Examen partiel d'Arithmétique

Mercredi 22 février 2023. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

Exercice 1 Existe-t-il des nombres premiers $p > 10$ tels que l'entier $p^6 + 6$ est également un nombre premier ?

Corrigé : Comme $p > 10$ premier n'est pas divisible par 7, par le petit théorème de Fermat, $p^6 \equiv 1\,[7]$, de sorte que $p^6 + 6$ est divisible par 7. Comme $p^6 + 6 > 7$, ce n'est donc pas un nombre premier, quel que soit $p > 10$ premier.

Exercice 2 Soient a, b, $c \in \mathbb{N}^*$. On note (a, b) le plus grand commun diviseur de a et b, et on note $[a, b]$ le plus petit commun multiple de a et b.

1. Montrer que $([a, b], c) = [(a, c), (b, c)]$.
2. En déduire que $(a + b, [a, b]) = (a, b)$.
3. Si $a + b = 288$ et $[a, b] = 1716$, que valent a et b ?

Corrigé :

1. En notant $p_1, p_2, p_3, \ldots$ la suite des nombres premiers, écrivons la décomposition des entiers a, b et c en puissances de facteurs premiers : $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$, $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_N^{\beta_N}$ et $c = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_N^{\gamma_N}$, où p_N est le plus grand nombre premier divisant abc. La plus grande puissance de p_i divisant $([a, b], c)$ est $\min(\max(\alpha_i, \beta_i), \gamma_i)$. La plus grande puissance de p_i divisant $[(a, c), (b, c)]$ est $\max(\min(\alpha_i, \gamma_i), \min(\beta_i, \gamma_i))$. On vérifie la relation $\min(\max(\alpha_i, \beta_i), \gamma_i) = \max(\min(\alpha_i, \gamma_i), \min(\beta_i, \gamma_i))$ pour chacun des ordres possibles de $\alpha_i, \beta_i, \gamma_i$ une fois classés par ordre croissant, et on obtient ainsi l'identité désirée.
2. Prenons $c = a + b$ dans l'identité précédente. On obtient $([a, b], a + b) = [(a, a + b), (b, a + b)]$. Comme $(a, a + b) = (a, b)$ et $(b, a + b) = (b, a)$ par l'algorithme d'Euclide, et que $[(a, b), (a, b)] = (a, b)$, on obtient l'identité désirée.
3. Calculons le pgcd de 1716 et 288 par l'algorithme d'Euclide. Comme $1716 - 5 * 288 = 276$, on a $(1716, 288) = (288, 276)$. Puis comme $288 - 276 = 12$, on a $(288, 276) = (276, 12)$. Comme $12|276$, on obtient $(1716, 288) = 12$. On en déduit $ab = (a, b)[a, b] = 12 * 1716 = 20592$. Connaissant la somme et le produit de a et b, on obtient $a, b = \frac{1}{2}(288 \pm \sqrt{288^2 - 4 * 20592}) = \frac{1}{2}(288 \pm \sqrt{576}) = \frac{1}{2}(288 \pm 24)$ donc a et b sont 132 et 156.

Exercice 3 Trouver des entiers naturels $a_1, \dots, a_k$ et N tels que, pour tout nombre premier $p > 7$, l'entier 21 est un résidu quadratique modulo p si et seulement si $p \equiv a_i \,[N]$ pour un certain $i \in \{1, \dots, k\}$.

Corrigé : Par définition des symboles de Legendre, 21 est un résidu quadratique modulo p ssi $\left(\frac{21}{p}\right) = 1$. Or $\left(\frac{21}{p}\right) = \left(\frac{3}{p}\right) * \left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{7}\right)$ par la loi de réciprocité quadratique. De plus, $\left(\frac{p}{3}\right) = 1$ ssi $p \equiv 1\,[3]$. D'autre part, $\left(\frac{p}{7}\right) = 1$ ssi $p \equiv 1, 2$ ou $4\,[7]$. Les cas favorables vont correspondre à diverses valeurs pour p modulo 3 et 7, chaque cas correspondant à une congruence bien précise modulo 21, par le théorème des restes chinois. Si $p \equiv 1\,[3]$ et $p \equiv 1\,[7]$, cela correspond à $p \equiv 1\,[21]$. Si $p \equiv 1\,[3]$ et $p \equiv 2\,[7]$, cela correspond à $p \equiv 16\,[21]$. Si $p \equiv 1\,[3]$ et $p \equiv 4\,[7]$, cela correspond à $p \equiv 4\,[21]$.

