Les points rationnels des courbes elliptiques

Théophile Hontang

12 mars 2017

Table des matières

Introduction

I Géométrie et Arithmétique

I.1 Groupe des Rationnels

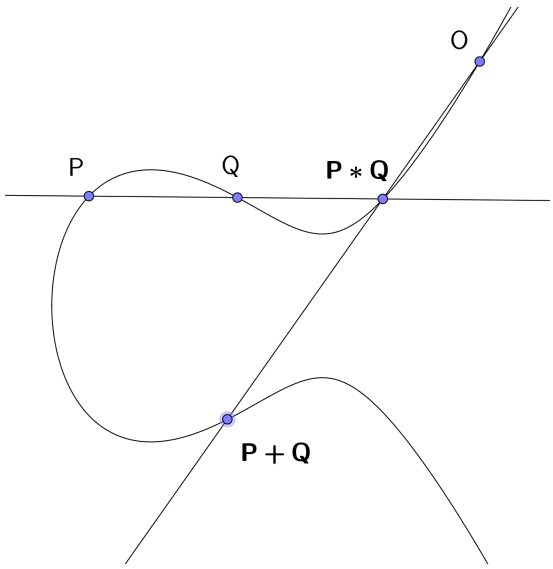

FIGURE 1 – Loi d'addition

On note $I(C_1 \cap C_2, P)$ la multiplicité de P, point d'intersection de $C_1 \cap C_2$

Théorème 1 (Bézout)**.** *Soit C_1 et C_2 deux courbes projectives avec des composantes non communes. Alors :*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = (\deg C_1)(\deg C_2)$$

Soit C une courbe elliptique. Elle est donnée par une équation de la forme $F(X, Y, Z) = 0$ où F est un polynôme homogène de degré 3. Nous verrons dans la prochaine section qu'une réduction est possible (dite de Weierstrass).
Soit $L \in \mathbb{P}^2$ une droite. Par le théorème de Bézout, L intersecte C en trois points(Ces points ne sont pas forcément distincts).
Définissons la loi de composition $+$ de C par la règle suivante.

Loi de Composition 1. *Soient $P, Q \in C$, L la droite joignant P et Q (ou la tangente si $P = Q$), et $P * Q$ le troisième point d'intersection de L par C. Soit L' la droite joignant $P * Q$ et O. Alors $P + Q$ est le point tel que L' intersecte C aux points $P * Q$, O et $P + Q$. C'est à dire :*

$$P + Q = O * (P * Q)$$

Proposition 1. *C, muni de la loi de composition $+$, est un groupe abélien avec O comme élément neutre. E vérifie alors les propriétés suivantes :*

1. *Si L intersecte C aux points P, Q et R alors*

$$(P + Q) + R = O$$

2. $\forall P \in C$,
$$P + O = P$$
3. $\forall P, Q \in C$
$$P + Q = Q + P$$
4. *Soit* $P \in C$*.Il existe un point, qu'on note* $-P$*, tel que*
$$P + (-P) = O$$
5. *Soit* $P, Q, R \in C$*. Alors*
$$(P + Q) + R = P + (Q + R)$$

Démonstration. 1. Trivial par la loi de composition.

2. (*Voir Figure 2) L et L′ coïncident. L intersecte C aux points* P, O, R *et L′ intersecte C aux points* $P + O, O, R$ *d'où* $P + O = P$.
3. *Par construction.*
4. *(Voir Figure 2) La droite, qui passe par P et O, intersecte C au point qu'on nomme R. En utilisant 1) et 2), nous obtenons*
$$O = (P + O) + R = P + R$$
5. *(Voir Figure 3)*

