Examen d'Arithmétique

Mercredi 16 avril 2025. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

Exercice 1 On considère l'irrationnel $\sqrt{41} \simeq 6,403124237432\ldots$ ainsi que le corps de nombres $K = \mathbb{Q}(\sqrt{41})$.

1. Calculer la décomposition en fraction continue de $\sqrt{41}$ et vérifier qu'elle est ultimement périodique de période 3.
2. Donner, si elle existe, la solution minimale $(x, y) \in \mathbb{N}^2$ de l'équation de Pell-Fermat
$$x^2 - 41y^2 = -1.$$
3. Déterminer tous les $(a, b) \in \mathbb{N}^2$ avec $0 < b \leq 62$ tels que
$$\left|\frac{a}{b} - \sqrt{41}\right| = \min\left\{\left|\frac{c}{d} - \sqrt{41}\right| \mid c, d \in \mathbb{N}, 0 < d \leq 62\right\}.$$
4. Montrer que la fraction irréductible $131168/20485 \simeq 6,403124237246766\ldots$ est l'une des réduites de $\sqrt{41}$, en utilisant un résultat du cours.
5. Donner un élément $\alpha \in K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$, en utilisant les résultats du cours.
6. Vérifier que le $\mathbb{Z}$-module I engendré par 2 et $1 + \sqrt{41}$ est un idéal de $\mathcal{O}_K$.
7. Calculer la norme de I.
8. Déterminer la factorisation de I en produit d'idéaux premiers de $\mathcal{O}_K$.

Corrigé :

1. Tout d'abord, $a_0 = \lfloor\sqrt{41}\rfloor = 6$, de sorte que $r_1 = \frac{1}{\sqrt{41}-6} = \frac{\sqrt{41}+6}{5}$. Donc $a_1 = \lfloor r_1\rfloor = 2$ et $r_2 = \frac{5}{\sqrt{41}-4} = \frac{\sqrt{41}+4}{5}$. Par conséquent, $a_2 = \lfloor r_2\rfloor = 2$ et $r_3 = \frac{5}{\sqrt{41}-6} = \sqrt{41} + 6$. Donc $a_3 = \lfloor r_3\rfloor = 12$ et $r_4 = \frac{1}{\sqrt{42}-6} = r_1$. On en déduit que $\sqrt{41} = [6; \overline{2, 2, 12}]$ est bien ultimement périodique de période 3 comme souhaité.
2. Comme la période $s = 3$ est impaire, l'équation de Pell-Fermat $x^2 - 41y^2 = -1$ a bien des solutions, et la solution minimale est donnée par la réduite $\frac{p_2}{q_2}$ de $\sqrt{41} = [6; \overline{2, 2, 12}]$, c'est-à-dire par $[6, 2, 2] = 6 + \frac{1}{[2,2]}$ où $[2, 2] = 2 + \frac{1}{2} = \frac{5}{2}$, de sorte que $\frac{p_2}{q_2} = \frac{32}{5}$. En effet, $x = 32$ et $y = 5$ satisfont bien à $x^2 - 41y^2 = 1024 - 41 \times 25 = 1024 - 1025 = -1$ comme souhaité.
3. Calculons la réduite $\frac{p_3}{q_3}$ suivante de $\sqrt{41}$, à savoir $[6, 2, 2, 12]$. On a $\frac{p_1}{q_1} = [6, 2] = \frac{13}{2}$ et $\frac{p_2}{q_2} = \frac{32}{5}$, de sorte que $p_3 = 12 \times 32 + 13 = 397$ et $q_3 = 12 \times 5 + 2 = 62$. Ainsi, $\frac{p_3}{q_3} = \frac{397}{62}$ est une meilleure approximation de $\sqrt{41}$. En

particulier, pour tout $c, d \in \mathbb{N}$ avec $0 < d \leq 62$, on a $|\sqrt{41} - \frac{397}{62}| \leq |\sqrt{41} - \frac{c}{d}|$, avec égalité si et seulement si $d = 62$ et $c = 397$. Ainsi, $(397, 62)$ est l'unique couple de naturels ayant la propriété souhaitée.

