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 ?

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 $\{-1, 0, +1\}$?

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

$$M_{\Lambda_k}(x) \sim_{+\infty} kx(\log x)^{k-1}.$$

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.