Université Paris 7 Denis Diderot
L1 Arithmétique
2009-2010

Contrôle de connaissance
du mercredi 17 mars 2010
(corrigé)

Exercice 1 Soit p un nombre premier congru à 1 modulo 4.

1) Montrer qu'il existe un entier $a \in [1, p[$ tel que $a^2 + 1$ soit divisible par p.
2) On développe a/p en fraction continue

$$a/p = [b_0, b_1, \ldots, b_N],$$

où $b_0 = 0$ et $b_i \geqslant 1$ quel que soit $i \in \{1, \ldots, N\}$. Pour tout entier $j \in \{0, 1, \ldots, N\}$, on désigne par p_j/q_j la réduite d'indice j de a/p. Montrer qu'il existe un unique indice k tel que $q_k < \sqrt{p} < q_{k+1}$.
3) Montrer que $|aq_k - pp_k| < \sqrt{p}$.
4) Soient $r = q_k$ et $s = aq_k - pp_k$. Montrer que $r^2 + s^2$ est divisible par p.
5) Montrer que $0 < r^2 + s^2 < 2p$.
6) En déduire que p s'écrit comme la somme de deux carrés.
7) Déterminer le nombre de classes de -4 (justifier votre réponse).
8) Donner une autre démonstration de la question 7) en utilisant les formes quadratiques.

Réponse : 1) Comme $p \equiv 1 \pmod 4$, -1 est un carré modulo p compte tenue de la loi de réciprocité quadratique. Soit ξ une classe de résidu modulo p tel que ξ^2 s'identifie à la classe de -1. On a nécessairement $\xi \neq 0$. Donc il existe un représentant de la classe ξ dans $\{1, \ldots, p-1\}$. On en déduit donc l'existence d'un $a \in \{1, \ldots, p-1\}$ tel que $a^2 \equiv -1 \pmod p$.

2) Comme $p_N/q_N = a/p$, on a $q_N = p > \sqrt{p}$. En outre, la suite d'entiers $(q_n)_{0 \leqslant n \leqslant N}$ est strictement croissante et strictement positive. Comme $\sqrt{p}$ n'est pas un entier, il existe alors un unique indice k tel que $q_k < \sqrt{p} < q_{k+1}$.

3) La suite $(p_n/q_n - a/p)_{0 \leqslant n \leqslant N-1}$ étant alternée, on a

$$\left|\frac{p_k}{q_k} - \frac{a}{p}\right| \leqslant \left|\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}}\right| = \frac{1}{q_k q_{k+1}}.$$

D'où $|aq_k - pp_k| \leqslant p/q_{k+1} < \sqrt{p}$.

4) On a

$$r^2 + s^2 = q_k^2 + a^2 q_k^2 + p^2 p_k^2 - 2aq_k pp_k \equiv q_k^2(a^2 + 1) \equiv 0 \pmod p.$$

5) Comme $q_k \neq 0$, on a $0 < r^2 + s^2$. En outre, d'après 3), on a

$$r^2 + s^2 = q_k^2 + (aq_k - pp_k)^2 < p + p = 2p.$$

6) D'après 4) et 5), on a $p = r^2 + s^2$.

7) Soit $ax^2 + bxy + cy^2$ une forme quadratique réduite de discriminant -4. On a $b^2 - 4ac = 4$ et $|b| \leqslant a \leqslant c$. La première relation montre que b est divisible par 2. Mais si $|b| \geqslant 2$, alors

$$b^2 - 4ac \leqslant b^2 - 4b^2 = -3b^2 < -4.$$

On en déduit que $b = 0$, et donc $a = c = 1$. Le nombre de classes de -4 est donc 1.

8) D'après un résultat du cours, comme le nombre de classes de -4 est 1, p est représentable par la forme $x^2 + y^2$ (de discriminant -4) si et seulement si -4 est un carré modulo p, ou de façon équivalente, -1 est un carré modulo p. C'est le cas ici (p est congru à 1 modulo 4).

Exercice 2 Pour tout entier $n \geqslant 1$, on désigne par d_n le ppcm de $1, 2, \ldots, n$. Pour tout nombre $x > 0$, on désigne par $\pi(x)$ le nombre des premiers $\leqslant x$. On admet le théorème des nombres premiers comme la suite :

$$\pi(x) \sim \frac{x}{\log x} \quad (x \to +\infty).$$

1) Montrer que $d_n < n^{\pi(n)}$. En déduire que $d_n < 3^n$ pour n suffisamment grand.

2) Soient r et s deux entiers strictement positifs, $r > s$. Montrer que le nombre

$$d_r^2 \int_0^1 \int_0^1 \frac{x^r y^s}{1 - xy} \, \mathrm{d}x\mathrm{d}y$$

est un entier.

3) Montrer que, pour tout entier $r \geqslant 0$, on a

$$\int_0^1 \int_0^1 \frac{(xy)^r}{1 - xy} \, \mathrm{d}x\mathrm{d}y = \zeta(2) - \sum_{1 \leqslant k \leqslant r} \frac{1}{k^2},$$

où

$$\zeta(2) := \sum_{k \geqslant 1} \frac{1}{k^2}.$$

4) Pour tout entier $n > 0$, soit

$$P_n(X) := \frac{1}{n!} \Big(\frac{\mathrm{d}}{\mathrm{d}X} \Big)^n (X^n (1 - X)^n).$$

Montrer que $P_n \in \mathbb{Z}[X]$.