4. Par un résultat du cours, toute fraction irréductible $\frac{a}{b}$ telle que $|\sqrt{41} - \frac{a}{b}| < \frac{1}{2b^2}$ est une réduite de $\sqrt{41}$. Les 9 premiers chiffres à droite de la virgule dans les approximations données de $\sqrt{41}$ et de $131168/20485$ coïncident, de sorte que $|\sqrt{41} - 131168/20485| < 10^{-9}$. Montrons que $10^{-9} < \frac{1}{2\times(20485)^2}$. En effet, $20485 < 22000$, de sorte que $2 \times (20485)^2 < 8 \times 121 \times 10^6 < 1000 \times 10^6 = 10^9$. Donc $131168/20485$ est bien une réduite de $\sqrt{41}$.
5. Comme $41 \equiv 1 \bmod 4$, on a $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{41}}{2}]$, de sorte que $\alpha = \frac{1+\sqrt{41}}{2}$ convient.
6. Il s'agit de vérifier la stabilité de I par multiplication par les éléments de $\mathcal{O}_K$. Pour cela, il suffit de vérifier que le produit des générateurs 2 et $1+\sqrt{41}$ avec α est encore dans I. D'une part, $2\alpha = 1 + \sqrt{41} \in I$. D'autre part, $(1 + \sqrt{41})\alpha = \frac{1}{2}(1 + 2\sqrt{41} + 41) = 21 + \sqrt{41} = 10 \times 2 + 1 \times (1 + \sqrt{41}) \in I$.
7. Comme $\mathcal{O}_K = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \frac{1+\sqrt{41}}{2}$ et $I = \mathbb{Z} \cdot 2 \oplus \mathbb{Z} \cdot (1 + \sqrt{41})$ en tant que $\mathbb{Z}$-modules, on en déduit que $\mathcal{O}_K/I = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. En particulier, $N(I) = \text{Card } \mathcal{O}_K/I = 4$.
8. Le polynôme minimal de α est $(X - \frac{1}{2})^2 - \frac{41}{4} = X^2 - X - 10$, de sorte que $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - X - 10)$. Comme I est engendré par 2 et par 2α, on a $\mathcal{O}_K/I = \mathbb{Z}[X]/(X^2 - X - 10, 2, 2X) = \mathbb{F}_2[X]/(X^2 + X)$, et on en déduit que les idéaux de $\mathcal{O}_K$ contenant I sont en correspondance bijective avec ceux de $\mathbb{F}_2[X]/(X^2 + X)$. Ce dernier anneau est $\{0, 1, X, X + 1\}$ avec la relation $X(X + 1) = 0$. Ses idéaux propres non nuls sont donc $\{0, X\}$ et $\{0, X + 1\}$. En remplaçant X par α et en rajoutant les générateurs 2 et 2α, leurs images inverses dans $\mathcal{O}_K$ sont $J_1 = (2, 2\alpha, \alpha) = (2, \frac{1+\sqrt{41}}{2})$ et $J_2 = (2, 2\alpha, \alpha+1) = (2, \frac{1-\sqrt{41}}{2})$. Ces idéaux maximaux sont donc premiers, et ce sont les seuls à contenir, c'est-à-dire diviser, I. Comme $\mathcal{O}_K$ est un anneau de Dedekind, on doit donc avoir $I = J_1^a J_2^b$ avec $a, b \in \mathbb{N}^*$. Par multiplicativité de la norme, on a alors $4 = N(J_1)^a N(J_2)^b$, de sorte que $N(J_1) = N(J_2) = 2$ et $a = b = 1$. La factorisation de I en produit d'idéaux premiers est donc $I = J_1 J_2 = (2, \frac{1+\sqrt{41}}{2})(2, \frac{1-\sqrt{41}}{2})$.

