Examen partiel d'Arithmétique

Mercredi 28 février 2024. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

Exercice 1 Résoudre dans $\mathbb{Z}^3$ l'équation $6x + 10y + 15z = 7$.

Corrigé : La solution particulière $(7, 7, -7)$ saute aux yeux. Posons $x' = x - 7$, $y' = y-7$ et $z' = z+7$, de sorte qu'il reste à résoudre $6x'+10y' = -15z'$. Comme le pgcd de 6 et 10 est 2, cette solution a des solutions ssi z' est pair : $z' = 2\lambda_1$ avec λ_1 entier. Il reste alors $3x'+5y' = -15\lambda_1$. Les solutions sont de la forme $x' = x_0+5\lambda_2$, $y' = y_0 - 3\lambda_2$ avec λ_2 entier et (x_0, y_0) une solution particulière. On peut prendre $(x_0, y_0) = -15\lambda_1(2, -1)$. On obtient ainsi $x' = -30\lambda_1 + 5\lambda_2$, $y' = 15\lambda_1 - 3\lambda_2$ et $z' = 2\lambda_1$, ou encore $x = 7 - 30\lambda_1 + 5\lambda_2$, $y = 7 + 15\lambda_1 - 3\lambda_2$ et $z = -7 + 2\lambda_1$ avec λ_1, λ_2 entiers quelconques.

Exercice 2 Soit p un nombre premier. Montrer que

$$1^k + 2^k + \ldots + (p-1)^k \equiv \begin{cases} -1 \bmod p & \text{si } p-1 \mid k, \\ 0 \bmod p & \text{sinon.} \end{cases}$$

Indication : écrire les termes m^k modulo p au moyen d'un générateur de $\mathbb{F}_p^\times$.

Corrigé : Soit g un générateur du groupe multiplicatif $\mathbb{F}_p^\times$, de sorte que $\{1, \ldots, p-1\} = \{1, g, g^2 \ldots, g^{p-2}\}$. Si $p-1 \mid k$, alors $g^k = 1$ et $\sum_{m=1}^{p-1} m^k = \sum_{i=0}^{p-2} g^{ik} = p - 1 \equiv -1 \bmod p$. Sinon, $g^k \neq 1$ et $\sum_{m=1}^{p-1} m^k = \sum_{i=0}^{p-2} g^{ik} = \frac{g^{k(p-1)}-1}{g^k-1} = 0$ puisque $g^{k(p-1)} = 1$.

Exercice 3 Soit $n \in \mathbb{N}^*$. On considère $T = \{(k, d) \in \mathbb{N}^2 : d \mid n, 1 \leq k \leq d, k \wedge d = 1\}$ et $S = \{\frac{kn}{d} \in \mathbb{N}^* : (k, d) \in T\}$.

1. Montrer que $\mathrm{Card}(T) = n$.
2. En déduire que $S = \{1, \ldots, n\}$.

Soit F une fonction arithmétique de la forme $F(n) = \sum_{k=1}^n f(\frac{k}{n})$ pour une fonction $f : \mathbb{Q} \cap [0, 1] \to \mathbb{C}$. On considère la fonction de Möbius μ.

3. Montrer en utilisant l'ensemble S que $G = \mu * F$ satisfait

$$G(n) = \sum_{\substack{k=1 \\ k \wedge n = 1}}^{n} f\left(\frac{k}{n}\right).$$

Pour tout $k \in \mathbb{N}$, on définit une généralisation

$$\varphi_k(n) = \sum_{\substack{m=1 \\ m \wedge n = 1}}^{n} m^k$$

de la fonction indicatrice d'Euler φ.

4. Montrer que
$$\sum_{d|n} \frac{\varphi_k(d)}{d^k} = \frac{1^k + \ldots + n^k}{n^k}.$$

5. En déduire que $\varphi_1(n) = \frac{1}{2} n \varphi(n)$ lorsque $n \geq 2$ et que le produit des générateurs du groupe multiplicatif $\mathbb{F}_p^\times$ avec p premier impair est $(-1)^{\varphi(p-1)}$.

