Examen partiel d'Arithmétique

Mercredi 19 février 2025. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

Exercice 1 Combien l'équation

$$x^2 \equiv 113 \bmod 173$$

possède-t-elle de solutions en x modulo 173 ?

Corrigé : Comme 173 est un nombre premier, pour savoir si cette équation possède des solutions, il faut calculer le symbole de Legendre $\left(\frac{113}{173}\right)$. On a

$$\begin{aligned}\left(\frac{113}{173}\right) &= (-1)^{56\cdot 86}\left(\frac{173}{113}\right) = \left(\frac{60}{113}\right) = \left(\frac{2^2}{113}\right)\left(\frac{15}{113}\right) = \left(\frac{15}{113}\right)\\ &= (-1)^{56\cdot 7}\left(\frac{113}{15}\right) = \left(\frac{8}{15}\right) = \left(\frac{2^2}{15}\right)\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\\ &= (-1)(-1) = +1.\end{aligned}$$

Cette équation possède donc $1 + \left(\frac{113}{173}\right) = 2$ solutions.

Exercice 2 Considérons le groupe $G = \widehat{(\mathbb{Z}/80\mathbb{Z})^\times}$ des caractères pour le groupe multiplicatif des inversibles parmi les entiers modulo 80.

1. Calculer le cardinal de G.
2. Montrer que tout $\chi \in G$ prend ses valeurs dans $\{\pm 1, \pm i\}$.
3. Déterminer un nombre fini d'éléments $n_1, \ldots, n_k \in (\mathbb{Z}/80\mathbb{Z})^\times$ et de sous-ensembles finis $E_1, \ldots, E_k \subset \mathbb{C}$ tels que l'application
$$G \to E_1 \times \ldots \times E_k : \chi \mapsto (\chi(n_1), \ldots, \chi(n_k))$$
soit une bijection.
4. Combien de caractères de Dirichlet de module 80 prennent leurs valeurs dans $\{-1, 0, +1\}$?

Corrigé :

1. Le groupe G est isomorphe au groupe multiplicatif $(\mathbb{Z}/80\mathbb{Z})^\times$. Le cardinal de ce dernier est donné par la fonction indicatrice d'Euler, c'est $\varphi(80) = \varphi(2^4 \cdot 5) = 2^3(2-1)(5-1) = 32$.

2. Par le théorème des restes chinois, $(\mathbb{Z}/80\mathbb{Z})^\times \simeq (\mathbb{Z}/2^4\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$. Le facteur $(\mathbb{Z}/5\mathbb{Z})^\times$ est cyclique d'ordre $\varphi(5) = 4$. D'autre part, par un résultat du cours, on a $(\mathbb{Z}/2^4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Ainsi, tous les éléments de $(\mathbb{Z}/80\mathbb{Z})^\times$ et donc aussi de G sont d'ordre divisant 4 : si $n \wedge 80 = 1$, on a donc $\chi(n)^4 = 1$, de sorte que $\chi(n) \in \{\pm 1, \pm i\}$.
3. Les éléments de G sont caractérisés par leurs valeurs sur les générateurs de $(\mathbb{Z}/80\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Déterminons $k = 3$ éléments de $(\mathbb{Z}/80\mathbb{Z})^\times$ induisant des générateurs de chaque facteur. L'élément n_3 induit un générateur de $\mathbb{Z}/5\mathbb{Z}^\times$ et induit le neutre dans $\mathbb{Z}/16\mathbb{Z}^\times$, de sorte que

$$\begin{cases} n_3 & \equiv & 2\,[5], \\ n_3 & \equiv & 1\,[16]. \end{cases}$$

car $\overline{2} \in \mathbb{Z}/5\mathbb{Z}$ est un générateur (autrement dit est d'ordre 4), puisque $\overline{2}^2 = -1 \in \mathbb{Z}/5\mathbb{Z}$. On peut donc prendre $n_3 = \overline{17} \in (\mathbb{Z}/80\mathbb{Z})^\times$. Comme cet élément est d'ordre 4, $\chi(n_3) \in \{\pm 1, \pm i\} = \mu_4 = E_3$ pour tout $\chi \in G$.