Exercice 2 On considère la fonction indicatrice d'Euler φ et sa fonction sommatoire $\Phi(x) = \sum_{n \leq x} \varphi(n)$.

1. Montrer que $\varphi = \mu * \text{Id}$, où μ est la fonction de Möbius et Id est la fonction identité.
2. Pour tout $s \in \mathbb{C}$ avec $\text{Re}(s)$ suffisamment grand, calculer la série de Dirichlet $D_\varphi(s)$.

3. En déduire l'abscisse de convergence absolue $\sigma_a(\varphi)$ de D_φ.
4. Montrer que D_φ s'étend en une fonction méromorphe sur le plan complexe. Donner ses pôles dans $\overline{\Pi}_1 = \{s \in \mathbb{C} \mid \mathrm{Re}(s) \geq 1\}$ avec leur multiplicité et leur résidu.
5. En déduire avec l'aide du théorème d'Ikehara que $\Phi(x) \sim_\infty \frac{1}{2\zeta(2)} x^2$.

Corrigé :

1. On calcule
$$\begin{aligned}\varphi(n) &= \sum_{1\leq q\leq n} e(n\wedge q) = \sum_{1\leq q\leq n} (\mu * \mathbb{1})(n\wedge q) = \sum_{1\leq q\leq n}\sum_{d\mid n\wedge q} \mu(d) \\ &= \sum_{\substack{1\leq d\leq n\\ d\mid n}} \mu(d) \sum_{\substack{1\leq q\leq n\\ d\mid q}} 1 = \sum_{\substack{1\leq d\leq n\\ d\mid n}} \mu(d)\frac{n}{d} = (\mu * \mathrm{Id})(n).\end{aligned}$$
2. Comme $\varphi = \mu * \mathrm{Id}$, on a $D_\varphi(s) = D_\mu(s) D_{\mathrm{Id}}(s)$, lorsque $\mathrm{Re}(s) > \sigma_a(\mu)$ et $\mathrm{Re}(s) > \sigma_a(\mathrm{Id})$. Pour de tels s, d'une part, $D_\mu(s) = \frac{1}{\zeta}(s)$ et d'autre part, $D_{\mathrm{Id}}(s) = \sum_{n\geq 1} \frac{n}{n^s} = \sum_{n\geq 1} \frac{1}{n^{s-1}} = \zeta(s-1)$. Par conséquent, $D_\varphi(s) = \frac{\zeta(s-1)}{\zeta(s)}$.
3. Comme $\varphi = \mu * \mathrm{Id}$, on a $\sigma_a(\varphi) \leq \max(\sigma_a(\mu), \sigma_a(\mathrm{Id}))$. Mais $\sigma_a(\mu) = 1$ car $D_\mu(s) = \frac{1}{\zeta}(s)$. D'autre part, $D_{\mathrm{Id}}(s) = \zeta(s-1)$ pour $\mathrm{Re}(s-1) > 1$, de sorte que $\sigma_a(\mathrm{Id}) = 2$. Ainsi, $\sigma_a(\varphi) \leq 2$. Mais d'autre part, pour $\mathrm{Re}(s)$ assez grand, on a $D_\varphi(s) = D_\mu(s) D_{\mathrm{Id}}(s) = \frac{\zeta(s-1)}{\zeta(s)}$. Comme $\zeta(s-1)$ a un pôle en $s = 2$, on ne peut pas avoir $\sigma_a(\varphi) < 2$, donc $\sigma_a(\varphi) = 2$.
4. On a $D_\varphi(s) = \frac{\zeta(s-1)}{\zeta(s)}$ pour $\mathrm{Re}(s) > 2$. Chaque membre est une fonction holomorphe sur ce domaine, et le membre de droite est une fonction méromorphe sur $\mathbb{C}$. Par prolongement unique des fonctions holomorphes, l'égalité est donc vraie sur le complémentaire des pôles du membre de droite dans $\mathbb{C}$. Les pôles de $D_\varphi(s)$ sont ceux de $\zeta(s-1)$ ainsi que les zéros de $\zeta(s)$. Mais la fonction zêta n'a pas de zéros dans $\overline{\Pi}_1$. Il n'y a donc qu'un seul pôle en $s - 1 = 1$, c'est-à-dire en $s = 2$. Il s'agit d'un pôle simple, comme pour la fonction zêta. Son résidu est égal à $1 \times \frac{1}{\zeta(2)}$.
5. Par le théorème d'Ikehara, comme la fonction $D_\varphi(s) - \frac{1}{\zeta(2)}\frac{1}{s-2}$ se prolonge en une fonction continue sur $\overline{\Pi}_2$, alors la fonction sommatoire Φ de φ a le comportement asymptotique suivant : $\Phi(x) \sim_\infty \frac{1}{\zeta(2)}\frac{x^2}{2}$, comme souhaité.