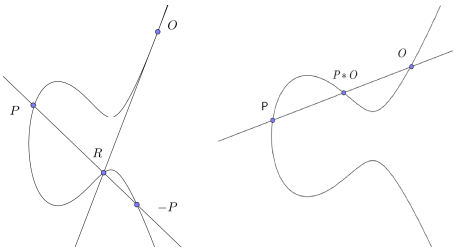

FIGURE 2 – Opposé et Élément neutre

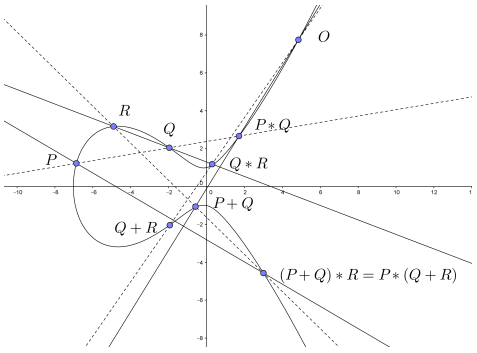

FIGURE 3 – Associativité

□

I.2 Weierstrass et formule de duplication

Une courbe elliptique C est donnée par $F(x,y) = 0$ où $\deg_x F = \deg_y F = 3$. Nous nous plaçons dans le plan projectif $\mathbb{P}^2$. L'idée est de réaliser une transformation projective pour réduire la forme de F. Pour cela, prenons un point rationnel $\mathcal{O}$ sur C. Soit $Z = 0$ la tangente de C en $\mathcal{O}$. Cette droite coupe C en un autre point qu'on nomme P. Soit $X = 0$ la tangente de C en P, elle coupe C en un point Q. On choisit $Y = 0$ une droite qui passe par $\mathcal{O}$ mais différent de $Z = 0$. En posant $x = X/Z$ et $y = Y/Z$, on obtient une transformation projective et l'équation est alors de la forme dite de Weierstrass :

$$F : y^2 = ax^3 + bx^2 + cx + d$$

Le lecteur pourra se reporter sur le livre [Silverman, 2009] pour les calculs.
La loi du groupe sur la forme de Weierstrass reste identique à celle vue précédemment. Dans ce cas , l'élément neutre $\mathcal{O}$ est un point à l'infini. Le point $P * Q = (x, y)$, défini comme précédemment, donne le point $P + Q = (x, -y)$, point symétrique par rapport à un axe. Nous remarquons alors que si $P = (x, y) \in C$ alors $-P = (x, -y) \in C$.

Proposition 2 (Formule de Duplication)**.** *Soit C une courbe elliptique de la forme de Weierstrass $(C) : y^2 = x^3 + ax^2 + bx + c$.*

1. *Soient $P_i = (x_i, y_i) \in C$ pour $i \in \{1, 2\}$. alors $P_1 + P_2 = (x_3, y_3)$ avec*

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad y_3 = \lambda x_3 + \nu \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

2. *Soit $P_0 = (x_0, y_0) \in C$. Alors la coordonnée en x de $2P$ est :*

$$x(2P) = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}$$

Démonstration. 1) Soient $P_1 * P_2 = (x_*, y_*)$. La droite joignant P_1 et P_2 est définie par l'équation $y = \lambda x + \nu$ avec $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ et $\nu = y_1 - \lambda x_1$. L'intersection de cette droite avec C est définie par :

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$$

Les trois racines de ce polynôme sont x_1, x_2 et x_*. Par les relations de Viète qui expriment les coefficients du polynôme par les racines, nous obtenons :

$$a - \lambda^2 = -(x_1 + x_2 + x_3)$$

Comme $x_3 = x_*$ et $y_3 = -y_*$, nous obtenons bien les coordonnées de $P_1 + P_2$.
2) $P * P$ est obtenu par l'intersection de C et de la tangente de C en P. La pente est $\lambda = \frac{dy}{dx}(P_0) = \frac{f'(x_0)}{2y_0}$. En substituant λ dans les équations obtenues en 1) et en remplaçant y^2 par $x^3 + ax^2 + bx + c$, nous obtenons le résultat.

□

I.3 Poins d'ordre fini

Définition 1. *Un point P est d'ordre fini m si*

$$mP = \underbrace{P + ... + P}_{m fois} = \mathcal{O}$$

Sinon P est d'ordre infini.

