Examen partiel d'Arithmétique

Mercredi 18 février 2026. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

Exercice 1 Soit $a \in \mathbb{Z}$. On considère le système de congruences

$$\begin{cases} x & \equiv & a & \mod 15, \\ x & \equiv & 10 & \mod 63. \end{cases}$$

1. Pour quelles valeurs de a ce système admet-il au moins une solution $x \in \mathbb{Z}$?
2. Pour de telles valeurs de a, combien de solutions $x \in \mathbb{Z} \cap [1, 945]$ possède ce système ?
3. Déterminer l'ensemble des solutions de ce système en fonction de a.

Corrigé :

1. Par le théorème des restes chinois, la première congruence est équivalente à $x \equiv a \bmod 3$ et $x \equiv a \bmod 5$, tandis que la deuxième congruence est équivalente à $x \equiv 10 \bmod 7$ et $x \equiv 10 \bmod 9$, ou encore $x \equiv 3 \bmod 7$ et $x \equiv 1 \bmod 9$. En particulier, la dernière congruence donne $x \equiv 1 \bmod 3$ et une comparaison avec la première congruence impose $a \equiv 1 \bmod 3$ pour avoir au moins une solution. Réciproquement, si $a \equiv 1 \bmod 3$, la première congruence est une conséquence de la dernière, et le système est équivalent aux 3 autres congruences, modulo 5, 7 et 9. Comme ces entiers sont premiers entre eux, ce système de congruence est équivalent à une unique congruence, qui a donc des solutions.
2. Plus précisément, le système est équivalent à une unique congruence modulo $5 \cdot 7 \cdot 9 = 315$. Comme $945 = 3 \cdot 315$, une classe de congruence modulo 315 est représentée par trois entiers dans $[1, 945]$, donc on obtient trois solutions.
3. Supposons que $a \equiv 1 \bmod 3$, car sinon il n'y a pas de solution. Dans ce cas, il suffit de résoudre le système de congruences constitué de $x \equiv a \bmod 5$ et $x \equiv 10 \bmod 63$. L'équation de Bézout $5k+63\ell = 1$ admet la solution $k = -25$ et $\ell = 2$, de sorte qu'en prenant $\alpha = 63\ell = 126$ et $\beta = 5k = -125$, on a $\alpha \equiv 1 \bmod 5$, $\alpha \equiv 0 \bmod 63$, $\beta \equiv 0 \bmod 5$ et $\beta \equiv 1 \bmod 63$. Le système de congruences est donc équivalent à $x \equiv 126a - 125 \cdot 10 \equiv 126a + 10 \bmod 315$. Les solutions entières sont donc de la forme $x = 126a+10+315k$ avec $k \in \mathbb{Z}$, lorsque $a \equiv 1 \bmod 3$.

Exercice 2 On considère le polynôme $P(X) = X^6 + X^3 + 1$. Pour p premier, on notera $\overline{P}$ la réduction de P modulo p.

1. Ecrire P comme produit de facteurs irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.
2. Utiliser le critère d'Eisenstein pour montrer que P est irréductible dans $\mathbb{Z}[X]$.
3. Vérifier que $\overline{P}$ est réductible dans $\mathbb{F}_p[X]$ et déterminer le nombre de ses facteurs irréductibles lorsque $p = 3$ ou $p \equiv 1 \bmod 9$.
4. Vérifier que $\overline{P}$ s'écrit comme produit de 2 facteurs irréductibles de degré 3 lorsque $p \equiv 4$ ou $7 \bmod 9$.

Corrigé :

1. Remarquons que P est le 9ème polynôme cyclotomique, dont les racines sont les racines 9èmes primitives de l'unité dans $\mathbb{C}$. Dans $\mathbb{C}[X]$, on a donc

$$P(X) = \prod_{\substack{k=1 \\ (k,9)=1}}^{9} (X - \zeta^k)$$

où $\zeta = e^{\frac{2\pi i}{9}}$. Dans $\mathbb{R}[X]$, il suffit de regrouper les 6 racines par paires conjuguées pour obtenir

$$P(X) = \prod_{k \in \{1,2,4\}} \left(X^2 - 2\cos\left(\frac{2\pi k}{9}\right) X + 1 \right).$$

