TIPE - Courbes elliptiques et factorisation (version détaillée)

Samuel MIMRAM

2001–2002

Dernière révision : 17 mai 2006.

Table des matières

Une décomposition : la factorisation

Dans ce TIPE, nous allons définir des ensembles particuliers appelés courbes elliptiques et munir ces derniers d'une structure de groupe. Nous proposerons ensuite une méthode basée sur l'utilisation de ces groupes pour décomposer un "grand" entier en produit de facteurs premiers. Cette méthode est, à l'heure actuelle, la plus rapide pour factoriser les entiers compris entre 10^6 et 10^{30}. Elle a été trouvée en 1985 par Lenstra.

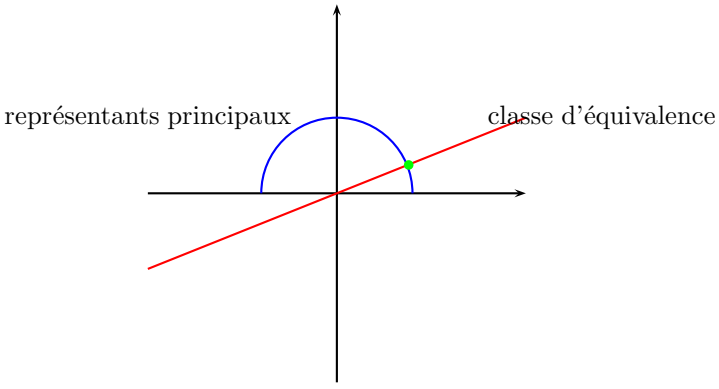
1 Les courbes elliptiques, définitions, propriétés

1.1 Définition des courbes elliptiques

Définition 1 (Plan projectif)**.** On appelle *plan projectif* sur un corps $\mathbb{K}$ l'ensemble, noté $\mathbb{P}^2(\mathbb{K})$, des classes d'équivalence $\left(\mathbb{K}^3\backslash\{(0,0,0)\}\right)/\mathcal{R}$, où $\mathcal{R}$ est une relation d'équivalence définie par :

$$\forall\left((a,b,c),(a',b',c')\right) \in \left(\left(\mathbb{K}^3\backslash\{(0,0,0)\}\right)^3\right)^2,$$
$$(a,b,c)\mathcal{R}(a',b',c') \Leftrightarrow [\exists t \in \mathbb{K}\backslash\{0\}, (a,b,c) = t(a',b',c')]$$

Pratiquement, cela revient à "projeter l'espace sur une demi-sphère" centrée en $(0,0,0)$.



Définition 2 (Courbe elliptique)**.** On appelle *courbe elliptique sur un corps* $\mathbb{K}$, notée $E(\mathbb{K})$, une courbe cubique dans le plan projectif $\mathbb{P}^2(\mathbb{K})$ i.e. définie par $F(X,Y,Z) = 0$ où F est un polynôme de degré 3, homogène en trois variables, à coefficients dans $\mathbb{K}$:

$$F(X,Y,Z) = \alpha_1X^3+\alpha_2Y^3+\alpha_3Z^3+\alpha_4X^2Y+\alpha_5X^2Z+\alpha_6Y^2X+\alpha_7Y^2Z+\alpha_8Z^2X+\alpha_9Z^2Y+\alpha_{10}XYZ = 0$$

et munie d'une origine $\mathcal{O} \in E(\mathbb{K})$.

Remarque 3. Dans la suite, nous nous intéresserons aux courbes elliptiques non singulières i.e. :

$$\forall P \in E(\mathbb{K}), \left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) \neq (0,0,0)$$

définies sur un corps $\mathbb{K}$ de caractéristique différente de 2 ou 3.
Lorsqu'il n'y a pas d'ambiguité sur le corps, nous noterons indifféremment les courbes $E(\mathbb{K})$ ou E.

Proposition 4. *Soit E une courbe elliptique. On peut se ramener à une équation de E, dite forme courte de Weierstrß :*

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{1}$$

On peut alors écrire cette équation en coordonnées non homogènes ($x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$) :

$$E : y^2 = x^3 + ax + b \tag{2}$$

plus le point $\mathcal{O} = (0, 1, 0)$ qui est le seul point à l'infini ($Z = 0$) et que l'on choisit comme origine.

Démonstration. Par un changement de variables homographique, on peut toujours se ramener à une équation dite *forme générale de Weierstraß* :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{3}$$

les changements de variable $Y \leftarrow (Y - \frac{1}{2}(a_1X + a_3))$ et $X \leftarrow (X - \frac{a_1^2+4a_2}{12}Z)$ permettent alors d'aboutir au résultat souhaité. On peut remarquer que l'on doit avoir $2 \neq 0$ et $12 \neq 0$ d'où la nécessité que $\mathbb{K}$ soit de caractéristique différente de 2 ou 3. □

Théorème 5. *Soit E une courbe donnée par une équation de Weierstraß. Alors E est non singulière si et seulement si la quantité $\Delta = 4a^3 + 27b^2$ est non nulle.*

Démonstration. Montrons d'abord que le point à l'infini $\mathcal{O} = (0, 1, 0)$ n'est jamais singulier. Regardons E comme une courbe de $\mathbb{P}^2(\mathbb{K})$ donnée par son équation :

$$F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$$

On a : $\frac{\partial F}{\partial Z} = Y^2 - 2aXZ - 3bZ^2$ donc :$\left(\frac{\partial F}{\partial Z}\right)(\mathcal{O}) = 1 \neq 0$; $\mathcal{O}$ n'est jamais un point singulier de E.
Pour les autres points considérons la définition de la courbe E par son équation de Weierstraß réduite :

$$E : f(x, y) = y^2 - x^3 - ax - b = 0$$

La courbe est singulière en un point $P_0 = (x_0, y_0) \in E$ si et seulement si :

$$\begin{cases} \left(\dfrac{\partial f}{\partial x}\right)(x_0, y_0) = 3x_0^2 + a = 0 \\ \left(\dfrac{\partial f}{\partial y}\right)(x_0, y_0) = 2y_0 = 0 \end{cases}$$

soit encore :

$$\begin{cases} x_0^2 = -\dfrac{a}{3} \\ y_0 = 0 \end{cases}$$

Car $2 \neq 0$ et $3 \neq 0$. Or P_0 est un point de la courbe, par conséquent $y_0^2 = 0 = x_0^3 + ax_0 + b = \frac{2}{3}ax_0 + b$. Il s'ensuit que $x_0^2 = \frac{9b^2}{4a^2} = -\frac{a}{3}$ soit $\Delta = 4a^3 + 27b^2 = 0$.
Finalement si E est non singulière si et seulement si $\Delta \neq 0$

□

1.2 Structure de groupe abélien

Montrons que l'on peut munir une courbe elliptique d'une structure de groupe abélien.