Corrigé :

1. Pour d fixé, $(k,d) \in T$ ssi $1 \leq k \leq d$ et $k \wedge d = 1$ de sorte que $\mathrm{Card}(T) = \sum_{d|n} \varphi(d) = \varphi * \mathbb{1}(n)$. Or $\varphi = \mu * \mathrm{Id}$ de sorte que $\varphi * \mathbb{1} = \mathrm{Id}$ et donc $\mathrm{Card}(T) = n$.
2. Si $(k,d) \in T$, alors $k \leq d$ de sorte que $\frac{kn}{d} \leq n$, donc $S \subset \{1, \ldots, n\}$. Soient $(k_1, d_1), (k_2, d_2) \in T$ tels que $\frac{k_1 n}{d_1} = \frac{k_2 n}{d_2}$ ou encore $k_1 d_2 = k_2 d_1$. Comme $k_1 \wedge d_1 = 1$, on a $k_1 \mid k_2$. Symétriquement, on a aussi $k_2 \mid k_1$ de sorte que $k_1 = k_2$ et donc aussi $d_1 = d_2$. Par conséquent, $\mathrm{Card}(S) = \mathrm{Card}(T) = n$ et l'inclusion $S \subset \{1, \ldots, n\}$ doit être une égalité.
3. Montrons plutôt que $\mathbb{1} * G = F$, ce qui est équivalent à $G = \mu * F$. On a
$$\begin{aligned} \mathbb{1} * G(n) = \sum_{d|n} G(d) &= \sum_{d|n} \sum_{\substack{k=1 \\ k \wedge d = 1}}^{d} f\left(\frac{1}{n}\frac{kn}{d}\right) = \sum_{(k,d) \in T} f\left(\frac{1}{n}\frac{kn}{d}\right) = \sum_{i \in S} f\left(\frac{i}{n}\right) \\ &= \sum_{i=1}^{n} f\left(\frac{i}{n}\right) = F(n). \end{aligned}$$

4. Posons $F(n) = \sum_{m=1}^{n} \left(\frac{m}{n}\right)^k$ et appliquons la propriété que nous venons de montrer. On obtient
$$F(n) = \mathbb{1} * G(n) = \sum_{d|n} G(d) = \sum_{d|n} \sum_{\substack{m=1 \\ m \wedge n = 1}}^{d} \left(\frac{m}{d}\right)^k = \sum_{d|n} \frac{\varphi_k(d)}{d^k},$$
ce qui est l'identité souhaitée.
5. Lorsque $k = 1$, l'identité ci-dessus donne $\sum_{d|n} \frac{\varphi_1(d)}{d} = \frac{n+1}{2}$. En d'autres termes, $\frac{1}{n}\varphi_1 * \mathrm{Id}(n) = \frac{n+1}{2}$. Comme $\mu * \mathbb{1} = e$ et Id est complétement multiplicative, on a $\mathrm{Id} \cdot (\mu * \mathbb{1}) = (\mathrm{Id} \cdot \mu) * \mathrm{Id} = \mathrm{Id} \cdot e = e$. Donc la relation précédente

pour φ_1 donne $\varphi_1 = g * (\mathrm{Id} \cdot \mu)$ où $g(n) = \frac{n(n+1)}{2}$. On obtient

$$\begin{aligned}\varphi_1(n) &= \sum_{d|n} \frac{d(d+1)}{2} \mu\left(\frac{n}{d}\right) \frac{n}{d} = \frac{n}{2} \sum_{d|n} (d+1)\mu\left(\frac{n}{d}\right) \\ &= \frac{n}{2}(\mathrm{Id} * \mu(n) + \mathbb{1} * \mu(n)) = \frac{n}{2}(\varphi(n) + e(n)) = \frac{n}{2}\varphi(n).\end{aligned}$$

