Correction feuille 6

1 Nombres premiers

Exercice 1. ***Postulat de Bertrand****: on va montrer que pour tout $n \geq 1$, il existe un nombre premier p tel que $n < p \leq 2n$.*

(1) Montrer que pour tout $m \geq 1$, on a

$$\prod_{m+1<p\leq 2m+1} p \leq C_{2m+1}^{m} \leq 2^{2m}$$

Pour tout x soit $q = 2m+1$ le plus grand nombre premier tel que $q \leq x$. Montrer que

$$\prod_{p\leq x} p = \prod_{p\leq q} p \leq 4^{2m} \leq 4^{x-1}$$

(2) Montrer que $n!$ s'écrit sous la forme $p^{v_p(n)}m$ avec p ne divisant pas m et

$$v_p(n) = \sum_{k\geq 1} \lfloor \frac{n}{p^k} \rfloor$$

que l'on appelle la valuation p-adique de n. En déduire que la valuation p-adique de C_{2n}^{n} est

$$\sum_{k\geq 1} \lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor) \leq \max\{r : p^r \leq 2n\}$$

(3) Montrer que pour $p > \sqrt{2n}$, $v_p(C_{2n}^{n}) \leq 1$ et que pour $\frac{2n}{3} < p \leq n$, $v_p(C_{2n}^{n}) = 0$.

(4) Pour $n \geq 3$, montrer que $\frac{4^n}{2n} \leq C_{2n}^{n}$ et en déduire que

$$4^n \leq (2n)^{1+\sqrt{2n}} \prod_{\sqrt{2n}<p\leq \frac{2n}{3}} p \prod_{n<p\leq 2n} p$$

(5) On suppose qu'il n'y a pas de nombre premier p tel que $n < p \leq 2n$. En déduire que $4^{n/3} \leq (2n)^{1+\sqrt{2n}}$. En utilisant la relation $a + 1 < 2^a$, en déduire que $n < 4000$.

(6) Conclure en considérant la suite

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

(7) Montrer que pour $n \geq 4000$, on a

$$\prod_{n<p\leq 2n} p \geq 2^{n/30}$$

et en déduire qu'il y a au moins $\log_{2n}(2^{n/30}) = \frac{1}{30}\frac{n}{\log_2 n+1}$ nombres premiers dans l'intervalle compris entre n et $2n$.

(8) Pouvez-vous commenter ce dernier résultat?

Preuve : (1) On a $C_{2m+1}^m = \frac{(2m+1)!}{m!(m+1)!}$ et tous les nombres premiers p tels que $m+1 < p \leq 2m+1$ sont clairement des facteurs du numérateurs et pas du dénominateur, d'où la première inégalité. En outre $C_{2m+1}^m = C_{2m+1}^{m+1}$ sont deux termes qui apparaissent dans la somme de termes positifs

$$\sum_{k=0}^{2m+1} C_{2m+1}^k = 2^{2m+1}$$

d'où la deuxième inégalité.

On a clairement $\prod_{p\leq x} p = \prod_{p\leq q} p = \prod_{p\leq m+1} p . \prod_{m+1<p\leq 2m+1} p$. La dernière inégalité découle alors aisément de $\prod_{p\leq m+1} p \leq 4^m$ que l'on peut montrer par exemple par récurrence.

(2) Il y a exactement $\lfloor \frac{n}{p} \rfloor$ termes parmi les facteurs de $n! = 1.2.3 \cdots n$ qui sont divisibles par p et qui fournissent donc $\lfloor \frac{n}{p} \rfloor$ p-facteurs. Il y a $\lfloor \frac{n}{p^2} \rfloor$ termes parmi les facteurs de $n!$ qui sont divisibles par p^2: ceux-ci sont déjà comptés une fois dans le terme $\lfloor \frac{n}{p} \rfloor$, on doit donc rajouter simplement $\lfloor \frac{n}{p^2} \rfloor$ facteurs p...

Le calcul de la valuation p adique de C_{2n}^n découle alors simplement de son écriture $\frac{(2m)!}{m!m!}$. La majoration découle du fait que

$$\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor < \frac{2n}{p^k} - 2(\frac{n}{p^k} - 1) = 2$$

de sorte que chaque terme de la somme est au plus égale à 1.

(3) Si $p > \sqrt{2n}$ alors $\max\{r : p^r \leq 2n\} \leq 1$. Pour $\frac{2}{3}n < p \leq n$, on a $3p > 2n$ ce qui implique que p et $2p$ sont les euls multiples de p qui apparaissent comme facteurs du numérateur de $\frac{(2n)!}{n!n!}$ alors qu'il y a deux p-facteurs au dénominateur.

(4) A partir de l'égalité $C_n^k = \frac{n-k+1}{k} C_n^{k-1}$ il est facile de voir que pour tout n, les coefficients binomiaux forment une suite qui est symétrique: elle croît vers son milieu de sorte que les coefficients du milieu sont les plus grands. Ainsi C_{2n}^n est le plus grand des C_{2n}^k: ceux-ci ont pour somme 4^n et ont pour moyenne $\frac{4^n}{2n}$ de sorte que

$$C_{2n}^n \geq \frac{4^n}{2n}$$

Par ailleurs on a

$$\prod_{p\leq\sqrt{2n}} p \leq (2n)^{1+\sqrt{2n}}$$

car il y a au plus $1 + \sqrt{2n}$ nombre premiers $p \leq \sqrt{2n}$, d'où la deuxième inégalité.

(5) D'après (1) on a $\prod_{p\leq 2n/3} p \leq 4^{2n/3}$ de sorte que l'inégalité de (4) devient

$$4^n \leq (2n)^{1+\sqrt{2n}} 4^{2n/3}$$

soit $4^{n/3} \leq (2n)^{1+\sqrt{2n}}$ ce qui est faux quand n est suffisament grand. En utilisant $a + 1 < 2^a$, par récurrence, on obtient

$$2n = (\sqrt[6]{2n})^6 < (\lfloor \sqrt[6]{2n} \rfloor + 1)^6 < 2^{6\lfloor \sqrt[6]{2n} \rfloor} \leq 2^{6\sqrt[6]{2n}}$$

de sorte que si $n \geq 50$, et donc $18 < 2\sqrt{2n}$, on a

$$2^{2n} \leq (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}$$

ce qui implique $(2n)^{1/3} < 20$ et donc $n < 4000$.

(6) La suite donnée est une suite de nombre premiers tels que $p_{n+1} < 2p_n$; d'où le postulat de Bertrand pour tout n.

(7) L'inégalité s'obtient à partir de celle de (4) comme précédemment; l'estimation en découle directement.

(8) Le théorème des nombres premiers donne que grosso modo, le nombre de premiers compris entre n et $2n$ est $\frac{n}{\ln n}$. Le résultat obtenu dans (7) n'est donc pas si mauvais.

Exercice 2. ***Tchebycheff 1848-1850*** *Pour tout $x \in \mathbb{R}_+$, on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.*

(1) Montrer que pour tout $k \in \mathbb{N}$, $\pi(2^{k+1}) \leq 2^k$.

(2) Soit $p \leq 2n$ et r tel que $p^r \leq 2n < p^{r+1}$. Montrer que $v_p(C_{2n}^n) \leq r$ puis que

$$\prod_{n<p\leq 2n} p \mid C_{2n}^n \mid \prod_{p^r \leq 2n < p^{r+1}} p^r$$

En déduire que $n^{\pi(2n)-\pi(n)} < C_{2n}^n \leq (2n)^{\pi(2n)}$.

(3) Prouver que $2^n \leq C_{2n}^n \leq 2^{2n}$ et en déduire en prenant $n = 2^k$ que:

$$k\big(\pi(2^{k+1}) - \pi(2^k)\big) < 2^{k+1}$$

et que $2^k \leq (k+1)\pi(2^{k+1})$.