L'élément n_2 induit le neutre dans $\mathbb{Z}/5\mathbb{Z}^\times$ et un générateur d'un sous-groupe cyclique d'ordre 4 dans $\mathbb{Z}/16\mathbb{Z}^\times$. On peut prendre $\overline{3} \in \mathbb{Z}/16\mathbb{Z}^\times$ qui est bien d'ordre 4 puisque $\overline{3}^2 = \overline{9} \neq \overline{1} \in \mathbb{Z}/16\mathbb{Z}^\times$. Ainsi,

$$\begin{cases} n_2 & \equiv & 1\,[5], \\ n_2 & \equiv & 3\,[16]. \end{cases}$$

On peut donc prendre $n_2 = \overline{51} \in (\mathbb{Z}/80\mathbb{Z})^\times$. Comme cet élément est d'ordre 4, $\chi(n_2) \in \{\pm 1, \pm i\} = \mu_4 = E_2$ pour tout $\chi \in G$.

L'élément n_1 induit le neutre dans $\mathbb{Z}/5\mathbb{Z}^\times$ et induit un élément d'ordre 2 dans $\mathbb{Z}/16\mathbb{Z}^\times$ qui n'appartient pas au sous-groupe cyclique engendré par n_2. Pour cet élément, on peut donc prendre $\overline{-1} \in \mathbb{Z}/16\mathbb{Z}^\times$, puisque $\overline{3}^2 = \overline{9} \neq \overline{-1} \in \mathbb{Z}/16\mathbb{Z}^\times$. Ainsi,

$$\begin{cases} n_1 & \equiv & 1\,[5], \\ n_1 & \equiv & -1\,[16]. \end{cases}$$

On peut donc prendre $n_1 = \overline{31} \in (\mathbb{Z}/80\mathbb{Z})^\times$. Comme cet élément est d'ordre 2, $\chi(n_1) \in \{\pm 1\} = \mu_2 = E_1$ pour tout $\chi \in G$.

L'application $G \to \mu_2 \times \mu_4 \times \mu_4 : \chi \mapsto (\chi(\overline{31}), \chi(\overline{51}), \chi(\overline{17}))$ ainsi construite est injective par construction. Par cardinalité, elle est donc bijective comme souhaité.
4. Il suffit de se rappeler que les caractères de Dirichlet sont en correspondance bijective avec les caractères de G, et qu'ils sont étendus à des entiers non premiers avec 80 par la valeur 0. Pour qu'un élément $\chi \in G$ prenne ses valeurs dans $\{\pm 1\}$, il faut et il suffit qu'il prenne de telles valeurs sur les

générateurs de $(\mathbb{Z}/80\mathbb{Z})^\times$, par exemple les 3 générateurs calculés ci-dessus. Avec les restrictions imposées, il reste alors 2 valeurs possibles pour chaque générateur, ce qui mène à $2^3 = 8$ caractères de Dirichlet modulo 80.

Exercice 3 On considère la fonction logarithme népérien log, la fonction de Möbius μ et la fonction de von Mangoldt $\Lambda = \log * \mu$. Pour tout entier $k \geq 1$, on définit une fonction arithmétique Λ_k par la relation $\Lambda_k = (\log)^k * \mu$.