Soit g un générateur de $\mathbb{F}_p^\times$. Les autres générateurs sont les éléments g^k avec $1 \leq k \leq p-2$ et $k \wedge (p-1) = 1$. Leur produit est donc g^N avec

$$N = \sum_{\substack{k=1 \\ k \wedge (p-1) = 1}}^{p-2} k = \varphi_1(p-1) = \frac{p-1}{2}\varphi(p-1).$$

Comme $g^{\frac{p-1}{2}} = -1$ puisque son carré est 1 mais pas lui-même, on obtient bien le produit $g^N = (-1)^{\varphi(p-1)}$ annoncé.

Exercice 4 Soit $b > 2$ entier impair et non divisible par un carré parfait > 1. On considère les ensembles $S_\pm(b) = \{m \in \mathbb{N}^* : 1 \leq m \leq b, \left(\frac{m}{b}\right) = \pm 1\}$ où $\left(\frac{m}{b}\right)$ désigne le symbole de Jacobi.

1. Montrer que $S_-(b) \neq \emptyset$.
2. En déduire que $\sum_{k=1}^{b} \left(\frac{k}{b}\right) = 0$ et que $\mathrm{Card} S_\pm(b) = \frac{1}{2}\varphi(b)$.

Soit p premier tel que $p \nmid b$ et $p \equiv 1 \bmod 4$.

3. Montrer que b est un résidu quadratique modulo p si et seulement si il existe $c \in S_+(b)$ tel que $b \mid p - c$.
4. Caractériser les nombres premiers impairs modulo lesquels 21 est un résidu quadratique, et lister ceux qui sont inférieurs à 50.

Corrigé :

1. Puisque $b > 2$ est impair et ne contient aucun facteur carré, $b = p_1 \dots p_k$ où les p_i sont des entiers premiers impairs distincts et $k \geq 1$. Prenons m solution du système de congruences suivant :

$$\begin{cases} m \equiv 1 \mod p_i, i = 1, \dots, k-1, \\ m \equiv s \mod p_k, \end{cases}$$

où s satisfait $\left(\frac{s}{p_k}\right) = -1$. Un tel s existe par les propriétés du symbole de Legendre. Par le théorème des restes chinois, ce système a une unique solution m modulo $p_1 \dots p_k = b$. On a alors

$$\left(\frac{m}{b}\right) = \left(\frac{m}{p_1}\right) \dots \left(\frac{m}{p_{k-1}}\right)\left(\frac{m}{p_k}\right) = 1 \dots 1(-1) = -1.$$

Donc $m \in S_-(b) \neq \emptyset$.

2. Soit m l'entier modulo b obtenu ci-dessus. Comme $\left(\frac{m}{b}\right) \neq 0$, on a $m \wedge b = 1$ de sorte que m est inversible modulo b. En particulier, la multiplication par m induit une permutation de $(\mathbb{Z}/b\mathbb{Z})^\times$.

   On calcule alors

$$\sum_{k=1}^{b} \left(\frac{k}{b}\right) = \sum_{k=1}^{b} \left(\frac{mk}{b}\right) = \sum_{k=1}^{b} \left(\frac{m}{b}\right)\left(\frac{k}{b}\right) = -\sum_{k=1}^{b} \left(\frac{k}{b}\right),$$

   de sorte que $\sum_{k=1}^{b} \left(\frac{k}{b}\right) = 0$.

   Dans la somme ci-dessus, les seuls termes non nuls sont ceux pour lesquels $k \wedge b = 1$, et ces termes sont égaux à ± 1. Il y a $\varphi(b)$ tels termes, et puisque leur somme est nulle, on doit en avoir autant de positifs que de négatifs, ce qui donne $\frac{1}{2}\varphi(b)$ termes de chaque signe.