(4) Montrer que pour tout entier k:

$$\frac{1}{2}\frac{2^{k+1}}{k+1} \leq \pi(2^{k+1}) \leq 3\frac{2^{k+1}}{k+1}$$

(5) Soit $n > 1$ et k tel que $2^k \leq n < 2^{k+1}$. Montrer que

$$\frac{\log 2}{4}\frac{n}{\log n} \leq \pi(n) \leq 6\log 2\frac{n}{\log n}$$

(6) Application: montrer que

$$\sum_{p\leq n} \frac{\log p}{p} = \log n + \mathcal{O}(1)$$

Preuve : (1) Pour tout $k > 0$, en remarquant qu'un nombre premier distinct de 2 est impair, on obtient que parmi les $2^{k+1} - 2$ entiers $3, 4, \cdots, 2^{k+1}$, il y a au plus $2^k - 1$ nombres premiers, d'où le résultat en rajoutant 2.

(2) La majoration $v_p(C_{2n}^n) \leq r$ est donnée dans l'exercice précédent; on en déduit donc que C_{2n}^n divise $\prod_{p^r\leq 2n<p^{r+1}} p^r$. Par ailleurs si $n < p \leq 2n$ alors p divise $(2n)!$ mais pas $(n!)$ d'où la première divisibilité. Par ailleurs on a

$$\prod_{n<p\leq 2n} > n^{\pi(2n)-\pi(n)} \qquad \prod_{p^r\leq 2n<p^{r+1}} p^r < (2n)^{\pi(2n)}$$

d'où l'encadrement demandé.

(3) On rappelle que $\sum_{k=0}^{2n} C_{2n}^k = 4^n$ et donc $C_{2n}^n \leq 4^n$. Par ailleurs on a vu dans l'exercice précédent que C_{2n}^n est le plus grand des coefficients binomiaux dont la moyenne est $\frac{4^n}{2n} \geq 2^n$ d'où le résultat. En combinant ces inégalités avec celles de (2) on obtient

$$(2^k)^{\pi(2^{k+1})-\pi(2^k)} < 2^{k+1} \qquad 2^{2^k} \leq (2^{k+1})^{\pi(2^{k+1})} = 2^{(k+1)\pi(2^{k+1})}$$

d'où les inégalités

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1} \qquad 2^k \leq (k+1)\pi(2^{k+1})$$

(4) En additionnant $\pi(2^{k+1})$ à la première des inégalités de (3), on obtient

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3.2^k$$

d'après (1). On somme cette dernière égalité pour $k = 0, 1, \cdots, n$ ce qui donne:

$$(n+1)\pi(2^{n+1}) < 3.2^{n+1}$$

En utilisant la deuxième inégalité de (3), on obtient

$$\frac{1}{2}.\frac{2^{n+1}}{n+1} \leq \pi(2^{n+1}) < 3\frac{2^{n+1}}{n+1}$$

(5) On a $k \leq \frac{\log n}{\log 2}$ et $k+1 > \frac{\log n}{\log 2}$ et donc

$$\pi(n) \leq \pi(2^{k+1}) \leq 3\frac{2^{k+1}}{k+1} \leq 6\frac{2^k \log 2}{\log n}$$

et donc $\pi(n) \leq 6 \log 2 \frac{n}{\log n}$. De même on a

$$\pi(n) \geq \pi(2^k) \geq \frac{1}{2}\frac{2^k}{k} \geq \frac{1}{4}\frac{n \log 2}{\log n}$$

(6) On pose $T(n) = \sum_{k \geq n} \log k$ et comme log est croissante on a pour $k > 1$:

$$\int_2^{n-1} \log t dt \leq T(n) \leq \int_1^n \log t dt$$

de sorte que $T(n) = n \log n - n + \mathcal{O}(1)$. On a $T(n) = \log n! = \sum_{p \leq n} v_p(n!) \log p$ et donc $\frac{T(n)}{n} = \sum_{p \leq n} \frac{\log p}{p} + A$ avec

$$A = \frac{1}{n}\sum_{p \leq n}(v_p(n!) - \frac{n}{p}) \log p \leq \sum_{p \leq n}(\frac{n}{p^2} + \frac{n}{p^3} + \cdots)\frac{\log p}{n} \leq \sum_{p \leq n} \frac{\log p}{p(p-1)}$$

et comme la série à termes positifs $\sum_k \frac{\log k}{k(k-1)}$ converge, A est majoré par une constante. Par ailleurs on a clairement $A \geq -\frac{\log n}{n}\pi(n) \geq -6 \log 2$ et donc $A = \mathcal{O}(1)$, d'où le résultat.

2 Courbes elliptiques: hors programme, cette section introduit à un des domaines actuellement les plus actifs de la théorie des nombres

Exercice 1. *Une fonction f est dite **elliptique** par rapport à un réseau Λ si c'est une fonction méromorphe sur $\mathbb{C}$ qui est Λ-périodique, i.e.*

$$f(z+\omega) = f(z)$$

pour tout $z \in \mathbb{C}$ et tout $\omega \in \Lambda$; c'est bien sûr équivalent à $f(z+\omega_1) = f(z) = f(z+\omega_2)$ pour tout $z \in \mathbb{C}$ avec $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.

(1) Montrer que si f n'a pas de poles, montrer que f est constante.

(2) Soit f une fonction elliptique par rapport à Λ et soit P un parallélogramme fondamental.

(i) On suppose que f n'a pas de poles sur le bord ∂P de P. Montrer alors que la somme des résidus de f dans P est égale à 0.

(ii) On suppose que f n'a ni zéros ni poles sur ∂P. On note a_i les zéros et poles de f dans P et on note m_i la multiplicité de f en a_i. Montrer que

$$\sum_i m_i = 0$$

$$\sum_i m_i a_i \equiv 0 \mod \Lambda$$

(3) On considère la fonction $\mathfrak{P}$ de Weierstrass:

$$\mathfrak{P}_\Lambda(x) = x^{-2} + \sum_{\omega \in \Lambda - 0}[(x-\omega)^{-2} - \omega^{-2}]$$

(i) Montrer que pour tout $s > 2$ la somme $\sum_{\omega \in \Lambda - 0} \frac{1}{|\omega|^s}$ converge. En déduire que la série qui définit $\mathfrak{P}$ converge uniformément sur tout compact de $\mathbb{C}$ ne contenant pas les points du réseau Λ.

(ii) En considérant $\mathfrak{P}'(x) = -2\sum_{x\in\Gamma}(x-\omega)^{-3}$*, montrer que* $\mathfrak{P}$ *est elliptique par rapport à* Λ*.*

(4) L'ensemble des fonctions elliptiques par rapport à Λ *est un corps sur* $\mathbb{C}$*; on veut montrer que celui-ci est engendré par* $\mathfrak{P}$ *et* $\mathfrak{P}'$*.*

(i) Soit f *elliptique paire et soit* $u \equiv -u \mod \Lambda$ *avec* $u \not\equiv 0 \mod \Lambda$*. Montrer que* $g(z) := \mathfrak{P}(z) - \mathfrak{P}(u)$ *a un zéro d'ordre* 2*. En déduire que* f *a un zéro d'ordre pair en* u*. Traitez le cas de* $u \equiv 0 \mod \Lambda$ *en considérant* $g = 1/\mathfrak{P}$*.*

(ii) Soit $(u_i)_{1\leq i\leq r}$ *un famille de points contenant un représentant de chaque classe* $(u, -u) \mod \Lambda$ *où* f *a un pole ou un zéro autre que la classe de* Λ*. On pose*

$$m_i = \mathrm{ord}_{u_i} f \text{ si } 2u_i \not\equiv 0 \mod \Lambda$$

$$m_i = \frac{1}{2}\mathrm{ord}_{u_i} f \text{ si } 2u_i \equiv 0 \mod \Lambda$$

Montrer, en utilisant le théorème de Liouville, que f *est égal à une constante fois* $\prod_{i=1}^{r}[\mathfrak{P}(z)-\mathfrak{P}(u_i)]^{m_i}$*.*