2. Remarquons que $P(X)$ est irréductible si et seulement si $P(X+1)$ l'est. Or $P(X+1) = (X+1)^6 + (X+1)^3 + 1 = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$. Tous coefficients de ce polynôme sont divisibles par 3 sauf le premier, et le dernier n'est pas divisible par 9. Le critère d'Eisenstein s'applique donc pour montrer que $P(X+1)$ est irréductible dans $\mathbb{Q}[X]$ ou, de manière équivalente pour ce polynôme primitif, dans $\mathbb{Z}[X]$.
3. Pour le cas $p = 3$, on a déjà constaté que $P(X) = \Phi_9(X)$, et ceci implique que $P(X) = \Phi_3(X^3)$. Posons $Y = X^3$. Avec des coefficients dans $\mathbb{F}_3$, on a $\overline{\Phi}_3(Y) = (Y-1)^2$, de sorte que $\overline{P}(X) = (X^3 - 1)^2 = (X-1)^{3\cdot 2}$. Par conséquent, $\overline{P}(X) = (X-1)^6$.
   Si $p \equiv 1 \bmod 9$, c'est-à-dire si $9 \mid p - 1$, il existe un élément g d'ordre 9 dans $\mathbb{F}_p$. De plus, pour $1 \leqslant k \leqslant 8$, g^k est également d'ordre 9 si $k \wedge 9 = 1$, on obtient donc $\varphi(9) = 6$ racines distinctes pour $\overline{P}$, qui s'écrit donc comme produit de 6 polynômes de degré 1.
4. Si $p \equiv 4$ ou $7 \bmod 9$, alors $3 \mid p - 1$ mais $9 \nmid p - 1$. Ainsi, $\mathbb{F}_p^\times$ contient un élément g d'ordre 3, mais pas d'élément d'ordre 9, donc pas de racine pour $\overline{P}$. Ce polynôme se factorise donc comme $\overline{P}(X) = (X^3 - g)(X^3 - g^2)$, puisque c'est bien $X^6 - (g + g^2)X^3 + g^3 = X^6 + X^3 + 1$. En effet, $g^3 = 1$ et $g^2 + g = -1$ puisque $g \neq 1$ est racine de $\Phi_3(X) = X^2 + X + 1$ dans $\mathbb{F}_p[X]$. De plus, chaque facteur de degré 3 est irréductible car il n'a pas de racine.

Exercice 3 On considère la fonction de Möbius μ, et la fonction "nombre de diviseurs premiers" définie par $\omega(n) = \mathrm{Card}\{p \in \mathcal{P} : p \mid n\}$ pour tout $n \in \mathbb{N}^*$. Celles-ci permettent de définir la fonction μ^2 par $\mu^2(n) = (\mu(n))^2$ pour tout $n \in \mathbb{N}^*$ et la fonction 2^ω par $2^\omega(n) = 2^{\omega(n)}$ pour tout $n \in \mathbb{N}^*$.

1. Les fonctions μ^2 et 2^ω sont-elles multiplicatives ? complètement multiplicatives ?
2. Déterminer l'inverse de la fonction μ^2 pour la convolution arithmétique.
3. Démontrer que $2^\omega = \mathbb{1} * \mu^2$.
4. En déduire l'inverse de la fonction 2^ω pour la convolution arithmétique, et l'exprimer au moyen des fonctions arithmétiques évoquées ci-dessus, sans faire apparaître de convolution arithmétique.

Corrigé :

1. La fonction μ est multiplicative, donc μ^2 l'est aussi. Par contre $\mu(p^2) = 0 \neq 1 = \mu(p)^2$ et donc aussi $\mu^2(p^2) \neq (\mu^2(p))^2$, de sorte que μ^2 n'est pas complètement multiplicative.