3. Supposons qu'il existe $c \in S_+(b)$ tel que $b \mid p - c$, ou encore $p \equiv c \bmod b$. Alors $\left(\frac{p}{b}\right) = \left(\frac{c}{b}\right) = 1$. Par la loi de réciprocité quadratique, on a alors

$$\left(\frac{b}{p}\right) = (-1)^{\frac{p-1}{2}\frac{b-1}{2}} \left(\frac{p}{b}\right) = 1.$$

   Comme $\left(\frac{b}{p}\right) = 1$ est un symbole de Legendre, ceci signifie que b est un résidu quadratique modulo p.

   Réciproquement, si b est un résidu quadratique modulo p, alors $\left(\frac{b}{p}\right) = 1$. Comme ci-dessus, la loi de réciprocité quadratique donne alors $\left(\frac{p}{b}\right) = 1$, de sorte que $p \bmod b$ est un élément de $S_+(b)$. En d'autres termes, il existe $c \in S_+(b)$ tel que $p = c + kb$ avec k entier, et donc $b \mid p - c$.

4. Déterminons les $\frac{1}{2}\varphi(21) = 6$ éléments de $S_+(21)$. Tout $c \in S_+(21)$ satisfait $\left(\frac{c}{21}\right) = \left(\frac{c}{3}\right)\left(\frac{c}{7}\right) = 1$, de sorte que soit $\left(\frac{c}{3}\right) = \left(\frac{c}{7}\right) = 1$, soit $\left(\frac{c}{3}\right) = \left(\frac{c}{7}\right) = -1$. Dans le premier cas, on a $c \equiv 1 \bmod 3$ et $c \equiv 1, 2$ ou $4 \bmod 7$, de sorte que $c \equiv 1, 16$ ou $4 \bmod 21$. Dans le deuxième cas, on a $c \equiv 2 \bmod 3$ et $c \equiv 3, 5$ ou $6 \bmod 7$, de sorte que $c \equiv 17, 5$ ou $20 \bmod 21$. On obtient donc $S_+(21) = \{1, 4, 5, 16, 17, 20\}$.

   Si $p = 3$ ou 7, 21 est trivialement un résidu quadratique modulo p. Si 21 est un résidu quadratique modulo $p \neq 3, 7$, on remarque que comme $\frac{21-1}{2} = 10$ est pair, la loi de réciprocité quadratique donne $1 = \left(\frac{21}{p}\right) = \left(\frac{p}{21}\right)$, de sorte que $p \equiv 1, 4, 5, 16, 17$ ou $20 \bmod 21$. En plus de 3 et 7, on obtient donc les nombres premiers $5, 17, 37, 41, 43$ et 47 entre 3 et 50.

Exercice 5 Soit p premier impair. Pour $\chi_1, \dots, \chi_k \in \widehat{\mathbb{F}_p^\times}$, on définit

$$J(\chi_1, \dots, \chi_k) = \sum_{\substack{(c_1,\dots,c_k)\in\mathbb{F}_p^k \\ c_1+\dots+c_k=1}} \chi_1(c_1)\dots\chi_k(c_k).$$

1. Montrer que, si il existe $\alpha, \beta \in \{1, \dots, k\}$ tels que χ_α est trivial et χ_β est non trivial, alors $J(\chi_1, \dots, \chi_k) = 0$.
2. Montrer que, si $\chi_1, \dots, \chi_k$ ainsi que le produit $\chi_1 \dots \chi_k$ sont non triviaux, alors
$$g_1(\chi_1)\dots g_1(\chi_k) = J(\chi_1, \dots, \chi_k) g_1(\chi_1 \dots \chi_k),$$
où $g_1(\chi)$ désigne la somme de Gauss du caractère χ.
3. Si k est impair et $a_1, \dots, a_k \in \mathbb{F}_p^\times$, montrer que le nombre de solutions de l'équation $a_1x_1^2 + \dots + a_kx_k^2 = 1$ dans $\mathbb{F}_p^k$ est égal à
$$p^{k-1} + \left(\frac{a_1}{p}\right)\dots\left(\frac{a_k}{p}\right)(-1)^{\frac{k-1}{2}\frac{p-1}{2}} p^{\frac{k-1}{2}}.$$

