Examen d'Arithmétique

Mardi 11 avril 2023. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

Exercice 1 On désigne par $\mathcal{P}$ l'ensemble des nombres premiers. Soit x un réel ≥ 3, on considère les deux ensembles

$$\mathcal{E}(x) := \{p \in \mathcal{P}, 3 \leq p \leq x, \left(\frac{60}{p}\right) = 1\}$$

et

$$\mathcal{F}(x) := \{p \in \mathcal{P}, 3 \leq p \leq x, p \text{ (mod 343) engendre } (\mathbb{Z}/(343\mathbb{Z}))^\times\}.$$

a. Caractériser les nombres premiers impairs $p \leq x$ dans $\mathcal{E}(x)$ par une relation de congruence, puis donner un équivalent asymptotique du cardinal de $\mathcal{E}(x)$ lorsque x tend vers l'infini.

b. Mêmes questions pour l'ensemble $\mathcal{F}(x)$.

c. Donner un équivalent asymptotique de la somme

$$\sum_{p \in \mathcal{E}(x) \cap \mathcal{F}(x)} \frac{1}{\sqrt{p}}$$

pour x tendant vers l'infini.
Indication : appliquer le lemme de sommation par parties avec la fonction différentiable $g(x) = \frac{1}{\sqrt{x}}$, et utiliser une intégration par parties.

Corrigé :

a. Comme $\left(\frac{60}{p}\right) = \left(\frac{15}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{5}{p}\right)$, on doit avoir $\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = 1$ ou $\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = -1$. Dans le premier cas, comme il y a un carré modulo 3 (qui est 1) et 2 carrés modulo 5 (qui sont 1 et 4), cela donne par le théorème des restes chinois 2 possibilités pour p modulo 15 (qui sont 1 et 4). Dans le deuxième cas, on obtient aussi 2 possibilités pour p modulo 15 (qui sont 2 et 8), donc on a 4 possibilités entre tout. Les nombres premiers se répartissent en $\varphi(15) = 2 \cdot 4 = 8$ classes de congruence modulo 15. Par le théorème de Dirichlet, Card $\mathcal{E}(x) \sim_{x\to\infty} \frac{4}{8}\frac{x}{\log x} = \frac{1}{2}\frac{x}{\log x}$.

b. Il y a $\varphi(343)$ éléments dans le groupe cyclique $(\mathbb{Z}/(343\mathbb{Z}))^\times$. Comme $343 = 7^3$, cela donne $7^2 \cdot 6 = 294$ éléments. Dans ce groupe cyclique, il y a $\varphi(294)$ générateurs. Comme $294 = 2 \ldots 3 \cdot 7^2$, cela donne $\varphi(294) = 2 \cdot 6 \cdot 7 = 84$ générateurs. Les nombres premiers se répartissent parmi $\varphi(343) = 294$ classes de congruence modulo 343. Par le théorème de Dirichlet, Card $\mathcal{F}(x) \sim_{x\to\infty} \frac{84}{294}\frac{x}{\log x} = \frac{2}{7}\frac{x}{\log x}$.

c. Remarquons que $S(x) = \sum_{p\in\mathcal{E}(x)\cap\mathcal{F}(x)} 1 \sim \frac{1}{2}\frac{2}{7}\frac{x}{\log x}$, car par le théorème des restes chinois la proportion de congruences modulo $15\cdot 343$ correspondant aux éléments de $\mathcal{E}(x)\cap\mathcal{F}(x)$ est le produit des proportions pour chacun des deux ensembles. Par le lemme de sommation par parties, on obtient

$$\sum_{p\in\mathcal{E}(x)\cap\mathcal{F}(x)} \frac{1}{\sqrt{p}} = \frac{1}{\sqrt{x}}S(x) + \int_3^x \frac{S(t)}{2t^{3/2}}dt.$$

Le premier terme est en $\frac{2}{7}\frac{\sqrt{x}}{\log x}$. Pour le deuxième terme, on remplace $S(t)$ par son équivalent et on intègre par parties pour obtenir

$$\frac{1}{7}\int_3^x \frac{1}{2\sqrt{t}\log t}dt = \frac{1}{7}\frac{\sqrt{x}}{\log x} + \frac{1}{7}\int_3^x \frac{1}{\sqrt{t}\log^2 t}dt.$$

Le dernier terme est en $o(\frac{\sqrt{x}}{\log x})$. Par conséquent, l'expression donnée est équivalente à $\frac{2}{7}\frac{\sqrt{x}}{\log x}$ lorsque x tend vers l'infini.