Exercice 3 On considère le corps de nombres $K = \mathbb{Q}(\sqrt{-13})$.

1. Donner un élément $\alpha \in K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$, en utilisant les résultats du cours.
2. En considérant des factorisations de l'élément $14 \in \mathcal{O}_K$, montrer que $\mathcal{O}_K$ n'est pas factoriel.
3. Déterminer toutes les formes quadratiques binaires définies positives, réduites et primitives de discriminant -52.
4. Montrer que le cardinal du groupe des classes de $\mathcal{O}_K$ est égal à 2.
5. Montrer que la forme quadratique binaire $[1, 0, 13]$ obtenue précédemment correspond à la classe des idéaux principaux de $\mathcal{O}_K$.

On cherche maintenant à résoudre l'équation de Bachet

$$x^2 + 13 = y^3 \tag{1}$$

avec $(x, y) \in \mathbb{Z}^2$.

6. Si (x, y) est une solution de (1), montrer par l'absurde qu'il n'existe pas d'idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ contenant les idéaux $(x + i\sqrt{13})$ et $(x - i\sqrt{13})$.
   Indication : montrer que les entiers 26 et y appartiennent à $\mathfrak{p}$ et sont premiers entre eux.
7. En déduire que si (x, y) est une solution de (1), alors l'idéal $(x + i\sqrt{13})$ est le cube d'un idéal de $\mathcal{O}_K$.
8. Déduire de ce qui précède que si (x, y) est une solution de (1), alors il existe un élément $\beta \in \mathcal{O}_K$ tel que $x + i\sqrt{13} = \beta^3$.
9. En déduire toutes les solutions $(x, y) \in \mathbb{Z}^2$ de (1).

Corrigé :

1. Comme $-13 \equiv 3 \bmod 4$, on a $\mathcal{O}_K = \mathbb{Z}[i\sqrt{13}]$, de sorte que $\alpha = i\sqrt{13}$ convient.
2. On a $14 = 2 \times 7 = (1 + i\sqrt{13})(1 - i\sqrt{13})$. Pour conclure, vérifions que ces 4 facteurs sont premiers dans $\mathcal{O}_K$. La norme de $a + bi\sqrt{13} \in \mathcal{O}_K$ est donnée par $a^2 + 13b^2$. Ainsi, la norme de 2 est 4, celle de 7 est 49, et celle de $1 \pm i\sqrt{13}$ est 14. D'autre part, les seuls éléments de norme 1 satisfont $b = 0$, de sorte que $a = \pm 1$: ces éléments sont les unités ± 1 de $\mathcal{O}_K$. Par conséquent, si l'un des éléments $2, 7$ ou $1 \pm i\sqrt{13}$ de $\mathcal{O}_K$ n'est pas premier, il doit être divisible par un élément de norme 2 ou 7. Mais $a^2 + 13b^2 = 2$ ou 7 implique que $b = 0$, puis n'admet pas de solution entière a. On a donc bien construit deux décompositions distinctes de 14 comme produit de facteurs premiers, de sorte que $\mathcal{O}_K$ n'est pas factoriel.
3. Recherchons les formes quadratiques binaires $[a, b, c]$ avec $-a < b \leq a \leq c$, $1 \leq a \leq \sqrt{\frac{52}{3}}$ et $b^2 - 4ac = -52$. Comme $\lfloor \sqrt{\frac{52}{3}} \rfloor = 4$, on doit avoir $a = 1, 2, 3$