Définition 2. *Soit C une courbe cubique donnée par*

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

est dite **non − singuliere** *si f et f' ont aucune racine commune ; i.e f n'admet que des racines simples.*

Théorème 2 (Points d'ordre 2 et 3)**.** *Soit C une courbe cubique non-singulière donnée par* (2)

1. *Un point $P = (x, y)$ sur C est d'ordre 2 ssi $y = 0$.*
2. *C a quatre points d'ordre divisant 2. Ces quatre points forment un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*
3. *Un point $P = (x, y)$ est d'ordre 3 ssi x est racine du polynôme :*

$$\chi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$$

4. *C a neuf points d'ordre divisant 3. Ces neuf points forment un groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Démonstration. □

Théorème 3 (Nagell-Lutz [Lutz, 1937] [Nagell, 1935])**.** *Soit*

$$y^2 = x^3 + ax^2 + bx + c$$

une courbe cubique non-singulière avec $a, b, c \in \mathbb{N}$ et D le discriminant ; i.e

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3$$

Soit $P = (x, y)$ un point rationnel d'ordre fini.
Alors $x, y \in \mathbb{N}$ et soit P est d'ordre 2, soit y divise D.

Théorème 4 ([Mazur, 1977] [Mazur, 1978])**.** *Soit C une courbe cubique rationnel non-singulière, et supposons que $C(\mathbb{Q})$ contient un point d'ordre fini m. Alors*

$$1 \leqslant m \leqslant 10 \quad ou \quad m = 12$$

Dans la prochaine section, nous allons montrer que $C(\mathbb{Q})$ est de type fini, i.e $C(\mathbb{Q}) \simeq \mathbb{Z}^r \times C(\mathbb{Q})_{tors}$ où r est le rang de la courbe. Le sous-groupe de torsion $C(\mathbb{Q})_{tors}$ peut alors être identifié à quinze groupes :

$$\mathbb{Z}/n\mathbb{Z} \quad 0 \leqslant n \leqslant 10 \quad ou \quad n = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad 1 \leqslant n \leqslant 4$$

II Théorème de Mordell-Weil

Théorème 5 ([Mordell, 1922]). *Soit C une courbe elliptique définie par l'équation*

$$C : y^2 = x^3 + ax^2 + bx$$

avec $a, b \in \mathbb{N}$. Alors $C(\mathbb{Q})$ est un groupe abélien de type fini.

Démonstration.

Théorème 6 (Descente). *Soit Γ un groupe commutatif et soit la fonction*

$$h : \Gamma \to [0, \infty]$$

vérifiant les propriétés suivantes :

1. *Quelque soit M réel, $\{P \in \Gamma : h(P) \leqslant M\}$ est fini*
2. *Quelque soit P_0 point de Γ, il existe κ_0 tel que*

$$h(P + P_0) \leqslant 2h(P) + \kappa_0 \quad \forall P \in \Gamma$$

3. *Il existe une constante κ telle que :*

$$h(2P) \geqslant 4h(P) - \kappa \quad \forall P \in \Gamma$$

4. *$|\Gamma : 2\Gamma|$ est fini*

Alors Γ est de type fini

Démonstration. D'après 4), il existe un nombre fini de représentants de classe de $\Gamma/2\Gamma$ qu'on note $Q_1, Q_2, ..., Q_n$. Cela signifie que pour tout $P \in \Gamma$, il existe un indice i_1, dépendant de P, tel que $P - Q_{i_1} \in 2\Gamma$. On peut alors noter $P - Q_{i_1} = 2P_1$ pour $P_1 \in \Gamma$. En procédant de même, on peut écrire :

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

où $Q_{i_1}, ..., Q_{i_m}$ sont choisis parmi les représentants $Q_1, ..., Q_n$ et $P_1, ..., P_m \in \Gamma$. En substituant la j-ème ligne dans la(j-1)-ème ligne, et par une rapide récurrence, nous obtenons :

$$P = Q_{i_1} + 2Q_{i_2} + ... + 2^{m-1}Q_{i_m} + 2^m P_m \tag{1}$$

Nous allons appliquer la méthode de descente infinie dans le but de contrôler P_m par la hauteur. Par 2), $h(P - Q_i) \leqslant 2h(P) + \kappa_i \leqslant 2h(P) + \kappa'$ pour tout $P \in \Gamma$ et $\kappa' = \max\limits_{1 \leqslant j \leqslant n} k_j$. Par 3), pour tout $j \in [\![1, n]\!]$