Exercice 2 a. Vérifier que le développement en fraction continue de $\sqrt{13}$ est de la forme

$$\sqrt{13} = [a_0; \overline{a_1, a_2, a_3, a_4, a_5}],$$

avec $a_1 = a_2 = a_3 = a_4$.

b. Donner toutes les valeurs de $\xi = x + y\sqrt{13}$ correspondant aux solutions de l'équation

$$x^2 - 13y^2 = 1, \tag{1}$$

où les inconnues x et y sont des entiers ≥ 1.

c. Donner toutes les valeurs de $\xi = x + y\sqrt{13}$ correspondant aux solutions de l'équation

$$x^2 - 13y^2 = -1,$$

où les inconnues x et y sont des entiers ≥ 1.

d. Chaque solution entière de (1) avec $x, y \geq 1$ étant écrite sous la forme $\xi = x + y\sqrt{13}$, quel est le cardinal de l'ensemble

$$\{\xi; \xi \text{ solution de } (1), 1 \leq \xi \leq 10^{10}\}?$$

On donne les valeurs approchées de $\sqrt{13} = 3,60555\ldots$ et du logarithme $\log_{10}(36,02775\ldots) = 1,55663\ldots$

Corrigé :

a. On a $[\sqrt{13}] = [3;(\sqrt{13}-3)^{-1}] = [3;\frac{1}{4}(\sqrt{13}+3)] = [3;1,(\frac{\sqrt{13}-1}{4})^{-1}] = [3;1,\frac{\sqrt{13}+1}{3}] = [3;1,1,(\frac{\sqrt{13}-2}{3})^{-1}] = [3;1,1,\frac{\sqrt{13}+2}{3}] = [3;1,1,1,(\frac{\sqrt{13}-1}{3})^{-1}] = [3;1,1,1,\frac{\sqrt{13}+1}{4}] = [3;1,1,1,1,(\frac{\sqrt{13}-3}{4})^{-1}] = [3;1,1,1,1,\sqrt{13}+3]$
$= [3;1,1,1,1,6,(\sqrt{13}-3)^{-1}] = [3;\overline{1,1,1,1,6}]$.

b. La période de la fraction continue $[3;\overline{1,1,1,1,6}]$ est $s = 5$. Pour $k = 4$, on obtient la solution fondamentale de $x^2 - 13y^2 = \pm 1$: $[3;1,1,1,1] = [3;1,1,2] = [3;1,3/2] = [3;5/3] = 18/5$. On voit que $18^2 - 135^2 = 324 - 325 = -1$. Par conséquent, les solutions $x_k + \sqrt{13}y_k$ de $x^2 - 13y^2 = 1$ sont les puissances paires de cette solution : $x_k + \sqrt{13}y_k = (18 + \sqrt{13}\ 5)^{2k}$ pour $k \geq 1$.

c. Les solutions $x_k + \sqrt{13}y_k$ de $x^2 - 13y^2 = -1$ sont les puissances impaires de la solution fondamentale : $x_k + \sqrt{13}y_k = (18 + \sqrt{13}\ 5)^{2k-1}$ pour $k \geq 1$.

d. On cherche k tel que $(18 + \sqrt{13}\ 5)^{2k} < 10^{10}$, ou encore $k < \frac{1}{2}\frac{10}{\log_{10}(18+\sqrt{13}\ 5)}$. Or $18 + \sqrt{13}\ 5 = 36,0277\ldots$ donc $k < \frac{5}{1,55663\ldots}$. Il n'y a donc que $k = 1, 2, 3$ qui convient et le cardinal recherché est 3.

Exercice 3 Soit $K := \mathbb{Q}(\sqrt{-31})$ et soit $\mathcal{O}_K$ l'anneau d'entiers correspondant.

a. En utilisant sans les redémontrer les résultats du cours, donner le discriminant de K (sur $\mathbb{Q}$) et déterminer $\omega \in \mathcal{O}_K$ tel qu'on ait l'égalité

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot \omega.$$

b. A quel groupe bien connu le groupe de classes d'idéaux de $\mathcal{O}_K$ est-il isomorphe ?

c. Soit

$$I := 2 \cdot \mathbb{Z} \oplus \left(\frac{1+\sqrt{-31}}{2}\right) \cdot \mathbb{Z}.$$

(i) Prouver que I est un idéal de $\mathcal{O}_K$.

(ii) Quelle est la norme de I ?

(iii) Quelle est la forme quadratique binaire réduite associée à I ?

(iv) L'idéal I est-il principal ?

d. Trouver le plus petit entier $k_0 \geq 1$ tel que I^{k_0} soit principal. Trouver alors $\alpha \in \mathcal{O}_K$ tel que $I^{k_0} = \alpha \cdot \mathcal{O}_K$.

e. Montrer que $I\overline{I} = 2 \cdot \mathcal{O}_K$, où $\overline{I} = 2 \cdot \mathbb{Z} \oplus \left(\frac{1-\sqrt{-31}}{2}\right) \cdot \mathbb{Z}$.

f. Existe-t-il un idéal J de $\mathcal{O}_K$ non principal tel que J^5 soit principal ?

g. Existe-t-il un idéal de $\mathcal{O}_K$ de norme 3 ?