Si $p \equiv 2\,[3]$ et $p \equiv 3\,[7]$, cela correspond à $p \equiv 17\,[21]$. Si $p \equiv 2\,[3]$ et $p \equiv 5\,[7]$, cela correspond à $p \equiv 5\,[21]$. Si $p \equiv 2\,[3]$ et $p \equiv 6\,[7]$, cela correspond à $p \equiv 20\,[21]$.

On obtient donc $N = 21$, $a_1 = 1$, $a_2 = 16$, $a_3 = 4$, $a_4 = 17$, $a_5 = 5$, $a_6 = 20$ et $k = 6$.

Exercice 4 Soit $x > 2$.

1. En utilisant le lemme de sommation par parties, montrer que

$$\sum_{n \leqslant x} \frac{\log n}{n} = \frac{1}{2} \log^2 x + A + O\left(\frac{\log x}{x}\right)$$

   pour une certaine constante A que l'on écrira explicitement sous la forme d'une intégrale (sans chercher à la calculer).

2. En déduire que

$$\sum_{n \leqslant x} \frac{d(n)}{n} = \frac{1}{2} \log^2 x + 2\gamma \log x + O(1)$$

   où $d(n) = \sum_{\substack{a,b \in \mathbb{N}^* \\ ab = n}} 1$ et γ est la constante d'Euler.

Corrigé :

1. En appliquant le lemme de sommation par parties avec $f(x) = \frac{\log x}{x}$ et $g(n) =$

1 entre les bornes $\frac{1}{2}$ et x, on obtient

$$\begin{aligned}\sum_{n\leqslant x}\frac{\log n}{n} &= \lfloor x\rfloor\frac{\log x}{x} - \int_1^x \lfloor y\rfloor\frac{1-\log y}{y^2}\,dy\\ &= \lfloor x\rfloor\frac{\log x}{x} + \int_1^x (y-\lfloor y\rfloor)\frac{1-\log y}{y^2}\,dy - \int_1^x \frac{1-\log y}{y}\,dy\\ &= \lfloor x\rfloor\frac{\log x}{x} + A - \int_x^\infty (y-\lfloor y\rfloor)\frac{1-\log y}{y^2}\,dy - \log x + \frac{1}{2}\log^2 x\\ &= \frac{1}{2}\log^2 x + A + (\lfloor x\rfloor - x)\frac{\log x}{x} - \int_x^\infty (y-\lfloor y\rfloor)\frac{1-\log y}{y^2}\,dy,\end{aligned}$$

où $A = \int_1^\infty (y-\lfloor y\rfloor)\frac{1-\log y}{y^2}\,dy$.
Comme $|x-\lfloor x\rfloor| \leqslant 1$, on a $(\lfloor x\rfloor - x)\frac{\log x}{x} = O(\frac{\log x}{x})$ et

$$\left|\int_x^\infty (y-\lfloor y\rfloor)\frac{1-\log y}{y^2}\,dy\right| \leqslant \int_x^\infty \frac{\log y - 1}{y^2}\,dy = \frac{\log x}{x} = O\left(\frac{\log x}{x}\right).$$

2. On calcule

$$\begin{aligned}\sum_{n\leqslant x}\frac{d(n)}{n} &= \sum_{n\leqslant x}\sum_{\substack{a,b\in\mathbb{N}^*\\ ab=n}}\frac{1}{n} = \sum_{a\leqslant x}\frac{1}{a}\sum_{b\leqslant \frac{x}{a}}\frac{1}{b}\\ &= \sum_{a\leqslant x}\frac{1}{a}\left(\log\left(\frac{x}{a}\right)+\gamma+O\left(\frac{a}{x}\right)\right)\\ &= (\log x+\gamma)\sum_{a\leqslant x}\frac{1}{a} - \sum_{a\leqslant x}\frac{\log a}{a} + O(1)\\ &= (\log x+\gamma)\left(\log x+\gamma+O\left(\frac{1}{x}\right)\right) - \frac{1}{2}\log^2 x + O(1)\\ &= \frac{1}{2}\log^2 x + 2\gamma\log x + O(1).\end{aligned}$$

Exercice 5 Soit $n > 2$ un entier et p un nombre premier tel que $p \equiv 1\,[n]$. Le but de cet exercice est d'estimer le nombre $N(X^n + Y^n = 1)$ de solutions $(x, y) \in \mathbb{F}_p^2$ pour l'équation $X^n + Y^n = 1$.