ou 4. D'autre part, comme $b^2 - 4ac = -52$, b doit être pair. Si $a = 1$, alors $b = 0$ ou 1, donc $b = 0$ puisque b est pair. La relation du discriminant donne alors $-4c = -52$ donc $c = 13$. On obtient $[1, 0, 13]$. Si $a = 2$, alors $b = -1, 0, 1$ ou 2, donc $b = 0$ ou 2 puisque b est pair. Si $b = 0$, la relation du discriminant donne $-8c = -52$ et n'a pas de solution entière c. Si $b = 2$, la relation du discriminant donne $4 - 8c = -52$ donc $c = 7$. On obtient $[2, 2, 7]$. Si $a = 3$, alors l'entier pair $b = -2, 0$ ou 2. Si $b = 0$, la relation du discriminant donne $-12c = -52$ et n'a pas de solution entière c. Si $b = \pm 2$, la relation du discriminant donne $4 - 12c = -52$ et n'a pas non plus de solution entière c. Enfin, si $a = 4$, alors l'entier pair $b = -2, 0, 2$ ou 4. Si $b = 0$, la relation du discriminant donne $-16c = -52$ et n'a pas de solution entière c. Si $b = \pm 2$, la relation du discriminant donne $4 - 16c = -52$ et n'a pas non plus de solution entière c. Si $b = 4$, la relation du discriminant donne $16 - 16c = -52$ et n'a toujours pas de solution entière c. Au total, il n'y a que deux formes quadratique binaires définies positives, réduites et de discriminant -52, qui sont $[1, 0, 13]$ et $[2, 2, 7]$.

4. Par un résultat du cours, le cardinal h_K du groupe des classes d'idéaux de $\mathcal{O}_K$ est égal au nombre $h(D)$ de formes quadratique binaires définies positives, réduites et de discriminant $D = -52$, c'est-à-dire 2.
5. Considérons l'idéal principal $(1) = \mathcal{O}_K$, engendré par 1 et $i\sqrt{13}$ en tant que $\mathbb{Z}$-module. Une base directe de (1) est donc $(i\sqrt{13}, 1)$. La norme de cet idéal est égale à 1, puisque $\mathcal{O}_K/(1)$ est trivial. La forme quadratique associée à cette base directe est donc $q(x, y) = |xi\sqrt{13} + y|^2 = 13x^2 + y^2$. Cette forme quadratique est proprement équivalente à $[1, 0, 13]$ comme souhaité.
6. Si il existe un idéal premier $\mathfrak{p}$ qui contient $(x + i\sqrt{13})$ et $(x - i\sqrt{13})$, alors il contient aussi $(2i\sqrt{13})$ et donc l'élément 26. D'autre part, $\mathfrak{p}$ contient aussi $(x^2 + 13) = (y^3) = (y)^3$, donc (y) et en particulier l'élément y, puisque $\mathfrak{p}$ est premier. Montrons que 26 et y sont premiers entre eux. D'une part, si y est pair alors l'équation de Bachet dit que $x^2 + 13 \equiv 0 \bmod 8$, ou encore que $x^2 \equiv 3 \bmod 8$. Mais 3 n'est pas un résidu quadratique modulo 8, une contradiction. D'autre part, si $y = 13b$ avec b entier, alors l'équation de Bachet implique que x est aussi multiple de 13 : $x = 13a$ avec a entier. Mais alors l'équation de Bachet donne $13a^2 + 1 = 13^2 b^3$, une contradiction modulo 13. Comme 26 et y sont premiers entre eux, le théorème de Bezout fournit λ et μ entiers tels que $\lambda \times 26 + \mu \times y = 1$. Comme 26 et y appartiennent à $\mathfrak{p}$, on a aussi $1 \in \mathfrak{p}$, mais alors $\mathfrak{p} = \mathcal{O}_K$, ce qui contredit l'hypothèse que $\mathfrak{p}$ est premier.
7. L'équation de Bachet implique que $(x+i\sqrt{13})(x+i\sqrt{13}) = (y)^3$. Le théorème de factorisation des idéaux d'un anneau de Dedekind en idéaux premiers implique que $(x + i\sqrt{13}) = \prod_{\mathfrak{p} \in \mathcal{P}_K} \mathfrak{p}^{\alpha_\mathfrak{p}}$, $(x - i\sqrt{13}) = \prod_{\mathfrak{p} \in \mathcal{P}_K} \mathfrak{p}^{\beta_\mathfrak{p}}$ et $(y) =$