$$4h(P_j) \leqslant h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leqslant 2h(P_{j-1}) + \kappa' + \kappa$$

$$h(P_j) \leqslant \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa))$$

Si $(*)h(P_{j-1}) \geqslant \kappa' + \kappa$ alors $h(P_j) \leqslant \frac{3}{4}h(P_{j-1})$. Tant que la condition $(*)$ est vraie, le prochain point dans la suite $P_1, ..., P_n$ possède une hauteur plus petite. Il existe un indice m tel que $h(P_m) \leqslant \kappa' + \kappa$. Ainsi, l'ensemble

$$\{Q_1, Q_2, ..., Q_n\} \cup \{P \in \Gamma; h(P) \leqslant \kappa' + \kappa\}$$

engendre Γ. Par 1) et 4), l'ensemble est fini d'où Γ est de type fini. □

Définition 3. *Soit $t \in \mathbb{Q}$ et $t = p/q$ avec $pgcd(p, q) = 1$.*
*La **hauteur** $H(t)$ de t est défini par*

$$H(t) = max\{|p|, |q|\}$$

Définition 4. *La **hauteur** sur $C(\mathbb{Q})$ est la fonction :*

$$h : C(\mathbb{Q}) \to \mathbb{R}$$

$$h(P(x, y)) = log(H(x))$$

La hauteur fera office de fonction et $C(\mathbb{Q})$ de groupe commutatif dans le théorème de la descente. Les quatre hypothèses sur h sont démontrés ci-dessous et ainsi le théorème de Mordell sera démontré.

Lemme 1. *L'ensemble des rationnels, dont la hauteur est plus petit qu'un nombre fixé, est un ensemble fini.*
$\forall M \in \mathbb{R}, \{P \in \Gamma : h(P) \leqslant M\}$ *est fini*

Démonstration. Si $x = \frac{m}{n}$ est plus petite qu'une constante, alors $\mid m \mid$ et $\mid n \mid$ sont plus petites que cette constante donc il existe un nombre fini de possibilités pour m et n. □

Lemme 2. $\forall P_0 \in \Gamma$, *il existe κ_0 (dépendant de P_0, a, b, c) tel que*

$$h(P + P_0) \leqslant 2h(P) + \kappa_0 \quad \forall P \in \Gamma \tag{2}$$

Démonstration. Par des opérations élémentaires, on peut montrer que chaque point rationnel $P = (x, y)$ peut être mis sous la forme suivante :

$$x = \frac{m}{e^2} \qquad y = \frac{n}{e^3} \qquad e, m, n \in \mathbb{N}^* \tag{3}$$

avec $pgcd(e, m) = 1$ et $pgcd(e, n) = 1$.
En la mettant dans l'équation de la cubique, on a :

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

En utilisant le fait que : $\mid m \mid \leqslant H(P)$ et $e^2 \leqslant H(P)$ et par l'inégalité triangulaire, on a :

$$|n^2| \leqslant KH(P)^3 \qquad K = \sqrt{1 + |a| + |b| + |c|}. \tag{4}$$

Supposons que $P = (x, y) \notin \{P_0, -P_0, \mathcal{O}\}$ avec $P_0 = (x_0, y_0)$ et que $P + P_0 = (\xi, \eta)$. La formule de duplication nous donne :

$$\xi + x + x_0 = \left(\frac{y - y_0}{x - x_0}\right)^2 - a$$

$$\iff \xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$$

avec $A, B, C, D, E, F, G \in \mathbb{N}$. D'où $H(\xi) \leqslant max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}$ Par les inégalités obtenues en et ,

$$H(P + P_0) = H(\xi) \leqslant max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2$$

En appliquant la fonction logarithme, on a bien le résultat avec $\kappa_0 = log(max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\})$ □