1. Démontrer que, pour toutes fonctions arithmétiques f et g, on a
$$(f * g) \cdot \log = (f \cdot \log) * g + f * (g \cdot \log),$$
où la notation $f \cdot g$ désigne le produit usuel des fonctions f et g.
2. En déduire que $-\mu \cdot \log = \mu * \Lambda$.
3. Montrer à partir de tout ce qui précède que, pour tout $k \geq 1$, on a
$$\Lambda_{k+1} = \Lambda_k \cdot \log + \Lambda_k * \Lambda.$$
4. En déduire que si $n \in \mathbb{N}^*$ a strictement plus de k diviseurs premiers distincts, alors $\Lambda_k(n) = 0$, en procédant par récurrence sur k.
5. Rappeler par un résultat énoncé dans le cours pourquoi $M_\Lambda(x) \sim_{+\infty} x$, puis montrer par récurrence sur $k \geq 1$ que
$$M_{\Lambda_k}(x) \sim_{+\infty} kx(\log x)^{k-1}.$$

Corrigé :

1. pour tout $n \in \mathbb{N}^*$, on a
$$\begin{aligned}((f * g) \cdot \log)(n) &= \left[\sum_{d|n} f(d)g(\frac{n}{d})\right] \log(n) = \sum_{d|n} \left[f(d)g(\frac{n}{d}) \left(\log(d) + \log(\frac{n}{d})\right)\right] \\ &= \sum_{d|n} f(d)\log(d)g(\frac{n}{d}) + \sum_{d|n} f(d)g(\frac{n}{d})\log(\frac{n}{d}) \\ &= ((f \cdot \log) * g)(n) + (f * (g \cdot \log))(n).\end{aligned}$$
2. En prenant $f = \mathbb{1}$ et $g = \mu$, la propriété précédente donne
$$(\mathbb{1} * \mu) \cdot \log = (\mathbb{1} \cdot \log) * \mu + \mathbb{1} * (\mu \cdot \log).$$
Mais comme $\mathbb{1} * \mu = e$ et que $e(n) = 0$ si $n > 1$ tandis que $\log(n) = 0$ si $n = 1$, le membre de gauche est identiquement nul. D'autre part, $\mathbb{1} \cdot \log = \log$, et par définition $\log * \mu = \Lambda$. Ainsi, l'équation ci-dessus devient
$$0 = \Lambda + \mathbb{1} * (\mu \cdot \log).$$
En convolant arithmétiquement avec μ, on obtient la relation souhaitée.

3. Pour $k \geq 1$, on a

$$\Lambda_{k+1} = \Big((\log)^k \cdot \log\Big) * \mu = \Big((\log)^k * \mu\Big) \cdot \log - (\log)^k * (\log \cdot \mu)$$

par la propriété du point 1 avec $f = (\log)^k$ et $g = \mu$. En utilisant la définition de Λ_k dans le premier terme et la proprioété du point 2 dans le deuxième terme, on obtient

$$\Lambda_{k+1} = \Lambda_k \cdot \log + (\log)^k * (\mu * \Lambda) = \Lambda_k \cdot \log + \Lambda_k * \Lambda,$$

par associativité de la convolution arithmétique et par définition de Λ_k.

4. Pour $n \in \mathbb{N}^*$, notons $\omega(n)$ le nombre de diviseurs premiers distincts de n. Montrons que $\omega(n) > k$ implique $\Lambda_k(n) = 0$ par récurrence sur $k \geq 1$. Pour $k = 1$, remarquons que $\Lambda_1 = \Lambda$ car les définitions de ces deux fonctions sont identiques. La propriété souhaitée est alors l'une des propriétés de la fonction de von Mangoldt dans le cours.
Supposons maintenant que $\omega(n) > k$ implique $\Lambda_k(n) = 0$, ainsi que $\omega(n) > k + 1$. Par la propriété démontrée plus haut, on a

$$\Lambda_{k+1}(n) = \Lambda_k(n)\log(n) + \sum_{d|n} \Lambda_k(d)\Lambda(\frac{n}{d}).$$

