc possiblement une probabilité différente. Expérimentalement on a $p_{1,2}(\sigma = 10) = \frac{365}{502} \approx 73\%$, $p_{1,2}(\sigma = 11) = \frac{509}{509} = 100\%$ et $p_{1,2}(\sigma = 12) = \frac{389}{511} \approx 76\%$. Si on répète l'expérience on se rapproche de 75% pour le cas général.

Comme $E(\sigma = 10)$ et $E(\sigma = 11)$ ont exactement les mêmes $Gal(P_{12})$, les polynômes $P_{12}$ respectifs ont les même motifs de factorisation avec les mêmes fréquences.

**Conclusion** : Il ne suffit pas de regarder $Gal(P_m)$ pour étudier $E[m]$, mais il faut regarder $Gal(E[m]/\mathbb{Q})$. Dans le cas particulier de $m = 12$ et $E = E(\sigma = 10)$ on a un $Gal(P_{12})$ spécial sans pour autant changer $Gal(E[m]/\mathbb{Q})$. Donc $\sigma = 10$ "aime" avoir les points de $E[12]$ avec leur coordonnée $x$ dans $\mathbb{F}_p$, sans imposer rien sur la coordonnée $y$.

On remarque entre autres que le fait que le groupe $Gal(P_{12})$ soit plus simple se manif este aussi dans le motif de factorisation de $P_{12}$ sur $\mathbb{Q}$. Ainsi, pour une courbe quelconque de Suyama, le motif de factorisation sur $\mathbb{Q}$ est $\{(1,5),(2,4),(3,2),(4,1),(6,3),(8,1),(24,1)\}$. Par contre pour $\sigma = 10$ un facteur de degré 6 qui est irréductible dans le cas générique se décompose en deux facteurs de degré 3. De même pour $\sigma = 11$ l'unique facteur de degré 8 se décompose en deux facteurs de degré 4. En effet, ce facteur de degré 8 correspond au points de 3 division d'une paire de points de 4-torsion de la courbe $E(11)$. Comme $G_K^2$ est spécial pour $\sigma = 11$, les racines correspondant aux deux points de

4-torsion se séparent, donnant deux facteurs de degré 4. Par contre le fait que le facteur de degré 6 devienne réductible pour $\sigma = 10$ semble ne pas prevenir de la structure de $E[3]$ et $E[4]$.

## 6.3 Ouverture

**Proposition 5.** *Soit $p$ un premier et $E : y^2 = x^3 + Ax + B$ une courbe elliptique sur $\mathbb{Q}$ qui se réduit modulo $p$. Soient $n \geq 1$ et $\pi$ un premier autre que $p$. On munit $E[\pi^n]$ de la structure de groupe induite par $E$. Alors $G_K^n$ est un sous groupe de $Aut_{groupe}(E[\pi^n])$.*

*Démonstration.* Soit $\tau \in G_K^n = Aut_{corps}(\mathbb{Q}(E[\pi^n]))$. Montrons que $\tau|_{E[\pi^n]} \in Aut_{groupe}(E[\pi^n])$. On sait que $\tau$ s'étend à $\tilde{\tau} \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Comme $\tilde{\tau}(A) = A$ et $\tilde{\tau}(B) = B$, on a $\tilde{\tau}(E) = E$. Comme les formules de la loi de groupe de $E$ sont polynomiales, $\tilde{\tau}|_E$ est un morphisme de groupes. Ainsi $\tilde{\tau}|_E$ est un endomorphisme du groupe $E$. Comme $E[\pi^n] = \{x \in E/ordre(x) \mid \pi^n\}$, alors $\tau|_{E[\pi^n]} = \tilde{\tau}|_{E[\pi^n]}$ stabilise $E[\pi^n]$, donc $\tau|_{E[\pi^n]} \in End(E[\pi^n])$. Comme $\tau$ est un automorphisme de corps, il est injectif et alors $\tau_{E[\pi^n]}$ est injectif. Comme $E[\pi^n] \simeq \frac{\mathbb{Z}}{\pi^n\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^n\mathbb{Z}}\pi^{2n}$, il est fini, donc $\tau|_{E[\pi^n]}$ est bijectif. Ainsi $\tau|_{E[\pi^n]} \in Aut(E[\pi^n])$.