Lemme 3. *Il existe une constante κ(dépendant de a, b, c) tel que :*

$$h(2P) \geqslant 4h(P) - \kappa \quad \forall P \in \Gamma \tag{5}$$

Démonstration. Soit $P = (x, y)$ un point qui n'est pas d'ordre 2 et $2P = (\xi, \eta)$. *Formule de duplication*

$$\xi + 2x = \Big(\frac{f'(x)}{2y}\Big)^2 - a$$

$$\xi = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + ...}{4x^3 + ...}$$

ξ est le quotient de deux polynômes qui n'ont aucune racine complexe commune car C est non-singulière.
Comme $h(P) = h(x)$ et $h(2P) = h(\xi)$, nous allons prouver

$$h(\xi) \leqslant 4h(x) - \kappa$$

SubLemma 1. *Soit ϕ et ψ des polynômes à coefficients entiers et aucune racine complexe commune. Soit $d = max(deg(\phi), deg(\psi))$*

i) Il existe un entier $R \geqslant 1$ dépendant de ϕ et ψ telle que, pour tout rationnel m/n,

$$pgcd\Big(n^d\phi\Big(\frac{m}{n}\Big), n^d\psi\Big(\frac{m}{n}\Big)\Big) \mid R$$

ii) Ils existent des constantes κ_1 et κ_2 (dépendant de ϕ et ψ) telle que, pour tout rationnel m/n,

$$dh\Big(\frac{m}{n}\Big) - \kappa_1 \leqslant h\Big(\frac{\phi(m/n)}{\psi(m/n)}\Big)$$

Démonstration. Posons $deg(\phi) = d$ et $deg(\psi) = e \leqslant d$. On peut écrire

$$n^d\phi\Big(\frac{m}{n}\Big) = a_0nm^d + a_1m^{d-1} + ... + a_nn^d$$
$$n^d\psi\Big(\frac{m}{n}\Big) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e-1} + ... + b_en^d$$

On va poser $\Phi(m, n) = n^d\phi\Big(\frac{m}{n}\Big)$ et $\Psi(m, n) = n^d\psi\Big(\frac{m}{n}\Big)$ Comme ψ et ϕ n'ont pas de racines communes, ils sont premiers dans l'anneau euclidien $\mathbb{Q}[X]$. Il existe alors deux polynômes F et G de $\mathbb{Q}[X]$ tels que

$$F(X)\phi(X) + G(X)\psi(X) = 1$$

Soit A un entier tel que $AG(X)$ et $AF(X)$ soient à coefficients entiers. Soit $D = max(deg(F), deg(G))$. En évaluant en $X = m/n$

$$n^DAF\Big(\frac{m}{n}\Big) * n^d\phi\Big(\frac{m}{n}\Big) + n^DAG\Big(\frac{m}{n}\Big) * n^d\psi\Big(\frac{m}{n}\Big) = An^{D+d}$$

$\gamma = pgcd(\Phi(m,n), \Psi(m,n)) \mid An^{D+d}$ Comme γ divise $\Phi(m,n)$, γ divise aussi :

$$An^{D+d-1}\Phi(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + ... + Aa_dn^{D+2d-1}$$

Chaque terme contient An^{D+d} et on vient de prouver que γ divise An^{D+d}. Alors γ divise $Aa_0m^dn^{D+d-1}$. Ensuite

$$\gamma \quad divise \quad pgcd(Aa_0m^dn^{D+d-1}, An^{D+d})$$

Comme m et n sont premiers entre eux, γ divise $Aa_0m^dn^{D+d-1}$. En utilisant le fait que γ divise $Aa_0m^dn^{D+d-2}\Phi(m,n)$ et en répétant les mêmes arguments, γ divise $Aa_0^2m^dn^{D+d-2}$. Par récurrence, on arrive à la conclusion suivante : γ divise Aa_0^{d+D}, ce qui montre *i)*.
Pour *ii)*, en continuant avec les notations de *i)*,

$$\xi = \frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{\Phi(m,n)}{\Psi(m,n)}$$