Mais puisque $\omega(n) > k + 1$, on a en particulier $\omega(n) > k$ et donc $\Lambda_k(n) = 0$ par hypothèse de récurrence, de sorte que le premier terme du membre de droite est nul. Pour terminer la démonstration, montrons par l'absurde que tous les termes $\Lambda_k(d)\Lambda(\frac{n}{d})$ de la dernière somme sont nuls. Si $\Lambda_k(d) \neq 0$, la contraposée de l'hypothèse de récurrence donne $\omega(d) \leq k$. Et si $\Lambda(\frac{n}{d}) \neq 0$, cela implique que $\omega(\frac{n}{d}) = 1$. Comme l'ensemble des diviseurs premiers de n est la réunion des ensembles correspondants pour d et pour $\frac{n}{d}$, on en déduit que $\omega(n) \leq \omega(d) + \omega(\frac{n}{d}) \leq k + 1$, c'est la contradiction souhaitée.

5. On a $M_\Lambda = \psi$ par définition de la fonction ψ de Tchebychev. On a montré dans le cours que le comportement asymptotique $\psi(x) \sim_{+\infty} x$ est équivalent à $\pi(x) \sim_{+\infty} \frac{x}{\log x}$, c'est-à-dire au théorème des nombres premiers.
Montrons que $M_{\Lambda_k}(x) \sim_{+\infty} kx(\log x)^{k-1}$ par récurrence sur $k \geq 1$. Pour $k = 1$, on vient de rappeler que $M_{\Lambda_1}(x) = M_\Lambda(x) \sim_{+\infty} x$, ce qui est le comportement asymptotique souhaité. Supposons maintenant que $M_{\Lambda_k}(x)$ a le comportement asymptotique annoncé, et calculons $M_{\Lambda_{k+1}}(x)$ par le lemme

de sommation par parties. Par l'identité établie au point précédent, on a

$$\begin{aligned} M_{\Lambda_{k+1}}(x) &= \sum_{n\leq x}\left[\Lambda_k(n)\log(n) + \sum_{d|n}\Lambda_k(d)\Lambda(\frac{n}{d})\right] \\ &= \sum_{n\leq x}\Lambda_k(n)\log(n) + \sum_{d\leq x}\Lambda_k(d)M_\Lambda(\frac{x}{d}) \\ &\sim_{+\infty} \sum_{n\leq x}\Lambda_k(n)\log(n) + x\sum_{d\leq x}\Lambda_k(d)\frac{1}{d}. \end{aligned}$$

Calculons le premier terme au moyen du lemme de sommation par parties :

$$\sum_{n\leq x}\Lambda_k(n)\log(n) = M_{\Lambda_k}(x)\log(x) - \int_1^x \frac{M_{\Lambda_k}(y)}{y}\,dy$$

Le terme $M_{\Lambda_k}(x)\log(x)$ est équivalent à $kx(\log x)^k$ lorsque $x \to +\infty$ par hypothèse de récurrence. Comme $M_{\Lambda_k}(y) \leq Cy(\log y)^{k-1}$ pour une constante C assez grande, le terme intégral est quant à lui borné par $C\int_1^x(\log y)^{k-1}\,dy \leq Cx\log(x)^{k-1}$, qui est négligeable devant $x(\log x)^k$ lorsque $x \to +\infty$. Donc

$$\sum_{n\leq x}\Lambda_k(n)\log(n) \sim_{+\infty} kx(\log x)^k.$$

Calculons maintenant $x\sum_{d\leq x}\Lambda_k(d)\frac{1}{d}$ au moyen du lemme de sommation par parties :

$$x\sum_{d\leq x}\Lambda_k(d)\frac{1}{d} = M_{\Lambda_k}(x) + x\int_1^x \frac{M_{\Lambda_k}(y)}{y^2}\,dy.$$

Le premier terme est équivalent à $kx(\log x)^{k-1}$, qui est négligeable devant $x(\log x)^k$ lorsque $x \to +\infty$. D'autre part, comme $\frac{1}{y^2}M_{\Lambda_k}(y)$ est équivalent à $\frac{k}{y}(\log y)^{k-1}$, le terme avec l'intégrale est équivalent à la primitive $(\log x)^k$ de $\frac{k}{x}(\log x)^{k-1}$ multipliée par x, soit $x(\log x)^k$. Donc

$$x\sum_{n\leq x}\Lambda_k(n)\frac{1}{n} \sim_{+\infty} x(\log x)^k.$$

Au total, $M_{\Lambda_{k+1}}(x) \sim_{+\infty} kx(\log x)^k + x(\log x)^k = (k+1)x(\log x)^k$, comme souhaité.