(iii) En déduire que $\mathbb{C}(\mathfrak{P})$ *est le corps des fonctions elliptiques paires par rapport à* Λ*, puis que* $\mathbb{C}(\mathfrak{P}, \mathfrak{P}')$ *est le corps des fonctions elliptiques par rapport à* Λ*.*

(5) On veut montrer que les points $(\mathfrak{P}(z), \mathfrak{P}'(z))$ *appartiennent à une cubique d'équation* $y^2 = 4x^3 - g_2x - g_3$ *avec* $\Delta = g_2^3 - 27g_3^2 \neq 0$*.*

(i) Montrer que

$$\mathfrak{P}(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)s_{2n+2}(\Lambda)z^{2n}$$

avec $s_n(\Lambda) = s_n = \sum_{\omega\neq 0}\frac{1}{\omega^m}$*.*

(ii) En posant $g_2 = 60s_4$ *et* $g_3 = 140s_6$*, montrer que* $(\mathfrak{P}(z), \mathfrak{P}'(z))$ *appartiennent à une cubique d'équation* $y^2 = 4x^3 - g_2x - g_3$*.*

(iii) On pose $e_1 = \mathfrak{P}(\omega_1/2)$*,* $e_2 = \mathfrak{P}(\omega_2)$ *et* $e_3 = \mathfrak{P}(\frac{\omega_1+\omega_2}{2})$*. Montrer que modulo* Γ*,* $\mathfrak{P}'$ *a trois racines simples à savoir* $\omega_1/2$*,* $\omega_2/2$ *et* $(\omega_1+\omega_2)/2$*. En déduire que*

$$(\mathfrak{P}')^2 = 4(\mathfrak{P} - e_1)(\mathfrak{P} - e_2)(\mathfrak{P} - e_3)$$

avec $\Delta = g_2^3 - 27g_3^2 \neq 0$*.*

(iv) En déduire que

$$x = \frac{1}{2}\int_{\infty}^{\mathfrak{P}(x)}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy \mod \Gamma$$

avec $\omega_1 = \int_{\infty}^{e_1}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$ *et* $\omega_2 = \int_{e_1}^{e_2}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$*.*

(v) Montrer que l'équation $y^2 = x^3 - x$ *correspond au réseau* $\mathbb{Z}^2$ *en utilisant l'égalité*

$$\omega_1 = \int_0^1 (x-x^2)^{-1/2}dx = \int_1^{\infty}(x^3-x)^{-1/2}dx = \omega_2/i$$

que l'on montrer via le changement de variable $x \mapsto 1/x$*.*

Preuve : (1) Si f n'a pas de pôles, elle est alors bornée sur le compact $\mathbb{C}/\Lambda$ et donc par périodicité sur $\mathbb{C}$. Le théorème de Liouville donne alors que f est constante.

(2) (i) On a

$$2i\pi\sum \mathrm{res} f = \int_{\partial P} f(z)dz$$

qui est nul par périodicité de f.

(ii) Comme f est elliptique, on en déduit que f' et f/f' le sont aussi. On a alors comme précédemment

$$0 = \int_{\partial P} \frac{f'}{f}(z)dz = 2o\pi \sum m_i$$

Pour la deuxième égalité on utilise

$$\int_{\partial P} z\frac{f'(z)}{f(z)}dz = 2i\pi \sum m_i a_i$$

car $\mathrm{res}_{a_i} z\frac{f'(z)}{f(z)} = m_i a_i$. En effectuant le changement de variable $u = z - \omega_2$ dans la deuxième intégrale du membre de gauche ci-dessous, on obtient

$$\int_{\alpha}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz = -\omega_2 \int_{\alpha}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz = 2i\pi k\omega_2$$

pour $k \in \mathbb{N}$. On fait de même pour les deux autres cotés opposés, d'où le résultat.

(3) (i) La somme partielle pour $|\omega| \leq N$ peut se décomposer en une somme sur les anneaux $n-1 \leq |\omega| < n$, pour $1 \leq n \leq N$. Sur chaque anneau, le nombre de points du réseau est d'ordre n et donc

$$\sum_{|\omega|\leq N} \frac{1}{|\omega|^s} \leq \sum_{1}^{\infty} \frac{n}{n^s}$$

qui converge donc pour $s > 2$.

(ii) Par convergence uniforme sur tout compact, on a

$$\mathfrak{P}'(x) = -2\sum_{\omega\in\Lambda} \frac{1}{(x-\omega)^3}$$

qui est donc Λ-périodique et impaire. Ainsi on a

$$\mathfrak{P}(x+\omega_1) = \mathfrak{P}(x) + C$$

et en prenant $x = -\omega_1/2$, qui n'est pas un pôle de $\mathfrak{P}$, on obtient $C = 0$ car $\mathfrak{P}$ est paire. On procède de même pour ω_2 et donc $\mathfrak{P}$ est Λ-périodique.

(4) (i) On a $2u \equiv 0 \mod \Lambda$ ce qui donne dans P, $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Si f est elliptique paire et s'annule en u, on a alors $f'(u) = -f'(-u)$ et donc $f'(u) = 0$, i.e. f a un zéro d'ordre au moins 2 en u. Ainsi si $u \not\equiv 0 \mod \Lambda$, l'argument précédent montre que $g(z)$ a un zéro d'ordre au moins 2 en u et donc exactement d'ordre 2 d'après (ii) car $\mathfrak{P}$ a exactement un pôle d'ordre 2 dans P. Ainsi f/g est paire, elliptique, holomorphe en u. Si $f(u)/g(u) \neq 0$ alors $\mathrm{ord}_u f = 2$ et sinon, on répète l'argument.

Dans le cas où $u \equiv 0 \mod \Lambda$, on utilise $g = 1/\mathfrak{P}$ et on utilise les mêmes arguments.

(ii) D'après ce qui précède, pour $a \not\equiv 0 \mod \Lambda$, la fonction $\mathfrak{P}(z) - \mathfrak{P}(a)$ a un pôle d'ordre 2 en a si et seulement si $2a \equiv 0 \mod \Lambda$ et a deux zéros distincts d'ordre 1 en a et $-a$ sinon. Ainsi pour tout $z \not\equiv 0 \mod \Lambda$,

$$\prod_{i=1}^{r} (\mathfrak{P}(z) - \mathfrak{P}(u_i))^{m_i}$$

a le même ordre en z que f. C'est aussi vrai à l'origine d'après la première égalité de (2) (ii), le résultat découle alors du théorème de Liouville.

(iii) On en déduit donc que $\mathbb{C}(\mathfrak{P})$ est le cors des fonctions elliptiques paires par rapport à Λ. Par ailleurs si f est elliptique, elle s'écrit $f_+ + f_-$ avec f_+ paire et f_- impair. Pour f impair, le produit $f\mathfrak{P}'$ est pair et appartient donc à $\mathbb{C}(\mathfrak{P})$, d'où le résultat.

(5) (i) On écrit

$$\begin{aligned}
\mathfrak{P}(z) &= \tfrac{1}{z^2} + \textstyle\sum_{\omega\in\Lambda'} \left[\tfrac{1}{\omega^2}\left(1 + \tfrac{z}{\omega} + (\tfrac{z}{\omega})^2 + \cdots\right)^2 - \tfrac{1}{\omega^2}\right] \\
&= \tfrac{1}{z^2} + \textstyle\sum_{\omega\in L'} \sum_{m=1}^{\infty} (m+1)(\tfrac{z}{\omega})^m \tfrac{1}{\omega^2} \\
&= \tfrac{1}{z^2} + \textstyle\sum_{m=1}^{\infty} c_m z^m
\end{aligned}$$

avec $c_m = \sum_{\omega\neq 0} \frac{m+1}{\omega^{m+2}}$.

(ii) Ainsi on a

$$\mathfrak{P}(z) = \frac{1}{z^2} + 3s_4 z^2 + 5s_6 z^4 + \cdots \qquad \mathfrak{P}'(z) = \frac{-2}{z^3} + 6s_4 z + 20s_6 z^3 + \cdots$$

de sorte que $\phi(z) = \mathfrak{P}'(z)^2 - 4\mathfrak{P}(z)^3 + g_2\mathfrak{P}(z) + g_3$ est une fonction elliptique sans pôle et avec un zéro à l'origine; elle est donc identiquement nulle.