   Si $m \wedge n = 1$, alors $\omega(mn) = \omega(m) + \omega(n)$, de sorte que 2^ω est multiplicative. Par contre, $\omega(p^2) = \omega(p)$ donc 2^ω n'est pas complètement multiplicative.
2. Comme μ^2 est multiplicative, son inverse f l'est aussi. Il suffit donc de calculer f en p^k avec p premier et $k \geq 1$ entier. On a bien entendu $f(1) = 1$. En évaluant $\mu^2 * f = e$ en p, on obtient $\mu^2(1)f(p) + \mu^2(p)f(1) = 0$, c'est-à-dire $f(p) + f(1) = 0$, donc $f(p) = -1$. Plus généralement, l'évaluation en p^k avec $k \geqslant 2$ donne $f(p^k) + f(p^{k-1}) = 0$, de sorte que $f(p^k) = (-1)^k$. En particulier, f est complètement multiplicative. Ainsi, l'inverse de μ^2 est l'unique fonction complètement multiplicative qui envoie tous les nombres premiers sur -1.
3. Comme $\mathbb{1}$ et μ^2 sont multiplicatives, $\mathbb{1} * \mu^2$ l'est également, ainsi que 2^ω. Il suffit donc de vérifier l'égalité de ces deux fonctions en p^k avec p premier et $k \geq 1$ entier. D'une part, $2^{\omega(p^k)} = 2$. D'autre part, $(\mathbb{1} * \mu^2)(p^k) = \mu^2(1) + \mu^2(p) = 1 + 1 = 2$. On a donc bien l'égalité souhaitée.
4. L'inverse de $\mathbb{1}$ est μ et l'inverse de μ^2 est la fonction f déterminée au point 1. Par associativité du produit de convolution, l'inverse de $\mathbb{1} * \mu^2$ est $\mu * f$. Comme μ et f sont multiplicatives, $\mu * f$ l'est aussi et il suffit de l'évaluer en p^k avec p premier et $k \geq 1$ entier. On obtient $(\mu * f)(p^k) = \mu(1)f(p^k) + \mu(p)f(p^{k-1}) = (-1)^k - (-1)^{k-1} = 2(-1)^k$. On en déduit que l'inverse cherché est $\mu * f = 2^\omega f$.

Exercice 4 On considère la fonction arithmétique $\sigma = \mathbb{1} * \mathrm{Id}$, où $\mathbb{1}$ est la fonction constante égale à 1 et Id est la fonction identité.

1. Démontrer l'identité
$$\sum_{k=1}^{n} \sigma(k) = \frac{1}{2} \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \left(\left\lfloor \frac{n}{k} \right\rfloor + 1 \right).$$
2. En déduire que
$$\sum_{n \leqslant x} \sigma(n) =_{+\infty} \frac{\zeta(2)}{2} x^2 + O(x \log x),$$
où ζ désigne la fonction zêta de Riemann.

Corrigé :

1. On a
$$\sum_{k=1}^{n} \sigma(k) = \sum_{k=1}^{n} \sum_{d|k} d = \sum_{\substack{q,d=1 \\ 1 \leqslant qd \leqslant n}}^{n} d$$
en posant $k = qd$ pour obtenir la dernière égalité. Cela donne
$$\sum_{k=1}^{n} \sigma(k) = \sum_{q=1}^{n} \sum_{d=1}^{\lfloor \frac{n}{q} \rfloor} d = \sum_{q=1}^{n} \frac{1}{2} \left\lfloor \frac{n}{q} \right\rfloor \left(\left\lfloor \frac{n}{q} \right\rfloor + 1 \right)$$
comme souhaité.
2. En utilisant l'encadrement $\frac{n}{k} - 1 \leqslant \left\lfloor \frac{n}{k} \right\rfloor \leqslant \frac{n}{k}$, on obtient
$$\frac{n^2}{2} \sum_{k=1}^{n} \frac{1}{k^2} - \frac{n}{2} \sum_{k=1}^{n} \frac{1}{k} \leqslant \sum_{k=1}^{n} \sigma(k) \leqslant \frac{n^2}{2} \sum_{k=1}^{n} \frac{1}{k^2} + \frac{n}{2} \sum_{k=1}^{n} \frac{1}{k}$$
D'une part, on a $\sum_{k=1}^{n} \frac{1}{k^2} =_{+\infty} \sum_{k=1}^{\infty} \frac{1}{k^2} - \sum_{k=n+1}^{\infty} \frac{1}{k^2} = \zeta(2) + O(\frac{1}{n})$, car $0 < \sum_{k=n+1}^{\infty} \frac{1}{k^2} \leqslant \int_n^{\infty} \frac{1}{y^2} dy = \frac{1}{n}$. D'autre part $\sum_{k=1}^{n} \frac{1}{k} =_{+\infty} \log n + \gamma + O(\frac{1}{n})$, de sorte que
$$\sum_{n \leqslant x} \sigma(n) =_{+\infty} \frac{\zeta(2)}{2} x^2 + O(x \log x),$$
comme souhaité.

