Exercices de khôlle pour la MPSI

Vingt-septième semaine

David A. Madore
`david.madore@ens.fr`
`http://www.eleves.ens.fr:8080/home/madore/index.html`

(Jusqu'à présent : Moyenne des notes : 14.68 ± 0.21. Écart type : 2.54.)

Encore un classique. Si p est un nombre premier et n un entier, on appelle valuation p-adique de n, et on note $v_p(n)$, le plus grand $r \in \mathbb{N}$ tel que p^r divise n. Montrer que

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

où $\lfloor x \rfloor$ désigne la partie entière de x.

Premiers et seconds. Montrer qu'un nombre premier p est congru à 1 modulo 4 ss'il existe y tel que $y^2 \equiv -1 \pmod p$. [Indication : Sur $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z})\setminus\{0\}$ considérer la relation d'équivalence donnée par $a \sim b$ ssi $a = b$, $a = -b$, $ab = 1$ ou $ab = -1$.]

Équations diophantiennes. Montrer que les équations suivantes n'ont pas de solutions entières non triviales (on précisera le sens du mot "trivial").

(i) $x^2 = 2y^2$

(ii) $x^2 + y^2 = 3z^2$ [Indication : Regarder modulo 4.]

(iii) $x^6 + y^6 = 3(u^6 + v^6)$ [Même technique, modulo 7.]

(iv) $y^2 = x^3 + 7$ [Indication : Montrer que x est impair en regardant l'équation modulo 8. Ajouter 1 aux deux membres puis factoriser. Montrer que $x^2 - 2x + 4$, et donc aussi $y^2 + 1$, est divisible par un nombre premier congru à 3 modulo 4, et appliquer l'exercice précédent.]

(v) $x^4 + y^4 = z^2$ [Indication : Commencer par résoudre complètement l'équation de Pythagore $x^2 + y^2 = z^2$, puis appliquer deux fois cette résolution. Procéder par descente infinie.]

Une formule célèbre. φ désignant la fonction indicatrice d'Euler (le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$), montrer que pour tout n on a

$$\sum_{d|n} \varphi(d)$$

(la somme étant prise sur tous les diviseurs de n).

Formule d'inversion de Moebius. On dira qu'une fonction $\lambda\colon \mathbb{N}^* \to \mathbb{C}$ est multiplicative ssi $\lambda(ab) = \lambda(a)\,\lambda(b)$ pour tous a, b premiers entre eux. On définit $\mu\colon \mathbb{N}^* \to \mathbb{C}$ par $\mu(a) = 0$ si a est divisible par un carré, et sinon, $\mu(a) = (-1)^k$ où k est le nombre de facteurs premiers (nécessairement distincts) de a. Montrer que μ est multiplicative, puis que pour tout $n > 1$ on a $\sum_{d|n} \mu(d) = 0$ où la somme est prise sur tous les diviseurs d de n. On suppose maintenant que f est multiplicative, et que g est définie par $g(n) = \sum_{d|n} f(d)$. Montrer qu'alors $f(n) = \sum_{d|n} \mu(d)\, g(d)$ (formule d'inversion de Moebius).

Un exercice astucieux et classique. Montrer que pour tout $n > 1$ entier la quantité

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

n'est pas un entier. [Indication : Multiplier par le produit de tous les nombres impairs $\leq n$ et par l'avant-dernière puissance de 2 avant n.]

Théorème de Wilson. Montrer que $p > 1$ est un nombre premier ssi $(p-1)! \equiv 1 \pmod p$.

Théorème de Waring-Wolstenholme. Soit $p > 3$ un nombre premier. Montrer que le numérateur réduit de

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

est multiple de p^2. [Indication : Regrouper les termes deux par deux, éliminer le facteur p évident, et montrer que le numérateur divisé par p est congru, modulo p, et éventuellement à un facteur inversible près, à la somme des carrés de $\mathbb{Z}/p\mathbb{Z}$. Or celle-ci est nulle.] Dans le même ordre d'idées, montrer que p divise le numérateur réduit de

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{(p-1)^2}$$

Travail de recherche. On note φ la fonction indicatrice d'Euler ($\varphi(n)$ est le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$). Un conjecture indémontrée à ce jour affirme que pour tout $n \in \mathbb{N}^*$ il existe $n' \in \mathbb{N}^* \setminus \{n\}$ tel que $\varphi(n') = \varphi(n)$. Montrer que cette conjecture est vraie au moins jusqu'à 42 401 268.