Exercice 4 Pour tout $a \in \mathbb{Z}$ et pour tout entier $n \geq 1$, on pose $\zeta_n = e^{\frac{2\pi i}{n}}$ et on définit $G(a;n) = \sum_{k=0}^{n-1}\zeta_n^{ak^2}$.

1. Que vaut le module de $G(1;p)$ lorsque p est un nombre premier impair ?
2. Soient $a, b \in \mathbb{Z}$. Démontrer que, pour tout nombre premier p impair, $\left(\frac{ab}{p}\right) = 1$ implique $G(a;p) = G(b;p)$.
3. Pour tout nombre p premier impair, calculer la somme $\sum_{a=0}^{p-1} G(a;p)$ et en déduire que $G(a;p) = \left(\frac{a}{p}\right) G(1;p)$ lorsque p ne divise pas a.
4. Si m et n sont des entiers ≥ 1 premiers entre eux, montrer que $G(a;mn) = G(an;m)G(am;n)$.
5. Déduire de tout ce qui précède le module de $G(a;n)$ pour tout $a \in \mathbb{Z}$ et tout $n \in \mathbb{N}^*$ impair et sans facteur carré, tels que a et n sont premiers entre eux.

Corrigé :

1. Par un résultat du cours, $G(1;p) = g_1(\chi)$ où $\chi = \left(\frac{\cdot}{p}\right)$. Par un autre résultat du cours, le module de $g_1(\chi)$ pour un caractère χ non trivial défini sur $\mathbb{F}_p^\times$ est $\sqrt{p}$.
2. Si $\left(\frac{ab}{p}\right) = 1$ alors $ab \equiv \alpha^2 \,[p]$ pour un certain $\alpha \in \mathbb{Z}$ premier avec p, et donc $b \equiv \beta^2 a \,[p]$ pour $\beta = \alpha \overline{a}_p^{-1}$. Comme ζ_p^k ne dépend que de k modulo p, on a
$$G(a;p) = \sum_{k \in \mathbb{F}_p} \zeta_p^{ak^2} = \sum_{k \in \mathbb{F}_p} \zeta_p^{a\beta^2 k^2}$$
puisque $k \mapsto \beta k$ est une permutation de $\mathbb{F}_p$. On en déduit que
$$G(a;p) = \sum_{k \in \mathbb{F}_p} \zeta_p^{a\beta^2 k^2} = \sum_{k \in \mathbb{F}_p} \zeta_p^{bk^2} = G(b;p).$$
3. La somme $\sum_{a=0}^{p-1} G(a;p)$ est donnée par
$$\sum_{a=0}^{p-1} G(a;p) = \sum_{k=0}^{p-1} \sum_{a=0}^{p-1} \zeta_p^{ak^2}$$
qui est une somme géométrique de raison $\zeta_p^{k^2}$, nulle sauf lorsque $k^2 \equiv 0 \,[p]$ ou encore $k = 0$. Lorsque $k = 0$, l'expression $\zeta_p^{ak^2} = 1$, et leur somme sur les p valeurs de a donne donc p, de sorte que $\sum_{a=0}^{p-1} G(a;p) = p$.
Si on note par c un élément de $\mathbb{F}_p$ tel que $\left(\frac{c}{p}\right) = -1$, on a
$$\sum_{a=0}^{p-1} G(a;p) = G(0;p) + \frac{p-1}{2} G(1;p) + \frac{p-1}{2} G(c;p).$$
Mais comme $G(0;p) = p$, on en déduit que $G(c;p) = -G(1;p)$. Ainsi, si $\left(\frac{a}{p}\right) = 1$ on obtient $G(a;p) = G(1;p) = \left(\frac{a}{p}\right) G(1;p)$, tandis que si $\left(\frac{a}{p}\right) = -1$ on obtient $G(a;p) = -G(1;p) = \left(\frac{a}{p}\right) G(1;p)$, comme souhaité.