(iii) La fonction $h(z) = \mathfrak{P}(z) - e_i$ a un zéro en $\omega_i/2$ d'ordre pair, cf. ci-avant, de sorte que $\mathfrak{P}'(\omega_i/2) = 0$. La fonction elliptique $\mathfrak{P}$ prend la valeur e_i avec multiplicité 2 et n'a qu'un pôle d'ordre 2 modulo Λ de sorte que $e_i \neq e_j$ pour $i \neq j$. En comparant les zéros et les pôles, on en déduit donc que

$$(\mathfrak{P}')^2 = 4(\mathfrak{P} - e_1)(\mathfrak{P} - e_2)(\mathfrak{P} - e_3)$$

avec $\Delta \neq 0$.

(iv) De l'équation différentielle

$$dx = d\mathfrak{P}/d\mathfrak{P}' = \frac{1}{2}[(\mathfrak{P} - e_1)(\mathfrak{P} - e_2)(\mathfrak{P} - e_3)]^{-1/2} d\mathfrak{P}$$

on en déduit que

$$x = \frac{1}{2}\int_{\infty}^{\mathfrak{P}(x)} [(y - e_1)(y - e_2)(y - e_3)]^{-1/2} dy \mod \Gamma$$

et donc en particulier $\omega_1 = \int_{\infty}^{e_1} [(y - e_1)(y - e_2)(y - e_3)]^{-1/2} dy$ et $\omega_2 = \int_{e_1}^{e_2} [(y - e_1)(y - e_2)(y - e_3)]^{-1/2} dy$.

(v) On a $x^3 - x = x(x-1)(x+1)$ et donc

$$\omega_1 = \int_0^1 (x - x^3)^{-1/2} dx = \int_1^{\infty} (x^3 - x)^{-1/2} dx = \omega_2/i$$

ce qui correspond donc au réseau $\mathbb{Z}_2$.

Exercice 2. ***Loi d'addition*** *Etant donné des nombres complexes g_2, g_3 on peut se demander s'il existe un réseau pour lequel ce sont les invariants associés comme dans l'exercice précédent. La réponse est oui. On considère la courbe projective A d'équation*

$$uy^2 = 4x^3 - g_2 x u^2 - g_3 u^3$$

de point infini $(0, 0, 1)$ qui est l'image des points de Λ par l'application $z \mapsto (1, \mathfrak{P}(z), \mathfrak{P}'(z))$.

(1) Montrer que l'application ci-dessus induit une bijection $\mathbb{C}/\Lambda - 0 \longrightarrow A_{\mathbb{C}} - \{\infty\}$, où $A_{\mathbb{C}}$ désigne les points complexes de la cubique A.

(2) L'ensemble $\mathbb{C}/\Lambda$ est naturellement muni d'une structure de groupe; on veut exprimer celle-ci sur $A_{\mathbb{C}}$. Nous allons montrer que si $P_1 = (1, x_1, y_1)$ et $P_2 = (1, x_2, y_2)$ alors $P_3 = P_1 + P_2 = (1, x_3, y_3)$ s'exprime avec des fonctions rationnelles en x_1, x_2, y_1, y_2. Géométriquement on procède comme dans la figure (3): la droite (P_1P_2) intersecte $A_{\mathbb{C}}$ en un troisième point $Q_3 = -P_3$ et P_3 est le symétrique de Q_3 par rapport à l'axe des x.

(i) Soient $u_1, u_2 \in \mathbb{C} - \Lambda$ et supposons $u_1 \not\equiv u_2 \mod \Lambda$. Soient $a, b \in \mathbb{C}$ tels que

$$\mathfrak{P}'(u_1) = a\mathfrak{P}(u_1) + b$$

$$\mathfrak{P}'(u_2) = a\mathfrak{P}(u_2) + b$$

Montrer que $g(z) = \mathfrak{P}'(z) - a\mathfrak{P}(z) - b$ a 3 zéros comptés avec leur multiplicités. A quelle condition n'a-t-ont que 2 zéros distincts?

(ii) On suppose que $g(z)$ a 3 zéros distincts. En notant u_3 le troisième, montrer que $u_3 \equiv -(u_1+u_2)$ mod Λ. En déduire que

$$x_3 = -x_1 - x_2 + \frac{1}{4}\Big(\frac{y_1-y_2}{x_2-x_2}\Big)^2.$$

Traiter le cas des zéros multiples.

(iii) Pour $u_1 \equiv u_2 \mod \Lambda$ montrer que

$$\mathfrak{P}(2u) = -2\mathfrak{P}(u) + \frac{1}{4}\Big(\frac{\mathfrak{P}"(u)}{\mathfrak{P}'(u)}\Big)^2.$$

Preuve : (1) Pour tout nombre complexe α, $\mathfrak{P}(z)-\alpha$ a au plus deux zéros et au moins un, d'où la surjectivité. D'après ce qui précède, le zéro z_1 est simple si $2z_1 \not\equiv 0 \mod \Lambda$ et double sinon. Dans le premier cas, l'autre zéro est $-z_1$ avec $\mathfrak{P}'(-z_1) = -\mathfrak{P}'(z_1) \neq 0$, d'où l'injectivité.

(2) (i) $g(z)$ a un pôle d'ordre 3 en zéro et donc possède 3 zéros comptés avec multiplicités, dont u_1 et u_2. Si u_1 est double, on a alors d'après l'exercice précédent (2) (ii)

$$2u_1 + u_2 \equiv 0 \mod \Lambda$$

de sorte que pour u_1 fixé, il n'y a qu'un nombre fini de valeurs pour u_2.

(ii) L'égalité $u_3 \equiv -u_1-u_2 \mod \Lambda$ découle de l'exercice précédent (2) (ii). L'équation $4x^3-g_2x-g_3-(ax+b)^2 = 0$ a trois racines comptés avec multiplicité, à savoir $\mathfrak{P}(u_1), \mathfrak{P}(u_2), \mathfrak{P}(u_3)$. Les relations coefficients racines donnet

$$\mathfrak{P}(u_1) + \mathfrak{P}(u_2) + \mathfrak{P}(u_3) = \frac{a^2}{4}$$

avec $a = \frac{\mathfrak{P}'(u_1)-\mathfrak{P}'(u_2)}{\mathfrak{P}(u_1)-\mathfrak{P}(u_2)}$ ce qui donne

$$\mathfrak{P}(u_1+u_2) = -\mathfrak{P}(u_1) - \mathfrak{P}(u_2) + \frac{1}{4}\Big(\frac{\mathfrak{P}'(u_1)-\mathfrak{P}'(u_2)}{\mathfrak{P}(u_1)-\mathfrak{P}(u_2)}\Big)^2$$

d'où le résultat. Cette formule est vraie pour tous les $u_2 \not\equiv u_1 \mod \Lambda$ sauf un nombre fini; c'est donc vrai pour tout $u_2 \not\equiv u_1 \mod \Lambda$ par prolongement analytique.

(iii) La formule s'obtient à partir de la précédente en passant à la limite $u_1 \to u_2$.

Exercice 3. ***Une introduction à la géométrie algébrique***

(1) En vous appuyant sur la classification des coniques projectives de $\mathbb{P}^2_{\mathbb{R}}$, montrez qu'une conique non dégénérée C non vide de $\mathbb{P}^2_{\mathbb{R}}$ est projectivement équivalente à la courbe $XZ = Y^2$.

Montrez que cette courbe admet un paramétrage par $\mathbb{P}^1_{\mathbb{R}}$ via l'application qui à (U,V) associe (U^2, UV, V^2). Quelle est l'application inverse?