Finalement, pour voir que $\tau \mapsto \tau|_{E[\pi^n]}$ est un morphisme injectif de groupes, il suffit de remarquer que l'image de $\tau$ sur $\mathbb{Q}(E[\pi^n])$ est déterminer par $\tau|_{E[\pi^n]}$ et que $(\tau_1 \circ \tau_2)|_{E[\pi^n]} = (\tau_1|_{E[\pi^n]}) \circ (\tau_2|_{E[\pi^n]})$.

□

**Remarque 18.** *L'inclusion de la proposition 5 est une égalité dans le cas générique. Par exemple pour $\pi = 5$ et un $\sigma$ choisi au hasard, disons 13, on a $\#G_K^1 = 480$ et $\#Aut(E[5]) = 480$. Comme $G_k^1$ est un sous groupe de $Aut(E[5])$, on a $G_K^1 \simeq Aut(E[5])$.*

Jean-Pierre Serre a démontré dans [Ser72] le théorème suivant :

**Théorème 8.** *Soit $E/\mathbb{Q}$ une courbe elliptique. Alors il existe un ensemble fini $F \subset \mathcal{P}$ tel que pour tout $\pi \in \mathcal{P} \setminus F$ on a $G_K^1(\pi) = Aut(E[\pi])$.*

On remarque qu'il est relativement simple d'étudier le groupe $Aut(E[\pi^k])$. En effet le théorème 3 dit que $E[\pi^k] \simeq \frac{\mathbb{Z}}{\pi^k\mathbb{Z}} \times \frac{\mathbb{Z}}{\pi^k\mathbb{Z}}$, donc $Aut(E[\pi^k]) = Aut(R \times R)$ pour $R = \frac{\mathbb{Z}}{\pi^k\mathbb{Z}}$.

**Proposition 6.** *Soit $n \in \mathbb{N}$. On note $R := \frac{\mathbb{Z}}{\pi^n\mathbb{Z}}$, $r := \#R = \pi^n$ et $r' := \#R^* = \pi^n - \pi^{n-1}$. Alors on a :*

*(i)* $\#Aut(R \times R) = (2r - r')r'^2(2r - r' - 1)$ ;

*(ii)* $\#\{a \in Aut(R \times R) - \{id\}/ker(a - id) \neq 0\} = (2r - r')(2r \cdot r' - r'^2 - r' - 1)$ ;

*(iii) seule id fixe plus d'une droite.*

*Démonstration.* (i) On note $\{e_1, e_2\}$ la base canonique de $R \times R$. Un automorphisme est déterminé de façon unique par le choix des images $f_1$ respectivement $f_2$ des éléments de la base. Pour $f_1$ on peut choisir tout élément d'ordre $r$, soit tout élément de $R \times R^* \bigcup R^* \times R$. En tout $r \cdot r' + r' \cdot r - r' \cdot r' = r'(2r - r')$ choix. Pour $f_2$ on peut choisir tout élément d'ordre $r$ sauf ceux de $R^* f_1$. En tout, $r'(2r - r') - r' = r'(2r - r' - 1)$. Ainsi on a $(2r - r')r'^2(2r - r' - 1)$ choix de $(f_1, f_2)$ donc d'automorphismes.

(ii) On choisit un élément $a \cdot e_1 + b \cdot e_2$ d'ordre $r$. En tout $(2r - r')r'$ choix.
On choisit l'image de $b \cdot e_1 + a \cdot e_2$ comme un point d'ordre $r$, qui n'est pas sur $\mathbb{Z}e_1$ et qui n'est

pas $b \cdot e_1 + a \cdot e_2$. En tout $(2r - r')r' - r' - 1$ choix. On divise le résultat par $r'$ car on a compté le même automorphisme pour tous les éléments d'ordre $r$ de la droite fixée : $R \cdot (a \cdot e_1 + b \cdot e_2)$. Conclusion : $(2r - r')r'(2r \cdot r' - r'^2 - r' - 1)/r' = (2r - r')(2r \cdot r' - r'^2 - r' - 1)$.

(iii) Rien à montrer.