D'après *ii)*, il existe un entier $R \geqslant 1$ tel que $pgcd(\Phi(m,n), \Psi(m,n))$ divise R. On a :

$$\begin{aligned} H(\xi) &\geqslant \frac{1}{R} max\{\mid \Phi(m,n) \mid, \mid \Psi(m,n) \mid\} \\ &\geqslant \frac{1}{2R}\Big(\mid n^d\phi\Big(\frac{m}{n}\Big) \mid + \mid n^d\psi\Big(\frac{m}{n}\Big) \mid \Big) \end{aligned}$$

Ce qui équivaut à :

$$\frac{H(\xi)}{H(m/n)^d} \geqslant \frac{1}{2R}\frac{\mid n^d\phi\left(\frac{m}{n}\right) \mid + \mid n^d\psi\left(\frac{m}{n}\right) \mid}{max\{\mid m \mid^d, \mid n \mid^d}} = \frac{1}{2R}\frac{\mid \phi\left(\frac{m}{n}\right) \mid + \mid \psi\left(\frac{m}{n}\right) \mid}{max\{\mid \frac{m}{n} \mid^d, 1\}}$$

Considérons la fonction d'une variable réelle :

$$p(t) = \frac{\mid \phi(t) \mid + \mid \psi(t) \mid}{max\{\mid t^d, 1\}}$$

Comme ϕ est de degré d et ψ de degré au moins d, les limites en l'infini de p ne sont pas nulles. Dans un intervalle fermé, p est continue donc atteint ses bornes. Comme la fonction ne s'annule jamais (ϕ et ψ n'ont pas de racines communes), il existe une constante $C_1 > 0$ telle que $p(t) \geqslant C_1$ pour tout t. En utilisant l'inégalité précédente, on peut dire :

$$H(\xi) \geqslant \frac{C_1}{2R}H\Big(\frac{m}{n}\Big)^d$$

Par l'image du logarithme, on arrive au résultat avec $\kappa_1 = log(2R/C_1)$ □

Le Lemme 3 est un cas particulier de Sublemma 1. □

Lemme 4 (Mordell-Weil Faible)**.** $|C(\mathbb{Q}) : 2C(\mathbb{Q})|$ *est fini.*

Démonstration. Posons $\Gamma = C(\mathbb{Q})$. Soient $C : y^2 = f(x) = x^3+ax^2+bx+c$. Supposons que f ait une racine rationnel x_0. Comme f est un polynômes à coefficients entiers, par le théorème de Nagell-Lutz, x_0 est entier. Par un changement de coordonnées, on peut déplacer le point $(x_0, 0)$ à l'origine. C est alors de la forme : $y^2 = x^3 + ax^2 + bx$. Soient $T = (0,0)$, $\overline{C} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$ avec $\overline{a} = -2a$ et $\overline{b} = a^2 - 4b$.

Proposition 3. *On considère les applications suivantes :*

$$\phi((x,y)) = \Big(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\Big) \qquad \psi((\overline{x},\overline{y})) = \Big(\frac{\overline{y}^2}{\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{\overline{x}^2}\Big)$$

et $\phi(\mathcal{O}) = \phi(T) = \overline{\mathcal{O}}$ *et* $\psi(\overline{\mathcal{O}}) = \psi(\overline{T}) = \mathcal{O}$.

1. $\phi : C \to \overline{C}$ *et* $\psi : \overline{C} \to C$ *sont des homomorphismes.*
2. $\psi \circ \phi(P) = 2P$

Démonstration. 1. Plusieurs cas sont à distinguer. Si l'un des points est $\mathcal{O}$, il n'y a rien à prouver. Si l'un des points est T, en utilisant la loi d'addition, on a pour $P = (x, y)$

$$P + T = \Big(\frac{b}{x}, -\frac{by}{x^2}\Big)$$

En les remettant dans l'application ϕ, nous obtenons bien : $\phi(P+T) = \phi(P)$. Par un calcul rapide, on obtient que ϕ envoie les inverses sur les inverses. $\phi(-P) = \phi(x,-y) = -\phi(x,y) = -\phi(P)$. Si nous supposons que $P_1+P_2+P_3 = \mathcal{O}$ $(P_1, P_2, P_3 \neq T)$ et en réalisant l'intersection de la droite passant par ces trois points et la courbe, on peut alors montrer que $\phi(P_1)+\phi(P_2)+\phi(P_3) = \overline{\mathcal{O}}$. Ce qui montre que $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$ et donc que ϕ est un homomorphisme En posant $\overline{\overline{C}} : y^2 = x^3 + 4ax^2 + 16bx$, il est clair que $\overline{\overline{C}} \simeq C$. Nous pouvons alors associer $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$ à ψ d'où ψ est un homomorphisme.