(2) ***Cas simples du théorème de Bézout***

(i) Soit

$$F(U,V) = a_dU^d + a_{d-1}U^{d-1}V + \cdots + a_0V^d$$

un polynôme homogène non nul de degré d en 2 variables à coefficients dans un corps k. On lui associe le polynôme en une variable $f(u) = F(u,1)$ et on définit la multiplicité d'un zéro (u,v) de F dans $\mathbb{P}^1_k$ comme la multiplicité de u/v dans f si $v \neq 0$ et sinon en $(1,0)$ comme l'entier $d - \deg f$.

Montrer que F a au plus d zéros dans $\mathbb{P}^1_k$ comptés avec multiplicités.

(ii) Soit $L \subset \mathbb{P}^2_k$ une droite et $D \subset \mathbb{P}^2_k$ une courbe définie par une équation $G(X,Y,Z) = 0$ où G est un polynôme homogène de degré d en X,Y,Z. On suppose $L \not\subseteq D$. Montrer que le cardinal de $L \cap D$ est inférieur ou égal à d.

(iii) Même hypothèse qu'en (ii) en remplaçant L par une conique non dégénérée C: montrer que le cardinal de $C \cap D$ est inférieur ou égal à $2d$.

Remarque: On peut définir une notion de multiplicité d'une intersection en un point de sorte que les résultats précédents soient vrais en comptant avec multiplicité. En outre si k est algébriquement clos, on a alors égalité. Le théorème de Bézout concerne des courbes C et D de degré n et m: leur intersection est alors nm, en comptant les multiplicités et en travaillant sur un corps algébriquement clos.

(3) ***L'espace des coniques*** *Dans la suite on note $S_d(k)$ l'espace des polynômes homogènes de degré d à coefficients dans k, en les variables X, Y, Z. Etant donnés des points $P_1, \cdots, P_r$ de $\mathbb{P}^2_k$, on notera $S_d(P_1, \cdots, P_n)$ le sous-ensemble de $S_d(k)$ constitué des éléments F qui s'annulent sur les P_i.*

(i) Soient $P_1, \cdots, P_5 \in \mathbb{P}^2_{\mathbb{R}}$ des points distincts tels que 4 quelconques ne sont pas colinéaires. Montrer qu'il existe au plus une conique passant par ces 5 points.

(ii) Soit $n \geq 5$ et soient $P_1, \cdots, P_n$ des points tels que 4 quelconques ne sont jamais colinéaires. Montrer alors que l'ensemble des formes quadratiques qui s'annulent sur ces points est de dimension $6 - n$.

(iii) ***Un pinceau de coniques*** *est une famille de la forme*

$$C_{\lambda,\mu} := (\lambda Q_1 + \mu Q_2 = 0)$$

où Q_1 et Q_2 sont des coniques. On suppose que le pinceau possède au moins une conique dégénérée, montrer alors qu'elle en possède au plus 3. En outre si $k = \mathbb{R}$, montrer que le pinceau admet toujours une conique dégénérée.

(4) ***Cubiques: exemples***

(i) On considère la cubique de $\mathbb{R}^2$ définie par l'équation $y^2 = x^3 + x^2$. Donnez en une paramétrisation.

(ii) Même question avec la cubique $y^2 = x^3$.

(iii) Soit k un corps de caractéristique différente de 2 et soit $\lambda \in k$ avec $\lambda \neq 0, 1$. Montrer que pour si $f, g \in k(t)$ sont tels que $f^2 = g(g-1)(g-\lambda)$ alors $f, g \in k$. Quelle interprétation en donnez-vous sur la cubique $y^2 = x(x-1)(x-\lambda)$?

(5) ***Cas simples du Nullstellensatz****: soit k un corps infini et soit $F \in S_d(k)$ un polynôme homogène de degré d à coefficients dans k en les variables X, Y, Z.*

(i) Soit $L \subset \mathbb{P}^2_k$ une droite. Montrer que si F s'annule sur L alors $F = HF'$ où H est une équation de L et $F' \in S_{d-1}(k)$. En déduire que si $P_1, \cdots, P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1, \cdots, P_a \in L$ et $P_{a+1}, \cdots, P_n \notin L$ avec $a > d$, alors

$$S_d(P_1, \cdots, P_n) = HS_{d-1}(P_{a+1}, \cdots, P_n)$$

(ii) Soit $C \subset \mathbb{P}^2_k$, une conique non dégénérée et non vide. Montrer que si F s'annule sur C alors $F = QF'$ où Q est une équation de C et $F' \in S_{d-2}(k)$. En déduire que si $P_1, \cdots, P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1, \cdots, P_a \in C$ et $P_{a+1}, \cdots, P_n \notin C$ avec $a > 2d$, alors

$$S_d(P_1, \cdots, P_n) = QS_{d-2}(P_{a+1}, \cdots, P_n)$$

(iii) Soient $P_1, \cdots, P_8 \in \mathbb{P}^2_k$ des points distincts tels que 4 quelconques ne sont pas colinéaires et que 7 quelconques ne sont pas sur une conique non dégénérée. Montrer alors que $\dim S_3(P_1, \cdots, P_8) = 2$.

Indication*: on traitera séparément le cas où 3 points quelconques ne sont pas colinéaires et 6 quelconques ne sont pas sur une conique non dégénérée.*

(iv) Soient C_1, C_2 deux coniques dont l'intersection est 9 points distincts. Montrer que toute conique D qui passe par 8 d'entre eux passe aussi par le neuvième.

(6) ***Loi d'addition sur une conique***: *soit $k \subset \mathbb{C}$ et $C \subset \mathbb{P}^2_k$ une cubique d'équation $F = 0$. On suppose que F est irréductible et que pour tout point $P \in C$, il existe une unique droite $L \subset \mathbb{P}^2_k$ telle que P est un zéro multiple de $F_{|L}$. On fixe un point $O \in C$ et on considère la construction suivante:*

Construction: *(a) Soit $A \in C$ et soit $\bar{A}$ le troisième point d'intersection de C avec la droite OA.*

(b) Pour $A, B \in C$ soit R le troisième point d'intersection de AB avec C et on définit $A + B$ comme étant égal à $\bar{R}$.

On veut montrer que l'on définit ainsi une loi de groupe abélien sur C avec O comme élément neutre.

(i) *Montrer que la construction précédente est bien définie.*

(ii) *Montrer que O est bien un élément neutre et que la loi est commutative.*

(iii) *Montrer que l'inverse de A est le troisième point d'intersection de $\bar{O}A$ avec C.*

(iv) ***Associativité***: *soient A, B, C trois points de C; la construction de $(A+B)+C = \bar{S}$ utilise les 4 droite (cf. la figure (1)):*

$$L_1 = ABR, \quad L_2 = RO\bar{R}, \quad L_3 = C\bar{R}S, \quad L_4 = SO\bar{S}$$

La construction de $(B + C) + A = \bar{S}'$ utilise les 4 droites

$$M_1 = BCQ, \quad M_2 = QO\bar{Q}, \quad M_3 = A\bar{Q}S', \quad M_4 = S'O\bar{S}'$$

Il s'agit de prouver $\bar{S} = \bar{S}'$ ou de manière équivalente $S = S'$. On considère les deux cubiques

$$D_1 = L_1 + M_2 + L_3 \qquad D_2 = M_1 + L_2 + M_3$$

de sorte que

$$C \cap D_1 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\} \qquad C \cap D_2 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S'\}$$

Conclure en supposant les 9 points $\{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$ distincts.

(v) *Conclure dans le cas général en utilisant un argument de continuité et en utilisant l'hypothèse $k \subset \mathbb{C}$.*
Remarque: On peut montrer le cas général pour tout k avec une bonne notion de multiplicité, ou bien en utilisant la topologie de Zariski.

(vi) *Soit $C \subset \mathbb{P}^2_k$ une cubique possédant un point d'inflexion P. Montrer qu'un changement de coordonnées dans $\mathbb{P}^2_k$ permet de se ramener à une équation de la forme **normale**, i.e.*

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

Indication: *choisissez les coordonnées telles que $P = (0, 1, 0)$ et la droite d'inflexion $Z = 0$.*

(vii) ***Loi de groupe simplifiée***: *on considère une cubique sous forme normale et on prend $O = (0, 1, 0)$ comme élément neutre. Montrer que l'on a les propriétés suivantes et retrouver la loi de groupe donnée par les fonctions de Weierstrass.*
(a) $C = \{O\} \cup C_0$, où $C_O : (y^2 = x^3 + ax + b)$ est un courbe affine;
(b) les droites passant par O sont les droite projectives $X = \lambda Z$ et donc les droites affines $x = \lambda$;
(c) $-P = \bar{P}$.