Exercice 5 Soit p premier tel que $p \equiv 1 \bmod 4$.

1. Montrer qu'il existe deux éléments χ et $\overline{\chi}$ d'ordre exactement 4 dans $\widehat{\mathbb{F}_p^\times}$.
2. Montrer que $g(\chi)^4 = \chi(-1) p J(\chi, \chi) J(\chi, \chi^2)$ et que $J(\chi, \chi) = \chi(-1) J(\chi, \chi^2)$.
3. Montrer que $g(\chi) = \sqrt{p} e^{i\theta}$ pour un réel θ tel que $p \cos(4\theta)$ est un entier congru à 1 modulo 4.
4. Lorsque $p = 13$, vérifier que le réel θ ci-dessus satisfait $\cos(4\theta) = \frac{5}{13}$.

Corrigé :

1. Le cardinal de $\widehat{\mathbb{F}_p^\times}$ est $p-1$, qui est divisible par 4. On peut donc trouver un élément d'ordre exactement 4 dans ce groupe. Il y a autant d'éléments d'ordre exactement 4 dans $\widehat{\mathbb{F}_p^\times}$ que dans $\mathbb{F}_p^\times$ qui lui est isomorphe, et ces derniers sont les racines du 4ème polynôme cyclotomique $\Phi_4(X) = X^2+1$, qui a exactement deux racines. Si χ est l'un de ces éléments d'ordre 4 dans $\widehat{\mathbb{F}_p^\times}$, l'autre est $\chi^3 = \chi^{-1} = \overline{\chi}$.
2. Comme d'une part $\chi, \chi^2, \chi^3 \neq \varepsilon$, on a

$$J(\chi,\chi) = \frac{g(\chi)^2}{g(\chi^2)} \qquad \text{et} \qquad J(\chi,\chi^2) = \frac{g(\chi)g(\chi^2)}{g(\chi^3)}.$$

D'autre part, comme $\chi^4 = \varepsilon$, on a $g(\chi^3) = g(\overline{\chi}) = \overline{g_{-1}(\chi)} = \overline{\chi(-1)^{-1}g(\chi)}$. On doit avoir $\chi(-1) \in \{-1,+1\}$ puisque -1 est d'ordre 2, donc $g(\chi^3) = \chi(-1)\overline{g(\chi)}$. On en déduit que

$$J(\chi,\chi)J(\chi,\chi^2) = \frac{g(\chi)^3}{\chi(-1)\overline{g(\chi)}} = \frac{g(\chi)^4}{\chi(-1)|g(\chi)|^2} = \frac{1}{p\chi(-1)}g(\chi)^4$$

puisque $|g(\chi)|^2 = p$. C'est la première égalité souhaitée. D'autre part, comme $g(\chi^3) = \chi(-1)\overline{g(\chi)}$, on en déduit que

$$J(\chi,\chi^2) = \chi(-1)\frac{g(\chi)g(\chi^2)}{\overline{g(\chi)}} = \chi(-1)\frac{g(\chi)^2g(\chi^2)}{p}.$$

Comme χ^2 est le symbole de Legendre (unique caractère d'ordre 2), le théorème de Gauss dans le cas où $p \equiv 1 \bmod 4$ donne $g(\chi^2) = \sqrt{p}$. On en déduit que

$$J(\chi,\chi^2) = \chi(-1)\frac{g(\chi)^2}{\sqrt{p}} = \chi(-1)\frac{g(\chi)^2}{g(\chi^2)} = \chi(-1)J(\chi,\chi),$$