Corrigé :

1. Comme $J(\chi_1, \dots, \chi_k)$ ne dépend pas de l'ordre des caractères $\chi_1, \dots, \chi_k$, on peut supposer sans perte de généralité que $\chi_1 = e$ et $\chi_2 \neq e$. Alors
$$\begin{aligned} J(\chi_1, \dots, \chi_k) &= \sum_{\substack{(c_1,\dots,c_k)\in\mathbb{F}_p^k \\ c_1+\dots+c_k=1}} \chi_2(c_2)\dots\chi_k(c_k) = \sum_{(c_2,\dots,c_k)\in\mathbb{F}_p^{k-1}} \chi_2(c_2)\dots\chi_k(c_k) \\ &= \left(\sum_{c\in\mathbb{F}_p}\chi_2(c)\right) \sum_{(c_3,\dots,c_k)\in\mathbb{F}_p^{k-2}} \chi_3(c_3)\dots\chi_k(c_k), \end{aligned}$$
puisque $c_1 = 1 - c_2 \dots - c_k$. Comme $\sum_{c\in\mathbb{F}_p}\chi_2(c) = 0$ pour un caractère non trivial, on obtient le résultat souhaité.
2. Posons $\zeta_p = e^{\frac{2\pi i}{p}}$. Par définition, $g_1(\chi_i) = \sum_{t\in\mathbb{F}_p}\chi_i(t)\zeta_p^t$. Par conséquent,
$$\begin{aligned} g_1(\chi_1)\dots g_1(\chi_k) &= \sum_{(t_1,\dots,t_k)\in\mathbb{F}_p^k} \chi_1(t_1)\dots\chi_k(t_k)\zeta_p^{t_1+\dots+t_k} \\ &= \sum_{t\in\mathbb{F}_p}\zeta_p^t \sum_{\substack{(t_1,\dots,t_k)\in\mathbb{F}_p^k \\ t_1+\dots+t_k=t}} \chi_1(t_1)\dots\chi_k(t_k). \end{aligned}$$
Etudions séparément le terme avec $t = 0$, pour lequel on a $t_k = -t_1 \dots - t_{k-1}$ de sorte que
$$\sum_{\substack{(t_1,\dots,t_k)\in\mathbb{F}_p \\ t_1+\dots+t_k=0}} \chi_1(t_1)\dots\chi_k(t_k) = \sum_{t_k\in\mathbb{F}_p^\times} \left(\sum_{\substack{(t_1,\dots,t_{k-1})\in\mathbb{F}_p^{k-1} \\ t_1+\dots+t_{k-1}=-t_k}} \chi_1(t_1)\dots\chi_{k-1}(t_{k-1}) \right) \chi_k(t_k)$$

où on peut retirer le terme en $t_k = 0$ puisque $\chi_k \neq e$. En posant $u_i = -t_k^{-1} t_i$ pour $i = 1, \dots, k-1$, cette expression devient

$$\sum_{t_k \in \mathbb{F}_p^\times} \left(\sum_{\substack{(u_1,\dots,u_{k-1}) \in \mathbb{F}_p^{k-1} \\ u_1+\dots+u_{k-1}=1}} \chi_1(u_1) \dots \chi_{k-1}(u_{k-1}) \right) (\chi_1 \dots \chi_k)(-t_k) \chi_k(-1)$$

mais comme $\sum_{t_k \in \mathbb{F}_p^\times} (\chi_1 \dots \chi_k)(-t_k) = 0$ puisque $\chi_1 \dots \chi_k \neq e$, on ne garde que les termes avec $t \in \mathbb{F}_p^\times$ dans le calcul plus haut, et en posant $u_i = t^{-1} t_i$ pour $i = 1, \dots, k$, on obtient