Proposition 6. *Soit E une courbe elliptique et D une droite définies sur un corps $\mathbb{K}$. Si E a au moins deux points d'intersection (comptés avec leur multiplicité) avec la droite D, alors E a exactement trois points d'intersection (comptés avec leur multiplicité) avec la droite D.*

Démonstration. On suppose que E est définie par $E : f(x, y) = y^2 - (x^3 + ax + b) = 0 \cup \mathcal{O} = (0, 1, 0)$. On suppose que D n'est pas verticale ($x \neq$ constante) et qu'elle est décrite par l'équation $y = \alpha x + \beta$. Les points d'intersection de E et D vérifient $f(x, \alpha x + \beta) = 0$, soit $P(x) = x^3 - \alpha x^2 + (a - 2\alpha\beta)x + (b - \beta) = 0$. Soit $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points d'intersection de E et D (différents de $\mathcal{O}$). x_1 et x_2 sont donc deux racines réelles de P qui est un polynôme de degré 3 et admet donc une et une seule autre racine réelle x_3 (pas forcément distincte de x_1 et x_2). Le point $P_3 = (x_3, \alpha x_3 + \beta)$ sera alors *le* troisième point d'intersection de E et D.
On peut étendre cette démonstration au cas où D est verticale en montrant qu'alors le troisième point d'intersection est $\mathcal{O}$. De plus, dans le cas où par exemple $P_2 = \mathcal{O}$, on aura $P_3 = (x_1, -y_1)$. □

1.2.1 Approche géométrique de la loi de la sécante-tangente

Soit E une courbe elliptique définie sur $\mathbb{P}^2(\mathbb{K})$ par :

$$E : Y^2Z = X^3 + aXZ^2 + b \tag{4}$$

soit encore en coordonnées non homogènes (en posant $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$) :

$$E : y^2 = x^3 + ax + b \cup \mathcal{O} = (0, 1, 0) \tag{5}$$

On peut alors définir sur E une loi de composition $*$ dite *loi de composition de la sécante-tangente* :

- si $(P, Q) \in E^2$ avec $P \neq Q$, on définit $P * Q$ comme étant le troisième point d'intersection de la droite D passant par P et Q avec E

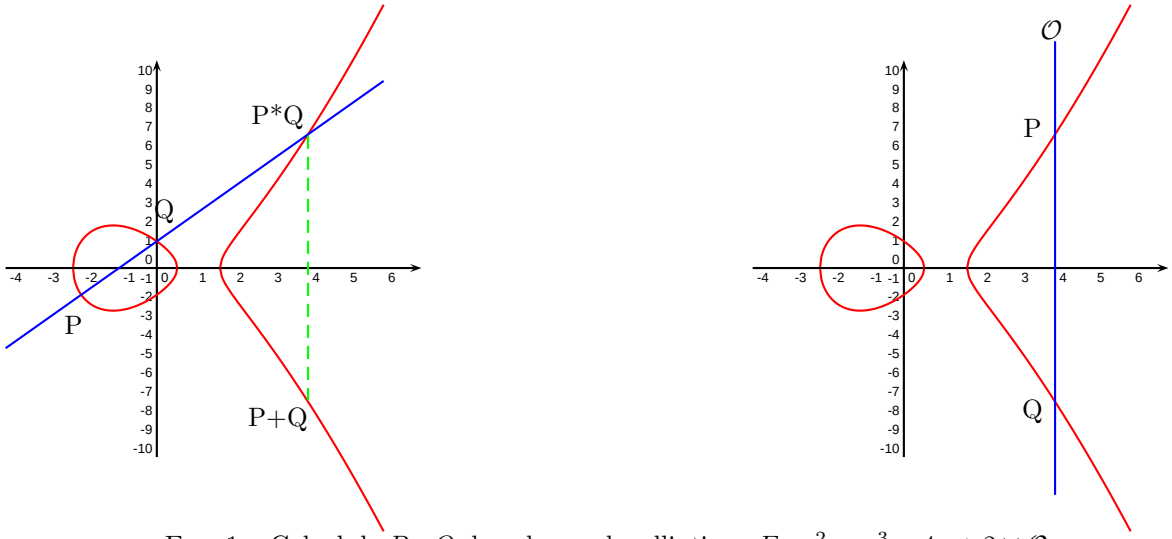


FIG. 1 – Calcul de $P * Q$ dans la courbe elliptique $E : y^2 = x^3 - 4x + 2 \cup \mathcal{O}$

- si $P \in E$, on définit $P * P$ comme étant le troisième point d'intersection de la droite D tangente à la courbe en P avec E (P est alors considéré comme un point double d'intersection)

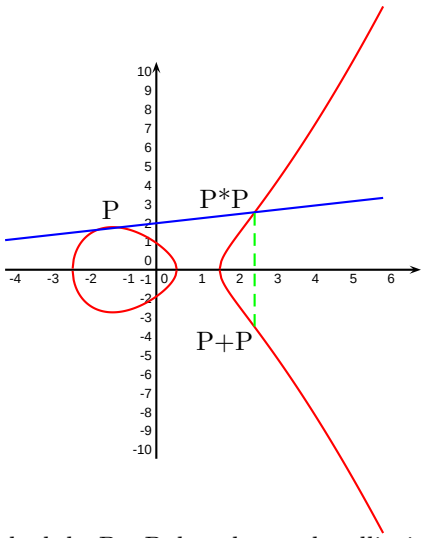


FIG. 2 – Calcul de $P * P$ dans la courbe elliptique $E : y^2 = x^3 - 4x + 2 \cup \mathcal{O}$

Remarque 7. On a aussi représenté $P + Q = \mathcal{O} * (P * Q)$.

1.2.2 Expression analytique de $*$

Soit E une courbe elliptique définie par :

$$E : f(x,y) = y^2 - (x^3 + ax + b) = 0 \cup \mathcal{O} = (0,1,0) \qquad \text{avec } 4a^3 + 27b^2 \neq 0 \quad (6)$$

Proposition 8. *Soit $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ et $P_3 = (x_3, y_3)$ trois points de $E\backslash\{\mathcal{O}\}$ tels que $P_1 \neq P_2$. Si $x_1 \neq x_2$ et si $P_3 = P_1 * P_2$, alors*

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_3 - x_1) + y_1 \end{cases}$$

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

Démonstration. Si $x_2 \neq x_1$ alors la sécante D passant par P_1 et P_2 a pour pente $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. Soit $\gamma = y_1 - \lambda x_1$. L'équation de D est alors : $y = \lambda x + \gamma$. On a alors :

$$\begin{aligned} f(x, \lambda x + \gamma) &= (\lambda x + \gamma)^2 - (x^3 + ax + b) \\ &= -x^3 + \lambda^2 x^2 + (2\lambda\gamma - a)x + (\gamma^2 - b) \end{aligned}$$

Or les points P_1, P_2 et P_3 sont racines de f car ils appartiennent à la courbe E. De plus ils appatiennent à la droite D. On doit donc avoir : $f(x_1, \lambda x_1 + \gamma) = f(x_2, \lambda x_2 + \gamma) = f(x_3, \lambda x_3 + \gamma) = 0$. x_1, x_2 et x_3 étant distincts, ce sont donc les trois racines du polynôme de degré 3 : $-x^3 + \lambda^2 x^2 + (2\lambda\gamma - a)x + (\gamma^2 - b)$. D'où :

$$\begin{aligned} -x^3 + \lambda^2 x^2 + (2\lambda\gamma - a)x + (\gamma^2 - b) \\ &= -(x - x_1)(x - x_2)(x - x_3) \\ &= -x^3 + (x_1 + x_2 + x_3)x^2 - (x_1x_2 + x_1x_3 + x_2x_3)x + (x_1x_2x_3) \end{aligned}$$

Par identification du coefficient de x^2, on obtient : $x_3 = \lambda^2 - x_1 - x_2$. De plus : $y_3 = (y_3 - y_1) + y_1 = \lambda(x_3 - x_1) + y_1$. □

Remarque 9. Cette définition est encore vraie dans le cas où $x_1 = x_2$ et $y_2 = -y_1$ avec $P_1 * P_2 = \mathcal{O}$.

Proposition 10. *Soit $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $E\backslash\{\mathcal{O}\}$. Si $P_2 = P_1 * P_1$, alors*

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_3 - x_1) + y_1 \end{aligned}$$

avec $\lambda = \frac{3x_1^2 + a}{2y_1}$.

Démonstration. La tangente D à E en P_1 a pour pente : $\lambda = -\frac{\frac{\partial f}{\partial x}(P_1)}{\frac{\partial f}{\partial y}(P_1)} = \frac{3x_1^2 + a}{2y_1}$. Soit $\gamma = y_1 - \lambda x_1$. L'équation de D est alors : $y = \lambda x + \gamma$. Et la démonstration est alors identique à celle de la proposition 8. □

Remarque 11. Le fait d'avoir imposé que la courbe soit non singulière nous permet d'être assurés que la tangente existera toujours.