c'est la deuxième égalité souhaitée.
3. On peut écrire $J(\chi,\chi) = a+bi$ avec $a,b \in \mathbb{Z}$. Alors $g(\chi)^4 = p(a+bi)^2 = p(a^2-b^2+2abi)$. Comme $|J(\chi,\chi)| = \sqrt{p}$, on a $a^2+b^2 = p$, de sorte que $(a^2-b^2)^2 + (2ab)^2 = p^2$. On en déduit que $g(\chi)^4 = p^2\left(\frac{a^2-b^2}{p} + \frac{2ab}{p}i\right)$, où le nombre complexe entre parenthèses est de module 1. Comme $g(\chi)^4 = p^2e^{4i\theta}$, on en déduit que $\cos(4\theta) = \frac{a^2-b^2}{p} = \frac{2a^2-p}{p}$. Pour conclure, il suffit donc de montrer que $2a^2 - p \equiv 1 \bmod 4$. Comme $p \equiv 1 \bmod 4$, ceci revient à montrer que a est impair. Or

$$a = -\operatorname{Re} J(\chi,\chi^2) = -\sum_{t=1}^{p-1} \operatorname{Re}(\chi(t))\chi^2(1-t).$$

Mais $\mathrm{Re}(\chi(t)) \neq 0$ ssi $\chi(t) = -1$ ou $+1$ ssi $\chi^2(t) = +1$, auquel cas $\mathrm{Re}(\chi(t)) = +1$ ou -1. Il faut donc sommer au signe près les symboles de Legendre $\left(\frac{1-t}{p}\right)$ sur les $\frac{p-1}{2}$ résidus quadratiques t modulo p. Tous valent $+1$ ou -1, sauf lorsque $t = 1$, où ce symbole est nul. Modulo 2, a est donc la somme de $\frac{p-1}{2} - 1$ termes égaux à 1, donc est impair comme souhaité, puisque $p \equiv 1 \bmod 4$.

4. Comme utilisé ci-dessus, on sait déjà que $|g(\chi)| = \sqrt{13}$, de sorte que $g(\chi) = \sqrt{13}e^{i\theta}$ pour un certain réel θ. Remarquons que 2 est un générateur de $\mathbb{F}_{13}^\times$. Quitte à échanger χ et $\overline{\chi}$, on a $\chi(2) = i$ (générateur de μ_4) et en prenant les puissances successives, on a aussi $\chi(4) = -1$, $\chi(8) = -i$, $\chi(3) = 1$, $\chi(6) = i$, $\chi(12) = -1$, $\chi(11) = -i$, $\chi(9) = 1$, $\chi(5) = i$, $\chi(10) = -1$, $\chi(7) = -i$) et bien entendu $\chi(1) = 1$. Ce caractère non trivial s'étend par $\chi(0) = 0$ sur $\mathbb{F}_{13}$. On calcule alors

$$\begin{aligned} J(\chi,\chi) = 2\chi(0)\chi(1) + 2\chi(12)\chi(2) + 2\chi(11)\chi(3) + 2\chi(10)\chi(4) \\ + 2\chi(9)\chi(5) + 2\chi(8)\chi(6) + \chi(7)^2 = 3 + 2i. \end{aligned}$$

Par les relations du point 2, on en déduit que $J(\chi,\chi^2) = -J(\chi,\chi) = -3+2i$ et que $g(\chi)^4 = 13(3-2i)^2 = 13^2\left(\frac{5}{13} - \frac{12}{13}i\right)$, où le nombre complexe entre parenthèses est de module 1. Comme $g(\chi)^4 = 13^2 e^{4i\theta}$, on en déduit que $\cos(4\theta) = \frac{5}{13}$.

Exercice 6 Soit $N \geqslant 2$ un entier et soit χ un caractère de Dirichlet modulo N tel que $\chi(\mathbb{Z}) \not\subset \{0,1\}$.