Corrigé :

a. Comme $-31 \equiv 1\,[4]$, il s'agit du discriminant de K et $\mathcal{O}_K = \mathbb{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{-31}}{2}$. On peut donc prendre $\omega = \frac{1+\sqrt{-31}}{2}$.

b. Calculons $h_K = h(-31)$, c'est-à-dire le nombre de formes quadratiques binaires réduites définies positives $[a, b, c]$ de discriminant -31. On a $-a < b \leq a \leq c$ avec $0 < a \leq \sqrt{\frac{31}{3}}$ donc $a = 1, 2$ ou 3. Comme $b^2 - 4ac = -31$, il faut que b soit impair. Si $a = 1$, on doit avoir $b = 1$ et donc $1 - 4c = -31$ et $c = 8$, ce qui donne $[1, 1, 8]$. Si $a = 2$, on doit avoir $b = \pm 1$ et $1 - 8c = -31$ de sorte que $c = 4$. On obtient donc $[2, \pm 1, 4]$. Si $a = 3$, on doit avoir $b = -1, 1$ ou 3. Si $b = \pm 1$, $b^2 - 4ac = 1 - 12c = -31$ n'a pas de solution entière.Si $b = 3$, $b^2 - 4ac = 9 - 12c = -31$ n'a pas de solution entière non plus. Puisqu'on a trouvé 3 formes quadratiques, $h_K = h(-31) = 3$. Le seul groupe d'ordre 3 est $\mathbb{Z}/3\mathbb{Z}$.

c.
- Il faut vérifier que $\omega I \subset I$. Mais $2 \cdot \omega \in I$ clairement et $\omega^2 = \frac{-15+\sqrt{-31}}{2} = -4 \cdot 2 + \omega \in I$ également.
- Le quotient $\mathcal{O}_K/I$ est $\cdot\mathbb{Z} \oplus \left(\frac{1+\sqrt{-31}}{2}\right) \cdot \mathbb{Z}/2 \cdot \mathbb{Z} \oplus \left(\frac{1+\sqrt{-31}}{2}\right) \cdot \mathbb{Z} = \mathbb{Z}_2$ donc la norme de I est 2.
- Prenons $\alpha_1 = 2$ et $\alpha_2 = -\frac{1+\sqrt{-31}}{2}$, de sorte que $\alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1} = 2\sqrt{-31}$ (base directe). On obtient la forme quadratique $q_\alpha(x, y) = \frac{1}{2}N_{K/\mathbb{Q}}(x\alpha_1 + y\alpha_2) = \frac{1}{2}|(2x - \frac{y}{2}) - \frac{y}{2}\sqrt{-31}|^2 = 2x^2 - xy + \frac{1}{8}y^2 + \frac{31}{8}y^2 = 2x^2 - xy + 4y^2$, c'est-à-dire la forme quadratique $[2, -1, 4]$.
- Si I était principal, donc de la forme $\beta\mathcal{O}_K$, on aurait $N(I) = 2 = N_{K/\mathbb{Q}}(\beta)$. Avec $\beta = \frac{x+y\sqrt{-31}}{2}$ et $x, y \in \mathbb{Z}$, cela donne $x^2 + 31y^2 = 8$ mais n'a pas de solution entière. Donc I n'est pas principal. Alternativement, si I était principal, la forme quadratique associée serait la même que pour $\mathcal{O}_K$, à savoir $[1, 1, 8]$, mais la question précédente montre que ce n'est pas le cas.

d. Comme $h_K = 3$, tout idéal non principal est d'ordre 3 dans le groupe des classes, c'est donc le cas de I est on a $k_0 = 3$. Donc $I^3 = \beta\mathcal{O}_K$ avec $\beta = \frac{x+y\sqrt{-31}}{2}$ et $x, y \in \mathbb{Z}$, cela donne $x^2+31y^2 = 32$, qui a pour solutions $x, y = \pm 1$. Donc $\beta = \frac{1+\sqrt{-31}}{2}$ ou $\beta = \frac{1-\sqrt{-31}}{2}$. Mais le premier est dans I et pas le second, donc on a $\beta = \frac{1+\sqrt{-31}}{2}$.

e. En argumentant comme pour I, on voit que $\overline{I}$ n'est pas principal, et que sa forme quadratique est $[2, 1, 4]$. Par conséquent, dans le groupe $\mathbb{Z}/3\mathbb{Z}$, c'est forcément l'inverse de I, de sorte que $I\overline{I} = \beta\mathcal{O}_K$ avec $\beta = \frac{x+y\sqrt{-31}}{2}$ et $x, y \in \mathbb{Z}$. La norme de cet idéal étant $2^2 = 4$, on doit avoir $x^2 + 31y^2 = 16$, dont les solutions entières sont $x = \pm 2$ et $y = 0$. Donc on a $\beta = 2$.

f. Comme 5 ne divise pas $h_K = 3$, il n'existe pas d'idéal J non principal tel que J^5 est principal.

g. Si on a un idéal d'ordre 3, alors 3 est représenté par l'une des 3 formes quadratiques que nous avons déterminées plus haut. Comme 3 est sans facteur carré, il est même représenté primitivement. Mais pour $[1, 1, 8]$ et $[2, \pm 1, 4]$ nous avons à chaque fois $0 < a < 3 < c$, or les deux premiers entiers représentés primitivement sont a et c. Donc il n'existe pas d'idéal d'ordre 3.