Proposition 12. *On a de plus* $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

Démonstration. Si E est définie par $F(X,Y,Z) = Y^2Z-(X^3+aXZ^2+bZ^3) = 0$, on a : $\frac{\partial F}{\partial X} = -3X^2 - aZ^2$, $\frac{\partial F}{\partial Y} = 2YZ$ et $\frac{\partial F}{\partial Z} = Y^2 - 2aXZ - 3bZ^2$. Donc un vecteur normal à la courbe a pour coordonnées : $\overrightarrow{\text{grad}}F(\mathcal{O}) = (0,0,1)$. Le plan d'équation $Z = 0$ est donc un plan tangent à la courbe en $\mathcal{O}$ (c'est une droite du plan projectif $\mathbb{P}^2(\mathbb{K})$). Or $F(X,Y,0) = 0 \Leftrightarrow X^3 = 0$. Le point $\mathcal{O} = (0,1,0)$ est donc le seul point (triple) d'intersection de la tangente à la courbe en $\mathcal{O}$ avec la courbe. Donc $\mathcal{O} * \mathcal{O} = \mathcal{O}$. □

Proposition 13. *Si* $P_2 = \mathcal{O} * P_1$ *ou* $P_2 = P_1 * \mathcal{O}$ *alors*

$$\begin{aligned} x_2 &= x_1 \\ y_2 &= -y_1 \end{aligned}$$

Remarque 14. La loi de composition interne $*$ est commutative par construction mais n'est pas, *a priori*, associative.

Corollaire 15. *Soit* E *est une courbe elliptique définie sur un corps* $\mathbb{K}$*, soit* P_1 *et* P_2 *deux points de* E*. Alors l'opération* $+$ *définie par*

$$\forall (P_1, P_2) \in E, P_1 + P_2 = \mathcal{O} * (P_1 * P_2)$$

permet de munir E *d'une structure de groupe abélien (commutatif) admettant* $\mathcal{O}$ *comme élément neutre.*
De plus, supposons $P_1 = (x_1, y_1) \neq \mathcal{O}$ *et* $P_2 = (x_2, y_2) \neq \mathcal{O}$*. Si* $x_1 = x_2$ *et* $y_2 = -y_1$ *alors* $P_1 + P_2 = \mathcal{O}$ *; dans les autres cas, si* $P_3 = (x_3, y_3) = P_1 + P_2$*, alors*

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

où

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & si\ P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & si\ P = Q \end{cases}$$

On a enfin

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

Démonstration. $+$ ainsi définie est une loi de composition interne. Le fait que $\mathcal{O}$ est élément neutre découle de la remaque 12. L'existence d'un inverse est immédiate avec la proposition 13. On vérifie de plus que $+$ est associative. □

Remarque 16. Cette proposition est encore vraie dans les cas où $\mathbb{K}$ est un corps de caractéristique 2 ou 3.

Remarque 17. Le calcul de λ fait appel à un inverse (dans $\mathbb{K}$) ce qui justifie la nécessité pour $\mathbb{K}$ d'être un corps.

1.3 Cardinalité

Remarque 18. Si p est un nombre premier, on notera dans la suite $\mathbb{F}_p$ un corps fini de cardinal p.

Théorème 19 (Théorème de Hasse)**.** *Soit p un nombre premier. Si $E(\mathbb{F}_p)$ est une courbe elliptique définie sur le corps fini $\mathbb{F}_p$ de cardinalité p alors la cardinalité $\#E(\mathbb{F}_p)$ de $E(\mathbb{F}_p)$ vérifie*

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p} \tag{7}$$

Remarque 20. Deuring a montré que pour tout entier premier p, pour tout entier e compris entre $p+1-2\sqrt{p}$ et $p+1+2\sqrt{p}$, il existe une courbe elliptique $E(\mathbb{F}_p)$ telle que $\#E = e$. C'est donc le meilleur encadrement possible.

2 Un test de primalité

Proposition 21 (Critère de Goldwasser-Kilian)**.** *Soit $N \in \mathbb{N}$ premier avec 6 (i.e. divisible ni par 2, ni par 3). S'il existe un entier m et un point P de la courbe elliptique*

$$E : y^2 \equiv x^3 + ax + b \pmod{N} \cup \mathcal{O} = (0, 1, 0)$$

tels que

1. *il existe un facteur premier q de m strictement supérieur à $(N^{1/4} + 1)^2$*
2. *$mP = \mathcal{O} = (0, 1, 0)$*
3. *$\frac{m}{q}P = (x, y, z)$ avec $z \in (\mathbb{Z}/N\mathbb{Z})^*$*

alors N est premier.

Démonstration. Raisonnons par l'absurde. Supposons que N a un facteur premier p. Notons E' la courbe E modulo p, m' la cardinalité de E' et P' le point de E' correspondant au point P de E. Par hypothèse, $mP = \mathcal{O}$ et $\frac{m}{q}P \neq \mathcal{O}$ sur E et donc $mP' = \mathcal{O}$ (car $p|N$) et $\frac{m}{q}P' \neq \mathcal{O}$ (car $z \in (\mathbb{Z}/N\mathbb{Z})^*$). Ceci implique que q divise l'ordre de P' comme point de E', d'où, d'après le théorème de Lagrange, q divise m'. Il s'ensuit, d'après le théorème de Hasse (théorème 19) que :

$$\begin{aligned} q \leq m' &\leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \\ &\leq (N^{1/4} + 1)^2 \qquad \text{car } p \text{ étant un facteur premier de } N,\ p \leq \sqrt{N} \end{aligned}$$

Il y a contradiction avec l'hypothèse. □

Remarque 22. Nous faisons tous les calculs comme si N était premier. Si l'algorithme de Schoof (qui est l'algorithme le plus efficace pour calculer la cardinalité de E) n'aboutit pas, alors cela signifie que N est composé. De même, lors du calcul de mP et de $\frac{m}{q}P$, il est possible que le dénominateur intervenant dans le calcul de λ ne soit pas inversible. Cela signifie que $\mathbb{Z}/N\mathbb{Z}$ n'est pas un corps et donc que N est composé (par le théorème de Bezout). Nous avons alors prouvé que N n'est pas premier.

3 Une méthode de factorisation

L'algorithme de factorisation utilisant les courbes elliptiques est une variante de la méthode $p-1$ de Pollard dans $\mathbb{F}_p$.

Définition 23 (B-lissité)**.** Soit $N \in \mathbb{N}$ et soit $N = \prod_{i=1}^{m} p_i^{\alpha_i}$ la décomposition de N en facteurs premiers.
N est dit *B-lisse* si et seulement si :

$$\forall i \in [\![1, m]\!], p_i \leq B$$

N est dit *B-superlisse* si et seulement si :

$$\forall i \in [\![1, m]\!], p_i^{\alpha_i} \leq B$$

Méthode 24 ($p-1$ de Pollard)**.** Soit $N \in \mathbb{N}$ un entier à factoriser. On suppose que N admet un facteur premier p tel que $p-1$ soit B-superlisse. On a alors : $(p-1)|\text{PPCM}(1, 2, \ldots, B)$ d'où, d'après le petit théorème de Fermat :

$$\forall a \in \mathbb{N}, a \wedge N = 1 \Rightarrow a^{\text{PPCM}(1,2,\ldots,B)} \equiv 1 \pmod{p}$$

Par conséquent :

$$l = [(a^{\text{PPCM}(1,2,\ldots,B)} - 1) \wedge N] > 1$$

Si $l \neq N$, on a alors trouvé un facteur non trivial de N, sinon nous calculons l pour une autre valeur de a ; si $l = 1$, nous augmentons la valeur de B.

L'avantage de la méthode de Lenstra, basée sur les courbes elliptiques, est qu'elle ne nécessite pas, contrairement à la méthode $p-1$ de Pollard, que N ait un facteur premier p tel que $p-1$ soit B-superlisse.

Méthode 25 (de Lenstra)**.** Soit $N \in \mathbb{N}$ un entier, supposé non premier, admettant un facteur premier p (que l'on veut trouver). Voici les étapes du déroulement de la méthode de Lenstra pour la factorisation de N à l'aide de la courbe elliptique E définie par :

$$E : y^2 = x^3 + ax + b \cup \mathcal{O} = (0, 1, 0)$$

où a et b sont des entiers. On supposera la cardinalité de $\#E(\mathbb{F}_p)$ B-superlisse.