*Remarque: Essayez de prouver **le théorème de l'hexagone de Pascal**: Soit un hexagone $ABCDEF$ dans $\mathbb{P}^2_k$ dont les paires de cotés opposés se rencontrent aux points P, Q, R. On suppose les 9 points et les 6 droites distinctes. Montrer alors que*

$$ABCDEF \text{ sont sur une même conique non dégénérée} \Leftrightarrow PQR \text{ sont colinéaires}$$

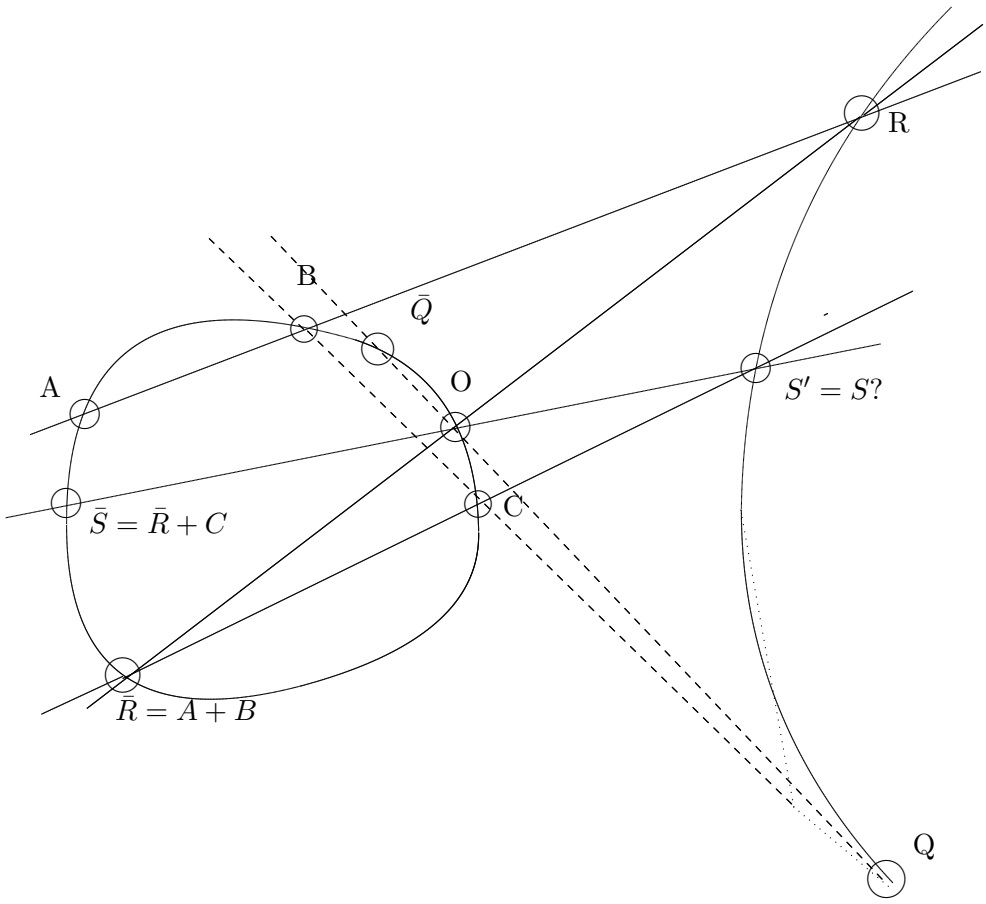

Figure 1: Loi d'addition sur une courbe elliptique

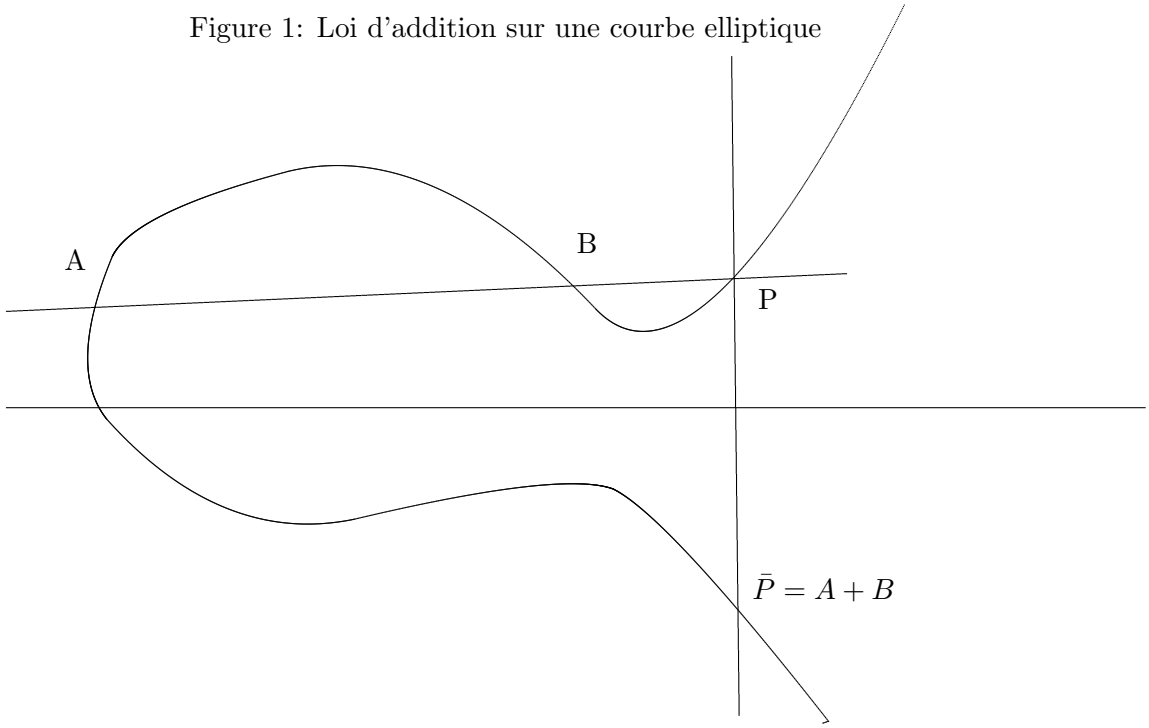

Figure 2: Loi d'addition simplifiée

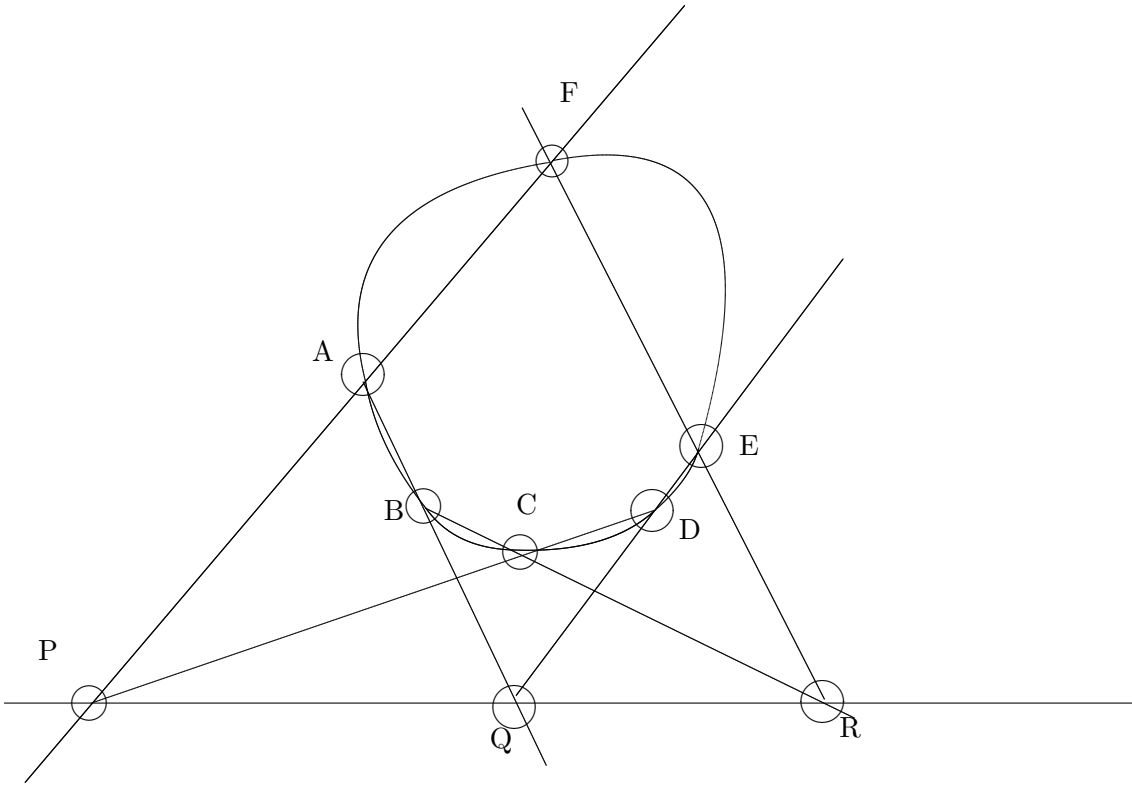

Figure 3: L'hexagone de Pascal

Preuve : (1) Les coniques projectives de $\mathbb{P}^2_{\mathbb{R}}$ sont en bijection avec les classes de similitudes des formes matrices symétriques de $\mathbb{M}_3(\mathbb{R})$ via l'action de $GL_3(\mathbb{R})$, où $A \in GL_3(\mathbb{R})$ agit sur M par ${}^tAMA$. Ces classes d'équivalence sont alors déterminées par la signature $(r, s$ avec $r \geq s$. Si on veut la conique non dégénérée il faut en plus que $r + s = 3$, ce qui laisse les couples $(3, 0)$ et $(2, 1)$. Le premier donne une conique vide et la deuxième la conique $U^2 = V^2 - W^2$ qui après le changement de variable $Y = U$, $X = V - W$ et $Z = V + W$ s'écrit $Y^2 = XZ$. En affine la parabole $y^2 = x$ se paramètre par y ce qui donne le paramétrage projectif de l'énoncé. L'application inverse est $(X, Y, Z) \in \mathbb{P}^2_{\mathbb{R}} \mapsto (X, Y) \in \mathbb{P}^1_{\mathbb{R}}$.

(2) (i) Soit m_∞ la multiplicité du zéro de F en $(1, 0)$; par définition $d - m_\infty$ est le degré de polynôme f qui a donc au plus $d - m_\infty$ racines.

Remarque: si k est algébriquement clos, on a évidemment égalité.

(ii) On paramètrise la droite L sous la forme

$$X = a(U, V), \quad Y = b(U, V), \quad Z = c(U, V)$$

où a, b, c sont des formes linéaires en U, V. L'intersection de L avec D est donnée par les $(U, V) \in \mathbb{P}^1_k$ tels que $F(U, V) = G(a(U, V), b(U, V), c(U, V)) = 0$, d'où le résultat d'après la question précédente.

(iii) On paramétrise la conique C sous la forme

$$X = a(U, V), \quad Y = b(U, V), \quad Z = c(U, V)$$

où a, b, c sont des formes quadratiques en U, V; en effet C est projectivement équivalente à $Y^2 = XY$ paramétrée par (U^2, UV, V^2), i.e.

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = M \begin{pmatrix} U^2 \\ UV \\ V^2 \end{pmatrix}$$

où $M \in GL_3(k)$. Il faut alors résoudre l'équation $F(U, V) = G(a(U, V), b(U, V), c(U, V)) = 0$, d'où le résultat d'après la question précédente.