1. Démontrer que pour tout $a, b \in \mathbb{Z}$ avec $a \leqslant b$, on a

$$\left|\sum_{n=a}^{b} \chi(n)\right| \leqslant \frac{\varphi(N)}{2}.$$

2. Déterminer tous les nombres premiers $p \geqslant 3$ et tous les entiers $b \geqslant 1$ pour lesquels

$$\left|\sum_{n=1}^{b} \left(\frac{n}{p}\right)\right| = \frac{\varphi(p)}{2}.$$

Corrigé :

1. Comme χ ne correspond pas au caractère trivial sur $(\mathbb{Z}/N\mathbb{Z})^\times$, on a $\sum_{n=1}^{N} \chi(n) = 0$. Comme le caractère de Dirichlet χ est périodique de période N, la somme des valeurs de χ sur N entiers consécutifs est toujours nulle. Comme la somme comprend $b - a + 1$ tels termes, on peut supposer sans perte de généralité que $b - a + 1 \leqslant N$, quitte à diminuer b par un multiple positif de N. En

particulier, l'ensemble $I = \{n \in [a,b] \cap \mathbb{Z} : n \wedge N = 1\}$ est de cardinal au plus $\varphi(N)$.

Comme χ est induit par un caractère de $(\mathbb{Z}/N\mathbb{Z})^\times$, toutes ses valeurs non nulles sont de module 1, de sorte que $|\chi(n)| = 1$ pour tout $n \in \mathbb{Z}$ tel que $n \wedge N = 1$.

Commençons par supposer que Card $I \leqslant \frac{N}{2}$. Dans ce cas,

$$\left|\sum_{n=a}^{b} \chi(n)\right| \leqslant \sum_{n=a}^{b} |\chi(n)| = \sum_{n\in I} 1 \leqslant \frac{\varphi(N)}{2}.$$

Si au contraire Card $I > \frac{\varphi(N)}{2}$, alors l'ensemble $J = \{n \in [b+1, a+N-1] \cap \mathbb{Z} : n \wedge N = 1\}$ est de cardinal $\varphi(N) -$ Card $I \leqslant \frac{\varphi(N)}{2}$. On a alors

$$\left|\sum_{n=a}^{b} \chi(n)\right| = \left|\sum_{n=b+1}^{a+N-1} \chi(n)\right| \leqslant \sum_{n=b+1}^{a+N-1} |\chi(n)| = \sum_{n\in J} 1 \leqslant \frac{\varphi(N)}{2}.$$

2. Commençons par étudier le cas où $1 \leqslant b \leqslant p-1$, quitte à diminuer b par un multiple positif de p, ce qui ne change pas la valeur de la somme. Comme $\left(\frac{n}{p}\right) \in \{-1, 0, 1\}$ pour tout $n \in \mathbb{N}^*$, on aura l'égalité dans l'inégalité du point 1 si et seulement si tous les symboles de Legendre non nuls sont de même signe pour $1 \leqslant n \leqslant b$ et si $\{n \in [1,b] \cap \mathbb{Z} : n \wedge p = 1\} = \{1, \ldots, b\}$ est de cardinal $b = \frac{1}{2}\varphi(p) = \frac{p-1}{2}$. Comme $\left(\frac{1}{p}\right) = 1$, il faut donc que $\left(\frac{n}{p}\right) = 1$ pour $n = 1, \ldots, \frac{p-1}{2}$. Ceci implique alors que $\left(\frac{n}{p}\right) = -1$ pour $n = \frac{p+1}{2}, \ldots, p-1$. En particulier, il ne peut y avoir aucun entier carré entre $\frac{p+1}{2}$ et $p-1$. Soit $k \in \mathbb{N}^*$ le plus grand entier tel que $k^2 < \frac{p+1}{2}$, de sorte que $(k+1)^2 > p-1$. La première inégalité donne $p > 2k^2 - 1$ et la seconde $p < k^2 + 2k + 2$. Par transitivité, on obtient $2k^2 - 1 < k^2 + 2k + 2$ ou encore $k^2 - 2k + 1 = (k-1)^2 < 4$, et donc $k < 3$. Si $k = 1$, on doit avoir $1 < p < 5$, de sorte que $p = 3$. Dans ce cas, on a bien $b = 1$ et $\left(\frac{1}{3}\right) = 1 = \frac{1}{2}\varphi(3)$. Si $k = 2$, on doit avoir $7 < p < 10$, ce qui est impossible.

Par conséquent, la seule valeur possible de p est 3, et les valeurs correspondantes de b sont $1 + 3\ell$ avec $\ell \in \mathbb{N}$.