- On vérifie que N **n'est divisible ni par** 2**, ni par** 3 (sinon, on a trouvé un facteur de N) pour nous assurer que $\mathbb{Z}/p\mathbb{Z}$ sera de caractéristique différente de 2 ou 3.
- En notant $\Delta = 4a^3 + 27$, on vérifie que $\mathbf{\Delta \wedge N = 1}$ pour nous assurer que $E(\mathbb{Z}/N\mathbb{Z})$ est non singulière. Si $1 < \Delta \wedge N < N$ alors nous avons trouvé un facteur non trivial de N et si $\Delta \wedge N = N$ alors nous choisissons une autre courbe elliptique (d'autres valeurs de a, b et B).

– On choisit un point $P \in E(\mathbb{Z}/N\mathbb{Z})\backslash\{\mathcal{O}\}$. $\#E(\mathbb{F}_p)$ étant supposée B-superlisse, $\#E(\mathbb{F}_p)$ divise $k = \text{PPCM}(1, 2, \ldots, B)$. D'où, d'après le théorème de Lagrange, l'ordre de P divise k donc $kP = \mathcal{O}$. Si l'on calculait $kP = P + P + \ldots + P$ dans $E(\mathbb{F}_p)$, on serait alors amené à calculer $Q + P = \mathcal{O}$ avec $Q = k'P$ et $k' < k$. En pratique, on va effectuer le **calcul de kP** non pas dans $E(\mathbb{F}_p)$ mais dans $E(\mathbb{Z}/N\mathbb{Z})$.
Rappelons les formules d'addition pour $R = P + Q$ avec $P \neq \mathcal{O}$ et $Q \neq \mathcal{O}$ où $P = (x_1, y_1)$, $Q = (x_2, y_2)$ et $R = (x_3, y_3)$:
– si $x_1 = x_2$ et $y_2 = -y_1$ alors $P + Q = \mathcal{O}$
– sinon

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

où

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{si } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{si } P = Q \end{cases}$$

On aura $P + Q = \mathcal{O}$ donc $x_1 \equiv x_2 \pmod{p}$, soit $p | x_1 - x_2$. Mais il se peut que l'on ait : $x_1 \not\equiv x_2 \pmod{N}$. Lors du calcul λ pour additionner Q et P, $(x_1 - x_2)$ ne sera alors pas inversible (dans $\mathbb{Z}/N\mathbb{Z}$) car $p | \text{PGCD}(x_1 - x_2, N)$ donc $(x_1 - x_2) \wedge N \neq 1$. Dans ce cas, si $1 < (x_1 - x_2) \wedge N < N$ alors nous avons trouvé un facteur non trivial de N et si $(x_1 - x_2) \wedge N = N$ alors nous choisissons un autre courbe elliptique.
Si le calcul de kP dans $E(\mathbb{Z}/N\mathbb{Z})$ aboutit alors nous choisissons une autre courbe elliptique.

Pour le choix de la borne de lissité, on peut tenir le raisonnement suivant : si p est un facteur premier de N alors $p < \sqrt{N}$; or, d'après le théorème de Hasse (théorème 19), on a $\#E(\mathbb{F}_p) < (\sqrt{p} + 1)^2$. On peut donc prendre $B \geq \lceil (N^{1/4} + 1)^2 \rceil$.

Remarque 26. Dans la pratique, pour des raisons évidentes de rapidité de calcul, on ne prend pas $k = \text{PPCM}(1, 2, \ldots, B)$ mais simplement $k = \text{PPCM}(B, B - 1)$. Cela diminue la probabilité de trouver un facteur premier mais améliore de beaucoup la rapidité de l'algorithme.

Remarque 27. De plus, plus au lieu de l'addition naïve, le calcul de kP est effectué avec l'exponentiation rapide ; le principe reste cependant valable.

Remarque 28. Pour le choix de P dans $E_{a,b}$, on peut imposer $b = -a$, ce qui permet d'être assuré que $P = (1, 1)$ appartient à la courbe elliptique.

Il a été montré que le temps moyen d'aboutissement de cette méthode est en $O(\mathrm{e}^{(1+\varepsilon)\ln N \ln\ln N})$.

L'inconvénient de cette méthode est qu'elle n'est pas, stricto sensu, un algorithme car elle n'aboutit pas forcément à un résultat. Il faut lui adjoindre des tests de primalité (il en existe utilisant les courbes elliptiques).

4 Résultats inutilisés

4.1 Précisions à propos de la définition

Définition 29 (Courbe elliptique)**.** Soit K un corps. On appelle *courbe elliptique sur* K une courbe E dans le plan projectif $\mathbb{P}_2(K)$, cubique [1], sans points singuliers [2] et munie d'un point distingué $\mathcal{O} \in E$.

Par un changement de variables homographique, on peut toujours se ramener à une équation dite *de Weierstraß* (forme générale) :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{8}$$

Pour alléger les notations, on peut écrire l'équation de Weierstraß en coordonnées non homogènes ($x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$) :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{9}$$

plus le point $(0, 1, 0)$ qui est le seul point à l'infini ($Z = 0$) et que l'on choisit comme point distingué $\mathcal{O}$.

On définit alors les quantités suivantes :

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^3 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4 \quad \text{et} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

Définition 30 (Discriminant)**.** On appelle *discriminant* Δ de l'équation de Weierstraß la quantité

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{10}$$

Définition 31 (j-invariant)**.** On appelle *j-invariant* de la courbe elliptique E la quantité

$$j(E) = \frac{c_4^3}{\Delta} \tag{11}$$

Théorème 32. *Si K est de caractéristique p autre que 2 ou 3, on peut toujours trouver une "forme courte" de Weierstraß, i.e. mettre E sous la forme :*

$$y^2 = x^3 + ax + b \tag{12}$$

dans ce cas on a :

$$\Delta = -16(4a^3 + 27b^2) \quad \textit{et} \quad j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \tag{13}$$

Démonstration. Si $p \neq 2$, alors $2 \neq 0_K$. On peut donc faire le changement de variable $y \leftarrow (y - \frac{1}{2}(a_1x + a_3))$ et on obtient : $y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. Si de plus $p \neq 3$, on peut faire le changement de variable $x \leftarrow (x - \frac{b_2}{12})$ pour obtenir : $y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$. D'où le résultat cherché en posant $a = -\frac{c_4}{48}$ et $b = -\frac{c_6}{864}$. □

[1] i.e. définie par $F(X, Y, Z) = 0$ où F est un polynôme de degré 3, homogène en trois variables, à coefficients dans K

[2] i.e. : $\forall P \in E, \left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) \neq (0, 0, 0)$

Remarque 33. Dans les cas où $p = 2$ ou 3 on a , suivant p et $j(E)$:

p	$j(E)$	E :	Δ	$j(E)$
2	0	$y^2 + cy = x^3 + ax + b$	c^4	0
2	$\neq 0$	$y^2 + xy = x^3 + ax^2 + b$	a	$1/a$
3	0	$y^2 = x^3 + ax + b$	$-a^3$	0
3	$\neq 0$	$y^2 = x^3 + ax^2 + b$	$-a^3b$	$-a^3/b$

Lemme 34. *Soit E une courbe donnée par son équation de Weierstraß générale :*

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

dont le discriminant vaut Δ et le j-invariant $j(E)$. Le changement de variables

$$(x, y) \leftarrow (u^2x + r, u^3y + u^2sx + t) \quad \textit{avec } r, s, t, u \in K^4 \textit{ et } u \neq 0$$

transforme l'équation précédente en

$$E' : f'(x, y) = y^2 + a'_1xy + a'_3y - x^3 - a'_2x^2 - a'_4x - a'_6 = 0$$

où les coefficients sont donnés par

$$\begin{aligned} ua'_1 &= a_1 + 2s \\ u^2a'_2 &= a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 &= a_3 + ra_1 + 2t \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \end{aligned}$$

De plus $u^{12}\Delta' = \Delta$ et $j(E') = j(E)$.