2. Le point $2P$ est donnée par la formule de duplication vu dans la section précédente. Les calculs de $\psi \circ \phi(P)$ sont laissés au lecteur.

□

Proposition 4. *1.* $\overline{\mathcal{O}} \in \phi(\Gamma)$

2. $\overline{T} = (0,0) \in \phi(\Gamma)$ *ssi* $\overline{b} = a^2 - 4b$ *est un carré parfait.*

3. $\overline{P} \in \phi(\Gamma)$ *ssi* $\overline{x}$ *est le carré d'un rationnel.*

Démonstration. 1) Trivial par $\phi(\mathcal{O}) = \overline{\mathcal{O}}$.
2) $\overline{T} = (0,0) \in \phi(\Gamma)$ ssi $x(x^2 + ax + b) = 0$ et $x^2 + ax + b$ n'admet qu'une racine rationnelle ssi le discriminant $a^2 - 4b$ est un carré parfait.
3) Si $\overline{P} = (\overline{x}, \overline{y}) \in \phi(\Gamma)$, par la définition de *phi*, $\overline{x} = y^2/x^2$ qui est le carré d'un rationnel. Supposons maintenant que $\overline{x} = \omega^2$ avec $\omega \in \mathbb{Q}$. Comme le noyau de ϕ contient deux éléments, deux points de Γ correspondent au point $\overline{P} = (\overline{x}, \overline{y}) \in \phi(\Gamma)$. Les points $P_i = (x_i, y_i)$ avec $i \in \{1, 2\}$ données par :

$$\begin{cases} x_1 &= \frac{1}{2}\Big(\omega^2 - a + \frac{\overline{y}}{\omega}\Big) \\ y_1 &= x_1\omega \end{cases} \qquad \begin{cases} x_2 &= \frac{1}{2}\Big(\omega^2 - a - \frac{\overline{y}}{\omega}\Big) \\ y_2 &= -x_2\omega \end{cases}$$

sont sur C et $\phi(P_i) = (\overline{x}, \overline{y})$, ce qui conclut la démonstration. □

Proposition 5. *Soit* $\mathbb{Q}^{*2} = \{p^2; p \in \mathbb{Q}^*\}$

1. $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ *donnée par*

$$\alpha(\mathcal{O}) = [1] \quad \alpha(T) = [b] \quad \alpha(x,y) = [x]$$

est un homomorphisme et $\ker(\alpha) = \Psi(\overline{\Gamma})$

2. *Soient $p_1, p_2, ..., p_t$ les premiers divisant b. Alors :*

$$\Gamma/\psi(\overline{\Gamma}) \simeq \alpha(\Gamma) \subset \{p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t}, \epsilon_i = 0, 1\}$$

3. $|\Gamma : \psi(\bar{\Gamma})| \leqslant 2^{t+1}$
4. $|\Gamma : 2\Gamma| \leqslant |\Gamma : \psi(\overline{\Gamma})||\overline{\Gamma} : \phi(\Gamma)|$

Démonstration. 1) Comme $\alpha(-P) = \alpha(x, -y)$, nous avons que :

$$\alpha(-P) = x = \frac{1}{x}x^2 \equiv \frac{1}{x} = \frac{1}{\alpha(P)}[\mathbb{Q}^{*2}]$$

α envoie les inverses sur les inverses. Nous allons procédé de la même manière que la proposition 2. Supposons que $P_1 + P_2 + P_3 = \mathcal{O}$. En intersectant C avec une droite et en utilisant la formule de Viète, nous obtenons :