□

**Corollaire 4.** *Pour $E$ et $n_1 \in \mathbb{N}$ génériques on a $q_{n_1} = \frac{1}{\pi^{4n_1}(\pi-1)^2\pi(\pi+1-\frac{1}{\pi^{n_1-1}})}$.*

*Démonstration.* C'est la conséquence directe de la proposition 3, du théorème 8 et de la proposition ci-dessus. □

**Projet.** Pour finir on fixe une courbe elliptique $E$ et propose la démarche suivante :

1. On suppose le théorème 8 vrai pour tout $\pi$ premier tel que $B_1 + 1 \leq \pi \leq p$ où $B_2$ et $p$ sont deux entiers.
2. On calcule pour chaque $\pi$, $Prob(\frac{\mathbb{Z}}{\pi\mathbb{Z}} \subset E/\mathbb{F}_p)$.
3. On suppose que pour $\pi_1 \neq \pi_2$ on a $Prob(\pi_1 \text{ divise } \#E/\mathbb{F}_p/p \in \mathcal{P}) \perp Prob(\pi_2 \text{ divise } \#E/\mathbb{F}_p/p \in \mathcal{P})$.
4. On calcule $Prob(\#E/\mathbb{F}_p \text{ est } B_1 - friable)$.

# Conclusion

Ce stage a permis de :

1. créer une démarche générale pour découvrir des paramétrisations, qui permet notamment de retrouver rapidement toutes les paramétrisations connues ;
2. découvrir les familles infinies *Suyama* 11 et *Suyama* 9/4 (à partir d'un nombre fini de courbes isolées par Kruppa et Zimmermann) et d'avoir contribué à montrer leur utilité ;
3. indiquer des nouvelles pistes de recherche permettant d'estimer la valuation moyenne.

# Annexe

Soit $E(A, B)$ une courbe elliptique sur un corps $K$. On munit $E(A, B)$ d'une loi de composition $P_1(X_1, Y_1, Z_1) + P_2(X_2, Y_2, Z_2) = P_3(X_3, Y_3, Z_3)$ par :

1. Si $x_1 z_2 \neq x_2 z_1$ alors
$$\begin{cases} (\lambda_n, \lambda_d) = (y_2 - y_1, x_2 - x_1) \\ (\mu_n, \mu_d) = (y_1 x_2 - y_2 x_1, x_2 - x_1) \\ x_3 = \lambda_d^2 \mu_d (\lambda_n^2 - (1 - x_1 - x_2)\lambda_d^2) \\ y_3 = -x_3 \lambda_n - \mu_n \lambda_d^2 \\ z_3 = \lambda_d^4 \mu_d \end{cases}$$
2. Si $x_1 z_2 \neq x_2 z_1$ et $y_1 z_2 = -y_2 z_1$ alors $(x_3, y_3, z_3) := (0, 1, 0)$.
3. Si $x_1 z_2 = x_2 z_1$ et $y_1 z_2 \neq -y_2 z_1$ alors

$$\begin{cases} (\lambda_n, \lambda_d) = (y_2 - y_1, x_2 - x_1) \\ (\mu_n, \mu_d) = (3x_1^2 + 2x_1 + A, 2y_1) \\ (\lambda_n, \lambda_d) = (-x_1^3 + Ax_1 + 2B, 2y_1) \\ \text{mêmes formules pour } x_3, y_3, z_3 \text{ qu'au cas } (i) \end{cases}$$

Dans [Sil86] on montre que + est une loi de groupe abélien. On remarque qu'on peut rendre les formules indépendante du test $x_1y_2 - y_1x_1 = 0$.

# Références


[CP00] R. Crandall and C. Pomerance. *Prime numbers – A Computational Perspective*. Springer Verlag, 2000.

[HS00] M. Hindry and J. Silverman. *Diophantine geometry. An introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer–Verlag, 2000.

[IR82] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer, 1982.

[Len87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126:649–673, 1987.

[Maz77] B. Mazur. Rational points on modular curves. In *Modular forms of one variable V*, volume 601 of *Lecture Notes in Math.*, pages 107–148. Springer Verlag, 1977. Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976.

[Mon92] P. L. Montgomery. *An FFT extension of the Elliptic Curve Method of factorization*. PhD thesis, University of California – Los Angeles, 1992.

[Ser72] J.-P. Serre. Prpriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones math.*, 15:259–331, 1972.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts in Math.* Springer, 1986.

[SL06] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *The mathematical intelligencer*, 18 NO.2, 2006.

[Suy] H. Suyama. Informal preliminary report (8). 25 Oct 1985.

[SW93] R. D. Silverman and S. S. Wagstaff, Jr. A practical analysis of the elliptic curve factoring method. *Math. Comp.*, 61:445–462, 1993.