Marin Mersenne et Pierre de Fermat. Montrer que si $2^n - 1$ est premier alors n est premier (on dit que $2^n - 1$ est un premier de Mersenne). Montrer que si $2^n + 1$ est premier alors n est une puissance de 2 (on dit que $2^n + 1$ est un premier de Fermat).

Nombres parfaits. On dit qu'un nombre n est parfait ssi la somme de tous les diviseurs de n est égale à $2n$. Montrer que si $2^\ell - 1$ est premier (voir l'exercice précédent) alors $2^{\ell-1}(2^\ell - 1)$ est parfait. [Ce résultat était déjà connu d'Euclide.] Nettement plus difficile : montrer que tous les nombres parfaits pairs sont de cette forme. Pour cela, on écrira $n = 2^\ell m$ avec m impair et $\ell \geq 1$. On admettra que la fonction σ qui à n associe la somme des diviseurs de n est multiplicative (i.e. $\sigma(ab) = \sigma(a)\,\sigma(b)$ dès que a, b sont premiers entre eux).

Remarque : On ne sait pas à ce jour s'il existe des nombres parfaits impairs.

Test de primalité de Lucas-Lehmer. Soit $p \in \mathbb{N} \setminus \{0, 1\}$. On suppose que pour tout facteur premier q de $p-1$ il existe un entier a tel que $a^{p-1} \equiv 1 \pmod p$ et $a^{(p-1)/q} \not\equiv 1 \pmod p$. Montrer qu'alors p est premier. [Indication : Considérer l'ordre de a dans le groupe des inversibles de $\mathbb{Z}/p\mathbb{Z}$, puis l'ordre du groupe lui-même.]

Remarque : Cette condition suffisante de primalité est en fait nécessaire, comme le montre l'exercice suivant.

Éléments primitifs. Soit $K = \mathbb{Z}/p\mathbb{Z}$ avec p premier (ou en fait n'importe quel corps fini). Montrer que le groupe multiplicatif K^* des éléments non nuls de K est cyclique. Pour cela, on appellera $\psi(d)$ le nombre d'éléments de K^* d'ordre d. On remarquera (grâce à une considération élémentaire sur le polynôme $X^n - 1$) que $\sum_{d|n} \psi(d) \leq n$. On en conclura habilement que $\psi(d) = \varphi(d)$ pour tout d (voir le quatrième exercice de cette série). On en déduira alors le résultat.

Théorème de Lagrange. Le but de cet exercice est de montrer le résultat suivant : tout entier naturel peut s'écrire comme somme de quatre carrés d'entiers naturels. Pour cela, on commencera par vérifier l'identité suivante :

$$\begin{aligned}(x^2 + y^2 + z^2 + t^2)(x'^2 + y'^2 + z'^2 + t'^2) = &(xx' + yy' + zz' + tt')^2 + (xy' - yx' - zt' + tz')^2 \\ &+ (xz' + yt' - zx' - ty')^2 + (xt' - yz' + zy' - tx')^2\end{aligned}$$

On expliquera alors pourquoi il suffit de montrer le résultat pour les nombres premiers (impairs). Soit donc p un nombre premier impair. En considérant les résidus modulo p de $0^2, 1^2, \dots, (\frac{p-1}{2})^2$, et $-1-0^2, -1-1^2, \dots, -1-(\frac{p-1}{2})^2$, montrer qu'il existe x, y, z, t entiers tels que $x^2+y^2+z^2+t^2 = lp$ pour un certain entier $0 < l < p$. On considère le plus petit tel entier l. Montrer que l est impair (car si l marche alors $l/2$ marche aussi). On suppose par l'absurde $l > 1$. En appelant x', y', z', t' les résidus de x, y, z, t modulo l compris entre $-\frac{l-1}{2}$ et $\frac{l-1}{2}$, et en réappliquant l'identité, arriver à une contradiction.