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = \nu^2 \equiv [\mathbb{Q}^{*2}]$$

ce qui montre le résultat si P_1, P_2, P_3 sont différents de $\mathcal{O}$. Les autres cas sont laissés au lecteur. $\ker(\alpha) = \Psi(\overline{\Gamma})$ n'est qu'une conséquence de la proposition 3.
2) L'isomorphisme est dû au théorème de l'isomorphie. Nous avons vus dans lemme 2 que les points rationnels peuvent être mis sous la forme $x = m/e^2$ et $y = n/e^3$. En substituant dans C, nous obtenons

$$n^2 = m(m^2 + ame^2 + be^4)$$

Comme m et e sont premiers entre eux, $pgcd(m, m^2 + ame^2 + be^4)$ divise b. Alors m est de la forme $m = \pm(entier)^2 p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t}$ avec $\epsilon_i = 0$ ou 1. Et :

$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t} [\mathbb{Q}^{*2}]$$

ce qui nous montre bien le résultat.
3) C'est une conséquence directe de 2) : $|\Gamma : \psi(\overline{\Gamma})| \leqslant \#\{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t}\} = 2^{t+1}$
4) Soit $\gamma \in \Gamma$. Soient $\gamma_1, ..., \gamma_n$ des représentants des classes de $\psi(\overline{\Gamma})$ dans Γ. Il existe des γ_i tels que $\gamma - \gamma_i = \psi(\bar{\gamma})$. Soient $\bar{\gamma_1}, ..., \bar{\gamma_n}$ des représentants des classes de $\phi(\Gamma)$ dans $\overline{\Gamma}$. Il existe des $\bar{\gamma_j}$ tels que $\bar{\gamma} - \bar{\gamma_j} = \phi(\gamma')$. On a : $\gamma = \gamma_i + \psi(\bar{\gamma_j} + \phi(\gamma'))$ En utilisant la proposition 1), on a :

$$\gamma = \gamma_i + \psi(\bar{\gamma_j}) + 2\gamma'$$

d'où le résultat. □

De même, $|\overline{\Gamma} : \phi(\Gamma)| < \infty$ et donc par 4), $|\Gamma : 2\Gamma| < \infty$. □

□

III Cryptographie

Data: n
Result: p tel que p divise n
$a := 2$ ou un nombre compris entre 2 et $n - 2$.
k une borne
for d *from* 2 *to* k **do**
  $b := a^d \mod n$
  $p := pgcd(b - 1, n)$
  if $p > 1$ **then**
    return p
  end
end

Algorithm 1: Algorithme p-1 de Pollard

Data: n
Result: p tel que p divise n
$a := 2$ ou un nombre compris entre 2 et $n - 2$.
k une borne
for d *from* 2 *to* k **do**
  $b := a^d \mod n$
  $p := pgcd(b - 1, n)$
  if $p > 1$ **then**
    return p
  end
end

Algorithm 2: ECM (Elliptic Curve factorization Method)

[?]

Conclusion

A Bibliographie

Références

[Lutz, 1937] Lutz, E. (1937). Sur l'équation $y^2 = x^3 - ax - b$ dans les corps p-adic. *J.Reine Angew. Math.177*, pages 237–247.

[Mazur, 1977] Mazur, B. (1977). Modular curves and the einsenstein ideal. *IHES Publ. Math. 47*, pages 33–186.

[Mazur, 1978] Mazur, B. (1978). Rational isogenies of prime degree. *Invent. Math. 44*, pages 129–162.

[Mordell, 1922] Mordell, L. (1922). On the rational solutions of the indetermine equations of the third and fourth degrees. *Proc. Camb. Philos. Soc. 21*, pages 179–192.

[Nagell, 1935] Nagell, T. (1935). Solutions de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. *Wid. Acad. Skrifter Oslo I.*

[Silverman, 2009] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. Springer.

[Silverman, 2013] Silverman, J. H. (2013). *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer.

[Tate and Silverman, 2015] Tate, J. T. and Silverman, J. H. (2015). *Rational Points on Elliptic Curves*. Springer.

Sites Internet :
math.lsa.umich.edu/wfulton/CurveBook.pdf
culturemath.ens.fr/maths/pdf/nombres/gaertner-2008.pdf