1. Montrer qu'il existe un caractère ψ de $\mathbb{F}_p^\times$ d'ordre n. En déduire que
$$N(X^n = a) = \sum_{i=0}^{n-1} \psi^i(a)$$
pour tout $a \in \mathbb{F}_p$.
2. Ecrire $N(X^n + Y^n = 1)$ en fonction des sommes de Jacobi $J(\psi^i, \psi^j)$ avec $0 \leqslant i, j \leqslant n-1$.
3. Montrer que
$$\sum_{\substack{i,j=1 \\ i+j=n}}^{n-1} J(\psi^i, \psi^j) = 1 - \frac{n}{2}\left((-1)^{\frac{p-1}{n}} + 1\right).$$
4. Déduire de ce qui précède que
$$\left|N(X^n + Y^n = 1) + \frac{n}{2}\left((-1)^{\frac{p-1}{n}} + 1\right) - (p+1)\right| < (n-1)(n-2)\sqrt{p}.$$
5. Sans utiliser les points précédents, lorsque $p \geqslant 3$, montrer que
$$N(X^2 + Y^2 = 1) = \begin{cases} p-1 & \text{si } \left(\frac{-1}{p}\right) = 1, \\ p+1 & \text{si } \left(\frac{-1}{p}\right) = -1. \end{cases}$$
Indication : Lorsque $x \neq 1$, poser $y = a(x-1)$ avec $a \in \mathbb{F}_p$.

Corrigé :

1. Le groupe $\widehat{\mathbb{F}_p^\times}$ est isomorphe au groupe $\mathbb{F}_p^\times$ qui est cyclique d'ordre $p-1$. Soit ϕ un générateur de $\widehat{\mathbb{F}_p^\times}$, il est donc d'ordre $p-1$. Alors $\psi = \phi^{\frac{p-1}{n}}$ est d'ordre n comme souhaité. De plus, si un élément quelconque ϕ^k de $\widehat{\mathbb{F}_p^\times}$ satisfait $\phi^{kn} = \varepsilon$, alors $kn \equiv 0\,[p-1]$ de sorte que k est un multiple de $\frac{p-1}{n}$ et ϕ^k est une puissance de ψ. Comme $\{\chi \in \widehat{\mathbb{F}_p^\times}, \chi^n = \varepsilon\} = \{\psi^0, \psi^1, \ldots, \psi^{n-1}\}$, la relation $N(X^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$ se réécrit en celle souhaitée.

2. On a

$$\begin{aligned} N(X^n + Y^n = 1) &= \sum_{\substack{a,b\in\mathbb{F}_p \\ a+b=1}} N(X^n = a)N(Y^n = b) \\ &= \sum_{\substack{a,b\in\mathbb{F}_p \\ a+b=1}} \sum_{i,j=0}^{n-1} \psi^i(a)\psi^j(b) \\ &= \sum_{i,j=0}^{n-1} J(\psi^i, \psi^j). \end{aligned}$$

3. Lorsque $i + j = n$ avec $1 \leqslant i \leqslant n-1$, $J(\psi^i, \psi^j) = J(\psi^i, \psi^{-i}) = -\psi^i(-1)$. Par conséquent,

$$\sum_{\substack{i,j=1 \\ i+j=n}}^{n-1} J(\psi^i, \psi^j) = -\sum_{i=1}^{n-1} \psi^i(-1) = 1 - N(X^n = -1).$$

D'autre part, -1 est une puissance $n$ième dans $\mathbb{F}_p^\times$ ssi $(-1)^{\frac{p-1}{n}} = 1$. En effet, si g est un générateur de $\mathbb{F}_p^\times$ et $\alpha \in \mathbb{Z}$ tel que $g^\alpha = -1$, alors $(-1)^{\frac{p-1}{n}} = g^{\alpha\frac{p-1}{n}} = 1$ ssi $n|\alpha$. De plus, si -1 est une puissance $n$ième dans $\mathbb{F}_p^\times$, alors il y a exactement n racines $n$ièmes g^β de -1, correspondant aux n solutions de $n\beta \equiv \alpha\,[p-1]$. Ainsi, $N(X^n = -1) = \frac{n}{2}\left((-1)^{\frac{p-1}{n}} + 1\right)$, ce qui donne la formule souhaitée.