(3) (i) Soient $C_1 \neq C_2$ deux coniques passant par $P_1, \cdots, P_5$; C_1 est donc non vide et non dégénérée et donc projectivement équivalente à $\{(U^2, UV, V^2) \ / \ (U, V) \in \mathbb{P}^1\}$. D'après la question précédente, on a $C_1 \subset C_2$ de sorte

que si Q_2 est une équation de C_2, alors $Q(U^2, UV, V^2) = 0$ pour tout $(U, V) \in \mathbb{P}^1$ et donc Q_2 est un multiple de $XZ - Y^2$ ce qui contredit l'hypothèse $C_1 \neq C_2$.

(ii) $S_2(k)$ est en bijection avec les matrices symétriques de $\mathbb{M}_3(k)$, c'est donc un k-espace vectoriel de dimension 6. Le sous-ensemble des F qui s'annulent en P est le noyau d'une forme linéaire, i.e. un hyperplan, d'où le résultat.

(iii) La conique $C_{\lambda,\mu}$ est dégénérée si et seulement si $\det(\lambda Q_1 + \mu Q_2) = 0$ ce qui donne une équation $F(\lambda, \mu)$ homogène de degré 3 en λ et μ, d'où le résultat.

(4) (i) Le point $(0, 0)$ est clairement un point double. On considère les droite passant par $(0, 0)$ de pente t qui doit couper la cubique en un unique autre point. On obtient alors une paramétrisation $t \mapsto (t^2 - 1, t^3 - 1)$.

(ii) On procède de même ce qui donne $t \mapsto (t^2, t^3)$.

(iii) On rappelle que l'anneau $k[t]$ est principal et donc factoriel. On écrit $f = r/s$ et $g = p/q$ avec r, s et p, q dans $k[t]$ premiers entre eux. On obtient alors

$$r^2 q^3 = s^2 p(p - q)(p - \lambda q)$$

On obtient alors que s^2 divise q^3 et q^3 divise s^2 de sorte que $s^2 = aq^3$ avec $a \in k$. Ainsi $aq = (s/q)^2$ est un carré et de $r^2 = ap(p - q)(p - \lambda q)$ on en déduit qu'il existe des constantes b, c, d tels que bp, $c(p - q)$ et $d(p - \lambda q)$ aussi. Passons dans $\bar{k}[t]$, de sorte que $q = u^2$ et $p = v^2$ avec $p - q = (u - v)(u + v)$ et $p - \lambda q = (u - \alpha v)(u + \alpha v)$ des carrés avec $\alpha^2 = \lambda$. Comme u et v sont premiers entre eux, on en déduit que $u - v$, $u + v$, $u + \alpha v$ et $u - \alpha v$) sont aussi des carrés. On conclut alors par un argument de descente à la Fermat sur le degré des polynômes.

Ainsi la cubique $y^2 = x(x - 1)(x - \lambda)$ n'a pas de paramétrisation rationnelle.

(5) (i) Quitte à faire un changement de coordonnées on suppose que $L = X$ Pour $F \in S_d$, on l'écrit sous la forme $F = X\tilde{F} + G(Y, Z)$ de sorte que G est nulle sur X Or si G était non nul il aurait d'après ce qui précède au plus $d - 1$ zéros sur la droite L d'où la contradiction car k est infini.

Ainsi si F est homogène de degré d et si la courbe $D : (F = 0)$ rencontre L aux points $P_1, \cdots, P_a$ avec $a > d$, alors $L \subset D$ et donc $F = H\tilde{F}$. Comme $P_{a+1}, \cdots, P_n \notin L$ alors $\tilde{F} \in S_{d-1}(P_{a+1}, \cdots, P_n)$.