Un résultat dû à Euler. Le but de cet exercice est de montrer que la somme des $\frac{1}{p}$, où p décrit l'ensemble des nombres premiers, diverge. Dans le cas contraire, notant p_i le i-ième nombre premier, il existe ℓ tel que

$$\sum_{i>\ell} \frac{1}{p_i} < \frac{1}{2}$$

On note $N_1(n)$ le nombre d'entiers entre 1 et n qui ne sont divisibles que par des p_i avec $i \leq \ell$ et $N_2(n)$ le nombre d'entiers entre 1 et n qui sont divisibles par un p_i avec $i > \ell$. On a ainsi $n = N_1(n) + N_2(n)$. Majorer séparément $N_1(n)$ et $N_2(n)$ de façon à obtenir une contradiction. [Les majorations à trouver sont $N_1(n) \leq 2^\ell \sqrt{n}$ et $N_2(n) \leq \frac{n}{2}$.]

Pafnuti Lvovitch Tchebytchev in memoriam. Pour x un nombre réel, on note $\pi(x)$ le nombre de nombres premiers p tels que $p \leq x$. On note de plus $\theta(x)$ la somme des logarithmes de ces nombres premiers. 1) Montrer que $\theta(x) \leq Cx$ pour une certaine constante C. Pour cela, on remarquera que

$$2^{2n} > C_{2n}^n > \prod_{p>n}^{p \leq 2n} p$$

ce qu'on traduira par une borne sur $\theta(2n) - \theta(n)$ qu'on traduira par une borne sur $\theta(x)$. 2) Montrer qu'il existe une constante C' telle que $\pi(x) \leq C'x/\ln x$. Pour cela, on remarquera que $\theta(x) \geq \sum_{p>\sqrt{x}}^{p\leq x} \ln p$. 3) Montrer que $\theta(x) \geq C''x$ pour une certaine constante C''. Pour cela, on remarquera que $C_{2n}^n \geq 2^n$. On rappelle que la valuation p-adique $v_p(n)$ d'un entier n est la plus grande puissance de p qui divise n. En utilisant la formule

$$v_p(n!) = \sum_{k=1}^{\lfloor \frac{\ln n}{\ln p} \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor$$

(où $\lfloor x \rfloor$ désigne la partie entière de x), montrer que $v_p(C_{2n}^n) \leq \lfloor \frac{\ln(2n)}{\ln p} \rfloor =: t_p$. Passant les égalités

$$2^n \leq C_{2n}^n \leq \prod_p p^{t_p}$$

au logarithme et divisant la somme sur p en deux termes selon que $p > \sqrt{2n}$ ou non, obtenir une minoration de la forme

$$\theta(2n) \geq n \ln 2 - \sqrt{2n} \ln(2n)$$

ce qui nous suffit. 4) Montrer qu'il existe une constante $C^{(3)}$ telle que $\pi(x) \geq C^{(3)}x/\ln x$.

> **Remarque :** On a donc montré que $\pi(x)$ est de l'ordre de $x/\ln x$ (dans le sens que le rapport de$\pi(x)$ à $\frac{x}{\ln x}$ est borné). Ce résultat est dû à Tchebytchev et date de 1852. En réalité, le rapport tend vers 1, c'est-à-dire $\pi(x) \sim \frac{x}{\ln x}$. Ce résultat difficile, connu sous le nom de "Théorème des Nombres Premiers", a été démontré en 1896 simultanément et indépendamment par Jacques Hadamard et Charles-Louis Xavier Joseph de la Vallée-Poussin.

Conséquence du théorème chinois. Montrer qu'il existe des segments d'entiers arbitrairement longs sans aucune puissance parfaite (une puissance parfaite est un entier de la forme n^k avec n entier et $k \geq 2$ entier).

Plaisanterie. Montrer que pour $n \geq 3$ l'équation $x^n + y^n = z^n$ n'a pas de solution entière avec x, y, z entiers non nuls. [Indication : On fera le lien avec la conjecture de Shimura-Taniyama-Weil.]