Théorème 35. *Soit E une courbe donnée par une équation de Weierstraß. Alors E est non singulière si et seulement si $\Delta \neq 0$.*

Démonstration. ($\Leftarrow$) Soit l'équation générale de Weierstraß :

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

On suppose que son discriminant Δ est non nul.
Montrons d'abord que le point à l'infini $\mathcal{O} = (0, 1, 0)$ n'est jamais singulier. Regardons E comme une courbe de $\mathbb{P}^2$ donnée par son équation :

$$F(W, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

Comme $\left(\frac{\partial F}{\partial Z}\right)(\mathcal{O}) = 1 \neq 0$, $\mathcal{O}$ n'est jamais un point singulier de E.
Raisonnons par l'absurde et supposons que E soit singulière en un point $P_0 = (x_0, y_0)$. Par le changement de variables $(x, y) \leftarrow (x - x_0, y - y_0)$, nous ramenons le point P_0 en $(0, 0)$. D'après le lemme 34, cette transformation ne modifie pas le discriminant (car $u = 1$). Nous avons alors $a_6 = f(0, 0) = 0$,$a_4 = \left(\frac{\partial f}{\partial x}\right)(0, 0) = 0$ et $a_3 = \left(\frac{\partial f}{\partial y}\right)(0, 0) = 0$. La courbe E a donc pour équation :

$$E : f(x, y) = y^2 + a_1xy - x^3 - a_2x^2 = 0$$

Or le discriminant de cette équation est nul : il y a contradiction avec l'hypothèse. La courbe E n'a donc aucun point singulier.

($\Rightarrow$) On ne s'intéressera ici qu'au cas où la caractéristique p de K est différente de 2 et de 3. La courbe E est alors donnée par l'équation de Weierstraß réduite :

$$E : f(x, y) = y^2 - (x^3 + ax + b) = 0$$

Raisonnons par l'absurde. Si la courbe est singulière en un point $P_0 = (x_0, y_0) \in E$, alors :

$$\left(\frac{\partial f}{\partial x}\right)(x_0, y_0) = 3x_0^2 + a_4 = 0 \Rightarrow x_0^2 = -\frac{a_4}{3}$$
$$\left(\frac{\partial f}{\partial y}\right)(x_0, y_0) = 2y_0 = 0 \Rightarrow y_0 = 0$$

Or P_0 est un point de la courbe, par conséquent $y_0^2 = 0 = x_0^3 + ax_0 + b = \frac{2}{3}ax_0 + b$. Il s'ensuit que $x_0^2 = \frac{9b^2}{4a^2} = -\frac{a}{3}$ et donc $\Delta = -16(4a^3 + 27b^2) = 0$. Finalement si E est non singulière alors $\Delta \neq 0$

□

4.2 Autres propriétés

Définition 36 (Isogénie)**.** Soit E et E' deux courbes elliptiques définies sur un corps K. Une *isogénie* (homomorphisme de courbes elliptiques) de E dans E' est une application rationnelle ϕ (homomorphisme de courbes algébrique) non identiquement nulle et telle que $\phi(\mathcal{O}) = \mathcal{O}'$.

Théorème 37. *Si ϕ est une isogénie de E dans E', alors c'est un homomorphisme du groupe $(E, +_E)$ dans $(E', +_{E'})$.*

Remarque 38. Soit E une courbe elliptique. Soit m un entier. La multiplication par m (au sens de la loi de groupe) est une isogénie notée :

$$[m]_E : E \to E$$
$$P \mapsto mP$$

Définition 39 (Degré)**.** Le noyau d'une isogénie $\phi : E \to E'$ est donc un sous-groupe fini de E. On appelle *degré* de ϕ l'ordre de $\operatorname{Ker}\phi$.

Remarque 40. Si E est une courbe elliptique définie sur un corps K, on notera $E(m)$ le noyau de $[m]_E$ défini sur $\overline{K}$, la clôture algébrique de K.

Définition 41 (Isogénie duale)**.** Soit $\phi : E \to E'$ une isogénie de degré d. Alors il existe une unique isogénie $\hat{\phi} : E' \to E$ telle que $\hat{\phi} \circ \phi = [d]_{E'}$. On l'appelle *isogénie duale* de ϕ.

Théorème 42. *Deux courbes elliptiques sont isogènes sur le corps $\mathbb{F}_q$ si et seulement si elles ont même cardinalité.*

Théorème 43. *Tout isomorphisme (isogénie bijective) de courbes elliptiques est de la forme :*

$$(x, y) \leftarrow (u^2x + r, u^3y + u^2sx + t) \quad \textit{avec } r, s, t, u \in K^4 \textit{ et } u \neq 0$$

Théorème 44. *Deux courbes données par leur équation de Weierstraß dont le discriminant est non nul sont isomorphes si et seulement si elles ont le même j-invariant.*

Théorème 45. *Soit E une courbe elliptique sur le corps fini $\mathbb{F}_q$. Alors le groupe $(E, +)$ est ou bien cyclique, ou bien isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ avec $n_2|(n_1 \wedge p - 1)$.*

4.2.1 L'algorithme de Shanks

Algorithme 46 ("Pas de bébé, pas de géant")**.** D'après le théorème de Hasse (théorème 19), l'ordre d'une courbe elliptique E définie sur $\mathbb{F}_q$ est de la forme $\#E = p + 1 - c$ où c est un entier de l'intervalle $[-2\sqrt{q}, 2\sqrt{q}]$. Pour un point P choisi aléatoirement dans E on doit alors avoir : $(q + 1 - c)P = 0$.
L'énumération naïve nécessiterait $O(\sqrt{q})$ opérations dans $\mathbb{F}_q$.
L'idée de Shanks est basée sur le fait que la calcul d'un opposé d'un point de E est immédiat (corollaire 15). Pour $P \in E$ il suffit donc de chercher deux entiers c_0 et c_1 respectivement dans $[0, 2q^{1/4}]$ et dans $[-\frac{q^{1/4}}{2}, \frac{q^{1/4}}{2}]$ tels que

$$(q + 1 - c_1 4\lceil q^{1/4} \rceil)P = \pm c_0 P$$

on pose alors $c = \pm c_0 + c_1 4\lceil q^{1/4} \rceil$ et $q + 1 - c$ est un multiple de l'ordre de P (et l'ordre de P divise l'ordre de E).
L'algorithme comporte deux phases :

- la phase des "pas de géant" qui consiste à stocker dans une table les $\lceil q^{1/4} \rceil + 1$ points $(q + 1 - c_1 4q^{1/4})P$
- la phase des "pas de bébé" qui consiste à calculer les points c_0P pour c_0 variant de 0 à $2\lceil q^{1/4} \rceil$ et à vérifier si les points c_0P et $-c_0P$ correspondent à une entrée dans la première table

On peut en moyenne espérer, avec cet algorithme, une complexité totale de $O(q^{1/4} \ln^2 q)$.

4.2.2 L'algorithme de Schoof

Définition 47 (Frobenius)**.** Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique p. L'*automorphisme de Frobenius* est défini par

$$\phi_E : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$$
$$P \mapsto \begin{cases} \mathcal{O} & \text{si } P = \mathcal{O} \\ (x^q, y^q) & \text{si } P = (x, y) \end{cases}$$

Théorème 48. *Le polynôme caractéristique de ϕ_E est*

$$\phi_E^2 - [c]_E \circ \phi_E + [q]_E = 0 \tag{14}$$

où c est défini par

$$\#E(\mathbb{F}_q) = q + 1 - c$$

Remarque 49. D'après le théorème de Hasse (théorème 19), on a : $|c| \leq 2\sqrt{q}$.