$$\begin{aligned} g_1(\chi_1) \dots g_1(\chi_k) &= \sum_{t \in \mathbb{F}_p^\times} \zeta_p^t (\chi_1 \dots \chi_k)(t) \sum_{\substack{(u_1,\dots,u_k) \in \mathbb{F}_p^k \\ u_1+\dots+u_k=1}} \chi_1(u_1) \dots \chi_k(u_k) \\ &= \sum_{t \in \mathbb{F}_p} \zeta_p^t (\chi_1 \dots \chi_k)(t) J(\chi_1, \dots, \chi_k) \\ &= g_1(\chi_1 \dots \chi_k) J(\chi_1, \dots, \chi_k), \end{aligned}$$

puisque $\chi_1 \dots \chi_k \neq e$ de sorte que le terme absent avec $t = 0$ est nul.

3. Calculons le nombre $N(a_1 x_1^2 + \dots + a_k x_k^2 = 1)$ de solutions recherché.

$$\begin{aligned} &N(a_1 x_1^2 + \dots + a_k x_k^2 = 1) \\ &= \sum_{\substack{(t_1,\dots,t_k) \in \mathbb{F}_p^k \\ a_1 t_1 + \dots + a_k t_k = 1}} N(x_1^2 = t_1) \dots N(x_k^2 = t_k) \\ &= \sum_{\substack{(t_1,\dots,t_k) \in \mathbb{F}_p^k \\ a_1 t_1 + \dots + a_k t_k = 1}} \left(1 + \left(\frac{t_1}{p}\right)\right) \dots \left(1 + \left(\frac{t_k}{p}\right)\right) \\ &= \sum_{\substack{(u_1,\dots,u_k) \in \mathbb{F}_p^k \\ u_1 + \dots + u_k = 1}} \left(1 + \left(\frac{a_1^{-1}}{p}\right)\left(\frac{u_1}{p}\right)\right) \dots \left(1 + \left(\frac{a_k^{-1}}{p}\right)\left(\frac{u_k}{p}\right)\right) \end{aligned}$$

en posant $u_i = a_i t_i$ pour $i = 1, \dots, k$. En vertu de la première propriété ci-dessus pour $J(\chi_1, \dots, \chi_k)$ avec au moins un $\chi_i = e$ et au moins un χ_j égal au symbole de Legendre, l'expression ci-dessus ne garde que les termes où tous les χ_i sont tous égaux à e ou tous égaux au symbole de Legendre $\psi(\cdot) = \left(\frac{\cdot}{p}\right)$. Cela donne

$$\begin{aligned} N(a_1 x_1^2 + \dots + a_k x_k^2 = 1) &= J(e, \dots, e) + \psi(a_1 \dots a_k)^{-1} J(\psi, \dots, \psi) \\ &= p^{k-1} + \psi(a_1 \dots a_k)^{-1} \frac{g_1(\psi)^k}{g_1(\psi^k)} \\ &= p^{k-1} + \psi(a_1 \dots a_k) g_1(\psi)^{k-1} \end{aligned}$$

en vertu de la deuxième propriété ci-dessus de $J(\chi_1, \ldots, \chi_k)$ parce que k est impair, de sorte que $\psi^k = \psi \neq e$. On sait que le carré de la somme de Gauss quadratique est donné par $g_1(\psi)^2 = (-1)^{\frac{p-1}{2}} p$ de sorte que

$$N(a_1 x_1^2 + \ldots + a_k x_k^2 = 1) = p^{k-1} + \left(\frac{a_1}{p}\right) \ldots \left(\frac{a_k}{p}\right) (-1)^{\frac{p-1}{2}\frac{k-1}{2}} p^{\frac{k-1}{2}}.$$