(ii) Quitte à faire un changement de coordonnées on suppose que $Q = XZ - Y^2$. Pour $F \in S_d$, on l'écrit sous la forme $F = Q\tilde{F} + A(X, Z) + YB(X, Y)$: en effet on substitue à chaque Y^2, $XZ - Q$ de sorte que modulo Q, on obtient $A(X, Z) + YB(X, Z)$. On paramétrise alors C par (U^2, UV, V^2) de sorte que $A(U^2, V^2) + UVB(U^2, V^2) = 0$ sur C. Comme précédemment, k étant infini, on en déduit que $A(U^2, V^2) + UVB(U^2, V^2) = 0$ dans $k[U, V]$ ce qui en séparant les parties paires et impaires donne $A(X, Z) = B(X, Z) = 0$. Le reste du raisonnement procède comme dans la question précédente.

(iii) Supposons d'abord que 3 points quelconques ne sont pas colinéaires et que 6 quelconques ne sont pas sur une même conique. Supposons par l'absurde que $\dim S_3(P_1, \cdots, P_8) \geq 3$ et soient P_9, P_{10} des points distincts sur la droite P_1P_2. On a alors

$$\dim S_3(P_1, \cdots, P_{10}) \geq \dim S_3(P_1, \cdots, P_8) - 2 \geq 1$$

de sorte qu'il existe $F \neq 0$ dans $S_3(P_1, \cdots, P_{10})$. On en déduit donc d'après (i) que $F = HQ$ avec $Q \in S_2(P_3, \cdots, P_8)$ d'où la contradiction car les 6 points $P_3, \cdots, P_8$ n'appartiennent pas à une même conique d'après l'hypothèse.

Supposons désormais que P_1, P_2, P_3 sont colinéaires, sur la droite L d'équation $H = 0$. Soit P_9 un quatrième point sur L. D'après (i) on a

$$S_3(P_1, \cdots, P_9) = HS_2(P_4, \cdots, P_8)$$

Comme 4 quelconques des $P_4, \cdots, P_8$ ne sont colinéaires alors $\dim S_2(P_4, \cdots, P_8) = 1$ et donc $\dim S_3(P_1, \cdots, P_9) = 1$ ce qui implique $\dim S_3(P_1, \cdots, P_8) \leq 2$.

Supposons enfin que $P_1, \cdots, P_6$ appartiennent à une même conique C d'équation $Q = 0$. Soit $P_9 \in C$ distincts de $P_1, \cdots, P_6$. D'après (ii), on a

$$S_3(P_1, \cdots, P_9) = QS_1(P_7, P_8)$$

La droite $L = P_7P_8$ est unique de sorte que $S_3(P_1, \cdots, P_9)$ est de dimension 1 et donc $\dim S_3(P_1, \cdots, P_8) \leq 2$.

(iv) Si 4 quelconques parmi $P_1, \cdots, P_9$ sont sur une droite L alors C_1 et C_2 qui rencontrent L en plus de 4 points, la contiennent ce qui n'est pas par hypothèse. Pour les mêmes raisons 7 points quelconques ne sont pas sur une même conique. On en déduit alors que

$$\dim S_3(P_1, \cdots, P_8) = 2$$

ce qui signifie que les équations F_1, F_2 de C_1 et C_2 forment une base de $S_3(P_1, \cdots, P_8)$ de sorte que $D = (G = 0)$ est de la forme $G = \lambda F_1 + \mu F_2$ et passe donc par P_9.

(6) (i) Si P et Q sont distincts alors la droite PQ est unique et bien définie: si $P = Q$ cela découle de l'hypothèse. L'équation $F_{|L}$ est de degré 3 et possède donc 2 zéros et donc un troisième car la somme des racines dans $\mathbb{C}$ est le coefficient sur x^2 et appartient donc à k.

(ii) La construction $O + A$ consiste à prendre la droite OA, puis le troisième point d'intersection $\bar{A}$ puis à reprendre la droite $O\bar{A} = OA$ et prendre le troisième point d'intersection qui est donc A. La commutativité est évidente.

(iii) On considère la droite qui possède O comme point double et soit $\bar{O}$ le troisième point d'intersection. On vérifie alors aisément que le troisième point d'intersection de $\bar{O}A$ avec C est l'inverse de A.

(iv) On utilise la question précédente: C et D_1 vérifient bien les hypothèses de sorte que D_2 doit passer par S et la seule possibilité est $S' = S$.

(v) Il suffit de remarquer que $A + B$ est une fonction continue en A et B et que quitte à bouger un tout petit peu A, B, C en A', B', C', on peut se ramener au cas où les neuf points précédents sont distincts.

(vi) Quitte à effectuer un changement de coordonnées on suppose que le point d'inflexion est $P = (0, 1, 0)$ et la tangente est $Z = 0$. Le fait que $P \in C$ impose qu'il n'y a pas de terme en Y^3. Le fait que $L : (Z = 0)$ soit une tangente d'inflexion en P signifie que $f_{|L}$ a un zéro d'ordre 3 en P, i.e. de la forme $ax^3 + bx^2z + x(cz^2 + c'z) + dz^3 + d'z^2 + d"z$ soit $f = aX^3 + bX^2Z + X(cZ^2 + c'ZY) + dZ^3 + d'Z^2Y + d"ZY^2$ que l'on peut écrire sous la forme demandée via un égalité du genre $Y^2Z + ZY(\alpha X + \beta Z) = ZY' + aX^2 + bXZ + cZ^2$.

(vii) C'est clair.

Remarque: L'hexagone de Pascal: on considère le triplet de droites

$$L_1 : PAF \qquad L_2 : QDE, \qquad L_3 : RBC$$

et

$$M_1 : PCD, \qquad M_2 : QAB, \qquad M_3 : REF$$

Soit $C_1 = L_1 + L_2 + L_3$ et $C_2 = M_1 + M_2 + M_3$. On a $C_1 \cap C_2 = \{A, B, C, D, E, F, P, Q, R\}$. Si PQR son colinéaires avec $L = PQR$; alors soit Γ la conique qui passe par $ABCDE$, par construction $L + \Gamma$ est un cubique qui passe par les 8 points $\{A, B, C, D, E, P, Q, R\}$. D'après (5) (iv), il continet aussi F. Par hypothèse $F \notin L$ de sorte que $F \in \Gamma$, ce qui prouve que les six points appartiennent à une même conique.

Réciproquement, supposons que $ABCDEF$ sont sur une même conique Γ et soit $L = PQ$. Alors $L + \Gamma$ est un cubique qui passe par $\{A, B, C, D, E, F, P, Q, R\}$ et passe donc par R. Or R ne peut pas être sur Γ, sinon Γ serait dégénérée et les 6 droites ne seraient pas toutes distinctes. Ainsi $R \in L$ et PQR sont colinéaires.

Exercice 4. ***Méthode de factorisation de Lenstra:***

- *On choisit une courbe elliptique au hasard à coefficients dans $\mathbb{Z}$ avec un point P sur celle-ci. On considère alors la loi de groupe sur cette courbe modulo n.*
- *On calcule $eP = (u, x, y)$ dans ce groupe où e est un produit de petit nombres premiers pris à de petites puissances comme dans la méthode $p - 1$ de Pollard.*
- *On calcule le pgcd de u (ou du dénominateur de x) avec n.*
- *Si on trouve 1, alors on essaye avec une nouvelle courbe elliptique et un autre point.*

Commentez cet algorithme et expliquez en quoi il est plus souple que celui de Pollard.
Remarque: L'ordre d'une courbe elliptique prise au hasard sur $\mathbb{Z}/p\mathbb{Z}$ varie de manière alléatoire entre $p + 1 - 2\sqrt{p}$ et $p + 1 + 2\sqrt{p}$.

Preuve : Il s'agit de l'algorithme $p - 1$ de Pollard sur la courbe elliptique plutôt que sur $(\mathbb{Z}/p\mathbb{Z})^\times$. L'avantage est que l'on peut changer de groupe et plus particulièrement l'ordre du groupe: ainsi l'algorithme fonctionne dès qu'il existe un q premier compris entre $p + 1 - 2\sqrt{p}$ et $p + 1 + 2\sqrt{p}$ qui n'ait que des petits facteurs premiers, ce qui est plus souple qu'espérer que ce soit vrai juste pour $p - 1$.