4. Comme ζ_{mn}^k ne dépend que de k modulo mn, on peut exprimer $G(a;mn)$ comme une somme sur les classes de congruence modulo mn. Comme $m \wedge n = 1$, par le théorème des restes chinois, l'application $\psi : \mathbb{Z}/(mn)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ de réduction modulo m et n est un isomorphisme, et son inverse est de la forme $\psi^{-1}(\bar{b}_m, \bar{c}_n) = \overline{n\alpha + m\beta}_{mn}$, où $\alpha = yb$ et $\beta = xc$ pour certains entiers x et y, inversibles respectivement modulo n et m. Ainsi, sommer une expression sur $k \in \mathbb{Z}/(mn)\mathbb{Z}$ revient à sommer sur $(\alpha, \beta) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ la même expression, où k a été remplacé par $n\alpha + m\beta$. On obtient donc

$$\begin{aligned} G(a;mn) &= \sum_{\alpha \in \mathbb{Z}/m\mathbb{Z}} \sum_{\beta \in \mathbb{Z}/n\mathbb{Z}} \exp\left(2\pi a i \frac{(n\alpha + m\beta)^2}{mn}\right) \\ &= \sum_{\alpha \in \mathbb{Z}/m\mathbb{Z}} \sum_{\beta \in \mathbb{Z}/n\mathbb{Z}} \exp\left(2\pi a i \frac{n^2\alpha^2 + m^2\beta^2}{mn}\right) \\ &= \sum_{\alpha \in \mathbb{Z}/m\mathbb{Z}} \sum_{\beta \in \mathbb{Z}/n\mathbb{Z}} \zeta_m^{an\alpha^2} \zeta_n^{am\beta^2} \\ &= G(an;m)G(am;n). \end{aligned}$$

5. Si $n \in \mathbb{N}^*$ est sans facteur carré, il peut s'écrire sous la forme $n = p_1 \dots p_r$ où les p_i sont des nombres premiers distincts. Montrons par récurrence sur $r \geq 2$ que

$$G(a;n) = \prod_{i=1}^{r} G(a\frac{n}{p_i}; p_i).$$

Pour $r = 2$, c'est exactement la propriété montrée au point précédent avec $m = p_1$ et $n = p_2$. Si la propriété est vraie pour $\tilde{n} = p_1 \dots p_{r-1}$, montrons-la pour $n = \tilde{n}p_r$. Par la propriété du point précédent, on a

$$\begin{aligned} G(a;n) &= G(a\tilde{n}; p_r)G(ap_r; \tilde{n}) \\ &= G(a\frac{n}{p_r}; p_r) \prod_{i=1}^{r-1} G(ap_r\frac{\tilde{n}}{p_i}; p_i) \\ &= G(a\frac{n}{p_r}; p_r) \prod_{i=1}^{r-1} G(a\frac{n}{p_i}; p_i) \\ &= \prod_{i=1}^{r} G(a\frac{n}{p_i}; p_i), \end{aligned}$$

comme souhaité. Par le point 3, on a $G(a;p) = \chi(a)G(1;p)$ pour $\chi = \left(\frac{\cdot}{p}\right)$. Par le point 1, on a $|G(1;p)| = \sqrt{p}$. Comme $|\chi(a)| = 1$ lorsque $a \wedge p = 1$, on obtient $|G(a;p)| = \sqrt{p}$. En insérant ceci dans la propriété ci-dessus, on obtient

$$|G(a;n)| = \prod_{i=1}^{r} \sqrt{p_i} = \sqrt{n}.$$