4. Si $i = j = 0$, on a $J(\varepsilon, \varepsilon) = p$. Si $i = 0$ mais $j \neq 0$, on a $J(\varepsilon, \psi^j) = 0$ et de même si $i \neq 0$ mais $j = 0$, on a $J(\psi^i, \varepsilon) = 0$. Des $(n-1)^2$ termes restants, si on retire encore les $n-1$ termes $\sum_{\substack{i,j=1 \\ i+j=n}}^{n-1} J(\psi^i, \psi^j)$, il reste $(n-1)(n-2)$ termes $J(\psi^i, \psi^j)$ avec $i, j, i+j \not\equiv 0\,[n]$. Par conséquent, $|J(\psi^i, \psi^j)| = \sqrt{p}$ et on obtient

$$\left|N(X^n + Y^n = 1) + \frac{n}{2}\left((-1)^{\frac{p-1}{n}} + 1\right) - (p+1)\right| \leqslant (n-1)(n-2)\sqrt{p}.$$

Dans cette inégalité, l'égalité n'est pas possible car le membre de gauche est toujours un entier, mais jamais le membre de droite.

5. Si $x = 1$, alors $y = 0$, ce qui donne une première solution. Si $x \neq 1$, on pose $y = a(x-1)$ avec $a \in \mathbb{F}_p$. En remplaçant dans l'équation $x^2 + y^2 = 1$, on obtient $(x-1)\left((a^2+1)x + (a^2-1)\right) = 0$. Cette équation a une unique solution $x \neq 1$ ssi $a^2+1 \neq 0$. Lorsque $\left(\frac{-1}{p}\right) = -1$, toutes les valeurs de $a \in \mathbb{F}_p$ conviennent et on obtient p solutions supplémentaires, soit un total de $p+1$ solutions. Lorsque $\left(\frac{-1}{p}\right) = 1$, deux valeurs de $a \in \mathbb{F}_p$ satisfont $a^2 = -1$, donc on a deux solutions de moins, soit un total de $p-1$.

Exercice 6 (Bonus)

1. Soit $p > 2$ un nombre premier et $x, y \in \mathbb{Z}$ tels que $p \nmid x$, $p \nmid y$ mais $p \mid x - y$. Montrer que $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$ pour tout $n \in \mathbb{N}^*$.
2. Comment adapter ce résultat au cas où $p = 2$, lorsque $4 \mid x - y$?

Corrigé :

1. Si $p \nmid n$, alors comme $x^n - y^n = (x-y)\sum_{i=0}^{n-1} x^i y^{n-1-i}$ et que $\sum_{i=0}^{n-1} x^i y^{n-1-i} \equiv nx^{n-1}\,[p]$, on obtient $v_p(x^n - y^n) = v_p(x - y)$.
   Lorsque $n = p$, en remplaçant y par $x+kp$ dans $\sum_{i=0}^{p-1} x^i y^{p-1-i}\,[p^2]$, on obtient $px^{p-1} + \sum_{i=0}^{p-2} x^{p-2}kp(p-1-i) \equiv px^{p-1}\,[p^2]$ puisque $p \mid \sum_{i=0}^{p-2}(p-1-i) = \frac{1}{2}p(p-1)$, de sorte que $v_p(x^p - y^p) = v_p(x - y) + 1$.
   Si $v_p(n) = a > 0$, de sorte que $n = bp^a$ avec $p \nmid b$, alors par les propriétés ci-dessus $v_p(x^n - y^n) = v_p(x^{p^a} - y^{p^a}) = v_p(x^{p^{a-1}} - y^{p^{a-1}}) + 1 = \ldots = v_p(x-y) + a$ comme souhaité.
2. Lorsque $n = p = 2$, le raisonnement ci-dessus ne fonctionne plus car $\frac{1}{2}p(p-1)$ n'est plus un multiple de p. Mais pour tout $a \geqslant 1$ on a alors $v_2(x^{2^a} - y^{2^a}) = v_2(x^{2^{a-1}} - y^{2^{a-1}}) + v_2(x^{2^{a-1}} + y^{2^{a-1}})$. Comme x et y sont impairs, $x^{2^{a-1}} - y^{2^{a-1}}$ et $x^{2^{a-1}} + y^{2^{a-1}}$ sont pairs mais distincts modulo 4. Donc si $4 \mid x - y$, alors $4 \mid x^{2^{a-1}} - y^{2^{a-1}}$ et donc $4 \nmid x^{2^{a-1}} + y^{2^{a-1}}$ de sorte que $v_2(x^{2^{a-1}} + y^{2^{a-1}}) = 1$. On retrouve donc la même relation que dans le cas où p est impair.