Définition 50 (Polynômes de division)**.** Avec les notations de la définition 29, les polynômes de division $f_m(X)$ d'une courbe elliptique E sont définis par

$$
\begin{aligned}
&f_0(X) = 0\\
&f_1(X) = 1\\
&f_2(X) = 1\\
&f_3(X) = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_6\\
&f_4(X) = 2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)
\end{aligned}
$$

et, en posant $F(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$,

$$
\begin{aligned}
f_{2m} &= f_m(f_{m+2}f_{m-1}^2 - f_{m-3}f_{m+1}^2)\\
f_{2m+1} &= \begin{cases} F^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3 & \text{si } m \text{ est pair} \\ f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3F^2 & \text{sinon} \end{cases}
\end{aligned}
$$

Le polynôme f_m est de degré au plus $\frac{m^2+1}{2}$ si m est impair et $\frac{m^2-1}{2}$ si m est pair.

Théorème 51. *Soit E une courbe elliptique définie sur un corps K, P un point de K et $m \in \mathbb{N}^*$. Alors*

$$
[m]_E(P) = \begin{cases} \mathcal{O} & \text{si } P \in E[m] \\ \left(\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right) & \text{si } P = (x,y) \in E(\overline{K})\backslash E[m] \end{cases}
$$

où les polynômes vérifient ψ_m, ϕ_m et ω_m satisfont (avec les notations de la définition 29)

$$
\psi_m = \begin{cases} (2Y + a_1X + a_3)f_m & \text{si } m \text{ est pair} \\ f_m & \text{sinon} \end{cases}
$$

et

$$
\begin{aligned}
\phi_m &= X\psi_m^2 - \psi_{m-1}\psi_{m+1}\\
2\psi_m\omega_m &= \psi_{2m} - \psi_m^2(a_1\psi_m + a_3\psi_m^2)
\end{aligned}
$$

Remarque 52. Ce théorème nous fournit une construction explicite de $[m]_E$.

Théorème 53. *Soit $P \in E(\overline{K})$. Alors $P \in E[m]$ si et seulement si $P = \mathcal{O}$ (trivial) ou, lorsque $P(x,y)$, si $f_m(x) = 0$.*

Algorithme 54 (Algorithme de Schoof)**.** Soit E une courbe elliptique définie sur $\mathbb{F}_q$. L'idée de Schoof est de restreindre l'équation caractéristique du Frobenius (14) aux sous-groupes $E[l]$ (où $l \in \mathbb{N}^*$) et $E(\overline{\mathbb{F}_q})$ ce qui donne

$$
\forall l \in \mathbb{N}^*, \phi_{E[l]}^2 + [q \bmod l]_{E[l]} = [c \bmod l]_{E[l]} \circ \phi_{E[l]} \tag{15}
$$

soit encore

$$\forall l \in \mathbb{N}^*, \forall (x,y) \in E[l], (x^{q^2}, y^{q^2}) + [q \bmod l](x,y) = [c \bmod l](x^q, y^q)$$

où c est tel que $\#E(\mathbb{F}_q) = q + 1 - c$.
L'algorithme consiste à calculer le membre de gauche de l'équation (15) pour un point P d'ordre l, dans $E(\overline{\mathbb{F}_q})$; puis à calculer $[\theta]_{E[l]}(\phi_{E[l]}(P))$ pour θ dans $\mathbb{F}_l$ jusqu'à ce que l'égalité (15) soit vérifiée. Lorsque c'est le cas, nous avons $c \equiv \theta \pmod{l}$. Il ne reste plus qu'á répéter ce calcul pour des entiers l premiers entre eux etvérifiant $\prod l > 4\sqrt{q}$ pour trouver c à l'aide du théorème chinois qui stipule que si $l_1, \ldots, l_n$ sont n entiers de $\mathbb{N}\backslash\{0,1\}$ premiers entre eux deux à deux alors $\mathbb{Z}/l_1\mathbb{Z} \times \ldots \times \mathbb{Z}/l_n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/(\prod_{i=1}^n l_i)\mathbb{Z}$.

La complexité totale de l'algorithme est $O(\ln^8 q)$.

4.3 Le critère de Pocklington

Théorème 55. *Soit $N \in \mathbb{N}^*$. Notons $N - 1 = \prod_{j=1}^n p_j^{e_j}$ la décomposition de $N-1$ en facteurs premiers. S'il existe un entier a et $i \in [\![1,n]\!]$ tels que :*

$$a^{N-1} \equiv 1 \pmod{N} \qquad et \qquad (a^{(N-1)/p_i} - 1) \wedge N = 1 \tag{16}$$

alors : $d|N \Rightarrow d \equiv 1 \pmod{p_i^{e_i}}$.

Démonstration. Comme tout facteur d de N est le produit de nombre premiers (éventuellement d'un seul nombre premier), il suffira de démontrer le théorème pour tout facteur premier q de N.
On a : $a^{N-1} \equiv 1 \pmod{N}$ donc a^{N-1} est inversible dans $\mathbb{Z}/N\mathbb{Z}$, soit $a^{N-1} \wedge N = 1$. Or $q|N$, donc $a^{N-1} \wedge q = 1$. q étant supposé premier, on en déduit, d'après le petit théorème de Fermat : $a^{q-1} \equiv 1 \pmod{q}$. Notons o l'ordre de a modulo q. La relation précédente implique : $o|q-1$.
D'autre part, $(a^{(N-1)/p_i} - 1) \wedge N = 1$ donc $(a^{(N-1)/p_i} - 1) \wedge q = 1$ (car $q|N$) donc $a^{(N-1)/p_i} - 1 \equiv 1 \pmod{q}$ donc $a^{(N-1)/p_i} \equiv 2 \not\equiv 1 \pmod{q}$. Les hypothèses impliquent donc :

$$\left.\begin{aligned} a^{N-1} &\equiv 1 \pmod{q} \\ a^{(N-1)/p_i} &\not\equiv 1 \pmod{q} \end{aligned}\right\} \Rightarrow o | p_i^{e_i} \prod_{\substack{j=1 \\ j\neq 1}}^n p_j^{e_j} \text{ et } o \not| p_i^{e_i - 1} \prod_{\substack{j=1 \\ j\neq 1}}^n p_j^{e_j}$$

$$\Rightarrow \exists (\alpha, \beta) \in (\mathbb{N}^*)^2, o\alpha = p_i^{e_i} M \text{ et } o\beta \neq p_i^{e_i - 1} M \quad \text{avec } M = \prod_{\substack{j=1 \\ j\neq 1}}^n p_j^{e_j}$$

$$\Rightarrow \exists (\alpha, \beta) \in (\mathbb{N}^*)^2, p_i^{e_i} | o\alpha \text{ et } p_i^{e_i} \not| o\beta$$
$$\Rightarrow p_i^{e_i} | o$$

Finalement, on a : $p_i^{e_i} | o$ et $o | q-1$. Donc $p_i^{e_i} | q-1$, soit $q - 1 \equiv 0 \pmod{p_i^{e_i}}$. D'où $q \equiv 1 \pmod{p_i^{e_i}}$. □

Corollaire 56 (Critère de Pocklington-Lehmer)**.** *Si il existe $(F, U) \in \mathbb{N}^2$ tel que :*

1. $N - 1 = FU$

2. $F \wedge U = 1$

3. $F > \sqrt{N} - 1$

et pour tout facteur premier p_i *de* F*, il existe* a_{p_i} *tel que :*

$$a_{p_i}^{N-1} \equiv 1 \pmod{N} \qquad et \qquad (a_{p_i}^{(N-1)/p_i} - 1) \wedge N = 1 \tag{17}$$

alors N *est premier.*

Démonstration. D'après le théorème 55, l'hypothèse (17) étant suposée vérifiée, tout facteur de N est congru à 1 modulo F. Les facteurs de N dont donc de la forme $\alpha F + 1$ (avec $\alpha \in \mathbb{N}^*$). Or, comme $F > \sqrt{N} - 1$ tout facteur de N est strictement supérieur à $\sqrt{N}$. Donc N est premier. □

Corollaire 57 (Critère de Pocklington)**.** *Le critère de Pocklington est le critère de Pocklington-Lehmer dans le cas particulier où* F *est un facteur premier de* $(N-1)$*.*

Remarque 58. L'hypothèse *2.* du critère de Pocklington-Lehmer est alors toujours vérifiée.