$\prod_{\mathfrak{p}\in\mathcal{P}_K} \mathfrak{p}^{\gamma_\mathfrak{p}}$, avec $\alpha_\mathfrak{p}, \beta_\mathfrak{p}, \gamma_\mathfrak{p} \in \mathbb{N}$ pour tout $\mathfrak{p} \in \mathcal{P}_K$. D'autre part, comme $(x + i\sqrt{13})$ et $(x+i\sqrt{13})$ sont premiers entre eux, on a $\alpha_\mathfrak{p}\beta_\mathfrak{p} = 0$ pour tout $\mathfrak{p} \in \mathcal{P}_K$. Comme $\alpha_\mathfrak{p} + \beta_\mathfrak{p} = 3\gamma_\mathfrak{p}$, ceci implique que si $\alpha_\mathfrak{p} \neq 0$, c'est un multiple de 3. Par conséquent, $(x + i\sqrt{13})$ est le cube d'un idéal J de $\mathcal{O}_K$.

8. On vient de montrer que $J^3 = (x + i\sqrt{13})$, de sorte que la classe de l'idéal J est de cube trivial dans $\mathrm{Cl}(\mathcal{O}_K)$. Mais on a montré plus haut que ce groupe est d'ordre 2, donc la classe de J est triviale : c'est un idéal principal. Donc il existe $\gamma \in \mathcal{O}_K$ tel que $J = (\gamma)$, de sorte que $(x + i\sqrt{13}) = (\gamma^3)$. Ces générateurs coïncident donc modulo multiplication par une unité de $\mathcal{O}_K$, c'est-à-dire ± 1 : $x + i\sqrt{13} = (\pm\gamma)^3$, et $\beta = \pm\gamma$ convient.
9. Posons $\beta = a + bi\sqrt{13}$ avec $a, b \in \mathbb{Z}$. En séparant parties réelle et imaginaire, la relation $x+i\sqrt{13} = \beta^3$ donne $x = a^3-39ab^2$ et $1 = 3a^2b-13b^3$. La deuxième équation implique que b divise 1, donc $b = \pm 1$. En remplaçant dans cette équation, on obtient $3a^2 - 13 = \pm 1$. Le signe + donne $3a^2 = 14$ qui est sans solution. Le signe $-$ donne $3a^2 = 12$ qui implique $a = \pm 2$. En remplaçant ces valeurs pour a et b dans la première équation, on obtient $x = \pm 70$. En remplaçant cette valeur dans l'équation de Bachet, on obtient $y^3 = 4913$, ce qui correspond à $y = 17$. Les solutions de l'équation diophantienne $x^2 + 13 = y^3$ sont donc $(\pm 70, 17)$.