4.4 Le critère de Goldwasser-Kilian dans $\mathbb{Z}/n\mathbb{Z}$

"Transposons" le critère de Pocklington aux coubes elliptiques.
Soit N un entier dont on veut tester la primalité. Des tests simples (calculs de congruences par exemple) peuvent nous permettre de nous assurer que N n'est divisible ni par 2, ni par 3. On peut donc restreindre notre étude à une courbe elliptique définie sur un corps de caractéristique différente de 2 et 3. Soit $(E, +) : y^2 = x^3 + ax + b \cup \mathcal{O}$ une telle courbe elliptique munie de la structure de groupe définie par le corollaire 15. Adaptons alors le test de Pocklington dans $(\mathbb{Z}/N\mathbb{Z}, \times)$ à $(E, +)$ où E est définie sur le corps $(\mathbb{Z}/N\mathbb{Z}, +, \times)$.

	$(\mathbb{Z}/n\mathbb{Z}\backslash\{0\}, \times)$	$(E, +)$
éléments	$[\![1, N-1]\!]$	$\{(x, y) \in (\mathbb{Z}/N\mathbb{Z}) \mid y^2 = x^3 + ax + b\} \cup \mathcal{O}$
l c i	.	$+$
neutre	1	$\mathcal{O}$
cardinalité	$N - 1$	$\#E$ avec $\lvert\#E - (N+1)\rvert \leq 2\sqrt{N}$

La condition $a^{N-1} \equiv 1 \pmod{N}$ s'écrit alors : $\#E \cdot P = \mathcal{O}$; la condition $(a^{(N-1)/q} - 1) \wedge N = 1$ équivalente à $a^{(N-1)/q} \not\equiv 1 \pmod{N}$ devient $\frac{\#E}{q} P \neq \mathcal{O}$. La condition $q > \sqrt{N} - 1$ signifie : $\forall p < \sqrt{N}, q > p$. Ce qui, transposée à $(E, +)$ devient $\forall p < \sqrt{N}, q > \#E_p$ où $\#E_p$ est la cardinalité de E modulo p. Or d'après le théorème de Hasse (théorème 19), $\#E \leq p+1+2\sqrt{p} = (\sqrt{p}+1)^2 \leq (N^{1/4}+1)^2$. La condition $q > (N^{1/4} + 1)^2$ suffit donc.

5 Notre implémentation

5.1 Détails de la mise en œuvre

Pour les variables numériques, nous n'utiliserons pas le type `int` limité à 32 bits (soit au maximum 8589934591) mais le type `largeint` qui nous permet de manipuler des entiers de taille quelconque.

5.1.1 La classe `ec_point`

On va travailler avec la courbe elliptique : $E : y^2 \equiv x^3 + ax + b \pmod{p} \cup \mathcal{O}$ avec $p \neq 2$ et $p \neq 3$. Les variables correspondantes `largeint a, b, p` sont définies globalement. On définit alors la classe `ec_point` dans laquelle on va implémenter les opérations dans la courbe elliptique :

```
class ec_point
{
public:
        largeint x;
        largeint y;
        bool Infty;

        ec_point() {Infty = false;};
        ec_point(largeint X, largeint Y) {x = X; y = Y; Infty = false;};
        ec_point(bool isO) {Infty = isO;};
        ~ec_point() {};
        void Print();

        void operator = (ec_point P) {x = P.x; y = P.y; Infty = P.Infty;};
        friend bool operator == (ec_point P1, ec_point P2);
        friend ec_point operator + (ec_point P1, ec_point P2);
        friend ec_point operator * (largeint m, ec_point P);
        friend ec_point operator * (int m, ec_point P);
};
```

La variable booléenne `Infty` vaut `true` si le point est $\mathcal{O}$; sinon le point est défini par ses coordonnées `x` et `y`. L'élément neutre $\mathcal{O}$ est donc défini par :

```
#define O_neutre ec_point(true)
```

On implémente ensuite l'addition de groupe par transcription directe du corollaire 15.

```
ec_point operator + (ec_point P1, ec_point P2)
{
        ec_point P3;
        largeint lambda;

        if (P1.Infty)
                P3 = P2;
        else if (P2.Infty)
                P3 = P1;
        else if (P1.x == P2.x && P1.y == mod (-P2.y, p))
                P3.Infty = true;
        else
        {
```

```
                if (P1 == P2)
15              {
                        if (gcd(P1.y, p) != 1)
                        {
                                //Lambda n'est pas inversible !
                                error_factor = P1.y;
20                              error = true;
                        }
                        lambda = mod((3 * P1.x * P1.x + a) * invModN(2 * P1.y, p), p);
                }
                else
25              {
                        if (gcd(P2.x - P1.x, p) != 1)
                        {
                                //Lambda n'est pas inversible !
                                error_factor = P2.x - P1.x;
30                              error = true;
                        }
                        lambda = mod((P2.y - P1.y) * invModN(P2.x - P1.x, p), p);
                }
                P3.x = mod((lambda * lambda - P1.x - P2.x), p);
35              P3.y = mod((lambda * (P1.x - P3.x) - P1.y), p);
        }
        return P3;
}
```

5.1.2 Calcul de kP

L'algorithme utilisé est une adaptation de l'algorithme classique d'exponentiation rapide. L'idée principale en est que si $k = \overline{k_n k_{n-1} \dots k_1 k_0}^{(2)}$ est l'écriture en base 2 de k alors $kP = \sum_{i=0}^{n} k_i(2^i P)$. Elle permet de calculer kP avec $O(\ln n)$ opérations au lieu de $O(n)$ pour l'addition naïve. Voici son implémentation pratique :

```
1   ec_point fast_scalarmult (largeint m, ec_point P)
    {
        ec_point tmpP, retP;

5       retP = O_neutre;
        tmpP = P;
        while (m != 0)
        {
            if(error)               //Lambda n'etait pas inversible !
10              return O_neutre;
            if(getbit(m, 0))        //Le bit de poids le plus faible est il non nul ?
                retP = retP + tmpP;
            m >> 1;                 //Decalage de 1 bit vers la gauche
            tmpP = 2 * tmpP;
15      }

        return retP;
    }
```

5.1.3 Calcul des inverses

Lors du calcul de λ, l'inverse de $(x_2 - x_1)$ ou de $2y_1$ modulo n est calculé à l'aide de l'algorithme d'Euclide étendu qui permet de calculer les coefficients de Bezout. Il est basé sur l'identité fontamentale de l'algorithme d'Euclide suivante :

$$d = a \wedge b = b \wedge (a \bmod b) \tag{18}$$

Démonstration. Montrons $(bq+r) \wedge b = b \wedge r$. Soit $d = (bq+r) \wedge b$ et $d' = b \wedge r$.
On a : $d|bq + r$ et $d|b$ donc $d|r$ d'où $d|r = (bq + r) - bq$ donc $d|d'$.
De plus : $d'|b$ donc $d'|bq$ et $d'|r$ donc $d'|bq + r$ d'où $d'|d$.
Finalement, on a bien $d = d'$.

□

Ceci implique que si $d = bx + (a \bmod b)y'$ alors $d = ax + by$ avec $x = y'$ et $y = x' - \lfloor a/b \rfloor y'$.

Démonstration. On a en effet d'après le théorème de Bezout et l'égalité (18) :

$$\begin{aligned} d &= bx' + (a \bmod b)y' \\ &= bx' + (a - \lfloor a/b \rfloor b)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y') \end{aligned}$$

□

On a de plus la condition d'arrêt de l'algorithme en posant

$$d = a \wedge 0 = a \wedge 1 = a$$

```
1   struct couple
    {
            largeint x;
            largeint y;
5   };

    couple Bezout(largeint a, largeint n)
    {
            couple cRet;
10          largeint tmp;

            if (b == 0)
            {
                    cRet.x = 1;
15                  cRet.y = 0;
                    return cRet;
            }
            cRet = Bezout(b, mod(a, b));
            tmp = cRet.y;
20          cRet.y = cRet.x - (a / b) * cRet.y;
            cRet.x = tmp;
            return cRet;
    }

25  largeint invModN(largeint a, largeint n)
```

```
{
        return mod((Bezout(a, n)).x, n);
}
```

5.1.4 Le ppcm$(1, 2, \ldots, B)$

Pour des raisons de rapidité, dans la pratique, on ne prend pas $k = \text{PPCM}(1, 2, \ldots, B)$ mais $k = \text{PPCM}(B, B-1)$:

```
1   largeint calc_k(largeint B)
    {
            return lcm(B, B - 1);
    }
```

5.1.5 La procédure principale

On va travailler sur les courbes elliptiques $E : y^2 \equiv x^3 + ax + b \pmod{n} \cup \mathcal{O}$. Le coefficient a étant fixé (c'est notre paramètre), on choisit b de sorte que $P = (1, 1)$ appartienne à $E : b = 1^2 - 1^3 - a \times 1 = -a$. On calcule alors kP pour `nb_essais` valeurs de a, puis on invcrémente B et on recommence jusqu'à ce que λ ne soit pas inversible dans le calcul de kP ce qui est signalé par la valeur `true` de la variable booléenne `error`. La variable `error_factor` contient alors la valeur du nombre qui n'a pas été inversible lors du calcul de λ.

```
1   #define B_incr          1
    #define a_incr          30
    #define nb_essais       40
    #define x_init          1
5   #define y_init          1

    largeint TrouveFacteur(largeint n, largeint B)
    {
            ec_point P, Q;
10          largeint k, tmp;
            int a_essais;
            bool nouvelle_courbe=false;

            error = false;
15          if ((n % 2) == 0)
            {
                    //Le facteur 2 a ete trouve
                    //...
                    return largeint(2);
20          }
            if ((n % 3) == 0)
            {
                    //Le facteur 3 a ete trouve
                    //...
25                  return largeint(3);
            }

            p = n;
            k = calc_k(B);
30          b = 1;
```

```
a = 1; a_essais = 0;

P.x = x_init; P.y = y_init;
while (1)
{
        b = (P.y * P.y) - (P.x * P.x * P.x) - (a * P.x);

        //PGCD(Delta, n) == 1 ?
        tmp = gcd(4 * a * a * a + 27 * b * b, n);
        while (tmp != 1)
        {
                if (tmp == n)
                {
                        a += a_incr;
                        b = (P.y * P.y) - (P.x * P.x * P.x) - (a * P.x);
                        tmp = gcd(4 * a * a * a + 27 * b * b, n);
                }
                else
                        return tmp;
        }
        if (a_essais > nb_essais)
                nouvelle_courbe = true;
        Q = k * P;
        //Lambda n'etait-il pas inversible ?
        if (error)
        {
                largeint g = gcd(error_factor, n);

                if(1 < g && g < n)
                {
                        //Impression des resultats
                        //...
                        return g;
                }
                else
                        nouvelle_courbe = true;
        }
        //On change de courbe
        if (nouvelle_courbe)
        {
                a = 1;
                a_essais = 0;
                B += B_incr;
                while (k == calc_k(B)) {B += B_incr;};
                k = calc_k(B);
        }
        else
        //On incremente a
        {
                a += a_incr;
                a_essais++;
        }
}
```

```
85          //Cette commande n'est jamais executee
            return largeint(1);
    }
```

5.2 Résultats

Voici quelques résultats renvoyés par notre programme. Il est à noter que le dernier facteur n'est jamais "trouvé" ; il faudrait pour cela implémenter un test de primalité. Ces tests on été effectués sous Windows 2000 sur un Pentium 4 cadencé à $1,5$ GHz et doté de 256 Mo de RAM.

5.2.1 $109849677793909 = 239633 \cdot 11131 \cdot 41183$

```
Nombre a factoriser : 109849677793909
B-lissite : 10487395

10:58:58

10:58:58
facteur : 11131
a : 151
b : -151
p : 109849677793909
B : 10487395
k : 109985443398630

10:58:59
facteur : 41183
a : 571
b : -571
p : 9868805839
B : 10487395
k : 109985443398630
```

5.2.2 $297401545550457017108 07 = 206083 \cdot 64849 \cdot 34729 \cdot 6407749$

```
Nombre a factoriser : 297401545550457017108 07
B-lissite : 54535001572

11:05:03

11:05:06
facteur : 34729
a : 511
b : -511
p : 297401545550457017108 07
B : 54535001572
k : 2974066396403507469612

11:05:20
facteur : 206083
a : 1
b : -1
p : 85634929167142783
```

```
B : 54535001634
k : 2974066403165847668322

11:06:08
facteur : 64849
a : 1
b : -1
p : 415536114901
B : 54535001634
k : 297406645519223945421O
```

5.2.3 $19480333860937071253 = 1562513 \cdot 6512647 \cdot 1914323$

```
Nombre a factoriser : 19480333860937071253
B-lissite : 4413785992

11:08:06

11:11:27
facteur : 6512647
a : 1
b : -1
p : 19480333860937071253
B : 4413789312
k : 19481536086311644032

11:13:28
facteur : 1562513
a : 1
b : -1
p : 2991154573699
B : 4413792774
k : 19481566647400822302
```

5.2.4 $13475501025457998797151 1 = 61494437 \cdot 42398497 \cdot 51684299$

```
Nombre a factoriser : 13475501025457998797151 1
B-lissite : 367091132971

18:47:46

19:03:32
facteur : 42398497
a : 1
b : -1
p : 13475501025457998797151 1
B : 367091143560
k : 13475590767982143833004O
```

5.2.5 Limites de l'implémentation

La gestion de la mémoire n'est pas optimale (ceci est lié à l'utilisation de la classe `largeint`) ; en effet la mémoire allouée pour les `largeint` (en particulier pour les `ec_point`) n'est désallouée qu'à la toute fin du programme. Au

bout d'un dizaine de minute la mémoire de l'ordinateur est saturée et le programme plante. C'est pourquoi dans la pratique nous n'avons pas pû réaliser de factorisation de nombre ayant des facteurs premiers de plus de 8 chiffres.

Une technique pour résoudre ce problème consisterait à untiliser des *smart pointers* qui sont des pointeurs dont on a surchargé l'opérateur `->`, ce qui permet de tenir en permanence un compte du nombre de références au pointeur et d'en appeler le destructeur (donc de libérer la mémoire qui lui a été allouée) lorsque ce nombre devient nul.

Bien d'autres optimisations sont possibles ; en particulier "linéariser" le code en enlevant les classes au détriment de la facilité de mise en œuvre et de la clarté du code.

Bibliographie

[1] Thomas Cormen, Charles Leiserson, Ronald Rivest. *Introduction à l'algorithmique*. Dunod, 1994.

[2] Johannes Buchmann. La factorisation des grands nombres. *Pour la science*, (251) : pages 88–96, septembre 1998.

[3] François Arnault. *Théorie des nombres et cryptographie*. Cours de DEA, Université de Limoges, mars 2000.
`http://www.unilim.fr/laco/perso/francois.arnault`.

[4] *Site de Certicom*.
`http://www.certicom.com/resources/ecc/ecc.html`.

[5] Marc Joye. *Une introduction élémentaire à la théorie des courbes elliptiques*. Technical report, Université catholique de Louvain, juin 1995.
`http://www.dice.ucl.ac.be/crypto`.

[6] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. Thèse, LIX – CNRS, juin 1997.
`http://www.medicis.polytechnique.fr/~lercier/preprints`.

[7] Douglas Stinson. *Cryptographie – Théorie et pratique*, chapître 5, pages 159–170. International Thomson publishing, 1995.

Réalisé à l'aide de LaTeX.