5) Pour tout entier $n > 0$, soit

$$I_n := \int_0^1 \int_0^1 \frac{(1 - y)^n P_n(x)}{1 - xy} \, \mathrm{d}x\mathrm{d}y.$$

Montrer qu'il existe des entiers A_n et B_n tels que $d_n^2 I_n = A_n + B_n \zeta(2)$.

6) Montrer que

$$I_n = (-1)^n \int_0^1 \int_0^1 \frac{y^n (1 - y)^n x^n (1 - x)^n}{(1 - xy)^{n+1}} \, \mathrm{d}x\mathrm{d}y.$$

7) Montrer que

$$\forall\,(x,y)\in[0,1]^2,\quad \frac{y(1-y)x(1-x)}{1-xy}\leqslant\Big(\frac{\sqrt{5}-1}{2}\Big)^5.$$

8) En déduire que

$$0<|A_n+B_n\zeta(2)|<\Big(\frac{5}{6}\Big)^n$$

pour n suffisamment grand.

9) Le nombre $\zeta(2)$ est-il rationnel ? Pourquoi ?

Réponse : 1) Soit $p\leqslant n$ un nombre premier. On a

$$v_p(d_n)=\sup_{1\leqslant k\leqslant n}v_p(k)=\left\lfloor\frac{\log n}{\log p}\right\rfloor.$$

Donc

$$\log(d_n)=\sum_{p\leqslant n}v_p(d_n)\log p\leqslant\sum_{p\leqslant n}\frac{\log n}{\log p}\log p=\pi(n)\log n.$$

L'inégalité est stricte dès que $n\geqslant 3$ car il existe alors un premier $p<n$ tel que $\log n/\log p\notin\mathbb{N}$ (i.e., n n'est pas une puissance de p). Pour n suffisamment grand, on a $\pi(n)\leqslant(\log 3)n/\log n$, d'où $\log(d_n)<(\log 3)n$ et $d_n<3^n$.

2) Pour tout $(x,y)\in[0,1[^2$, on a

$$\frac{1}{1-xy}=\sum_{n\geqslant 0}(xy)^n,$$

d'où

$$\begin{aligned}&\int_0^1\int_0^1\frac{x^ry^s}{1-xy}\,\mathrm{d}x\mathrm{d}y\\&=\sum_{n\geqslant 0}\int_0^1\int_0^1x^{r+n}y^{s+n}dxdy=\sum_{n\geqslant 0}\frac{1}{(r+n+1)(s+n+1)}\\&=\sum_{n\geqslant 0}\frac{1}{r-s}\Big(\frac{1}{s+n+1}-\frac{1}{r+n+1}\Big)=\frac{1}{r-s}\sum_{j=s+1}^{r}\frac{1}{j}.\end{aligned}$$

Comme $r-s$ divise d_r et $\mathrm{ppcm}(s+1,\dots,r)$ divise d_r aussi, on obtient le résultat.

3) On a

$$\begin{aligned}&\int_0^1\int_0^1\frac{(xy)^r}{1-xy}\,\mathrm{d}x\mathrm{d}y\\&=\sum_{n\geqslant 0}\int_0^1\int_0^1(xy)^{r+n}dxdy=\sum_{n\geqslant 0}\frac{1}{(r+n+1)^2}\\&=\zeta(2)-\sum_{k=1}^{r}\frac{1}{k^2}.\end{aligned}$$

4) On a

$$\begin{aligned}
P_n(X) &= \sum_{k=0}^{n} \frac{1}{n!}\binom{n}{k}\Big(\frac{\mathrm{d}}{\mathrm{d}X}\Big)^k (X^n)\Big(\frac{\mathrm{d}}{\mathrm{d}X}\Big)^{n-k}((1-X)^n) \\
&= \sum_{k=0}^{n} \frac{1}{k!}\Big(\frac{\mathrm{d}}{\mathrm{d}X}\Big)^k (X^n)\frac{1}{(n-k)!}\Big(\frac{\mathrm{d}}{\mathrm{d}X}\Big)^{n-k}((1-X)^n) \\
&= \sum_{k=0}^{n} \binom{n}{k}^2 (-1)^{n-k} X^{n-k}(1-X)^k \in \mathbb{Z}[X].
\end{aligned}$$

5) Comme P_n est proportionnel à la dérivée d'ordre n d'un polynôme de degré $2n$. Le polynôme P_n est de degré n. D'après 4), I_n est une combinaison linéaire à coefficients dans $\mathbb{Z}$ des intégrales de la forme

$$\int_0^1 \int_0^1 \frac{x^r y^s}{1-xy}\,\mathrm{d}x\mathrm{d}y$$

avec $0 \leqslant r, s \leqslant n$. D'après 2) et 3), on obtient le résultat (où on utilise aussi la symétrie entre x et y).

6) est une conséquence immédiate de l'intégration par partie.

7) La fonction $f(x,y) := y(1-y)x(1-x)/(1-xy)$ est bien défini et continue sur $[0,1]^2 \setminus \{(1,1)\}$ et s'étend en une fonction continue sur $[0,1]^2$. Elle est positive et prend valeur 0 sur $\partial[0,1]^2$, donc elle atteint son maximum à l'intérieur de $[0,1]^2$. Si (x_0,y_0) est un point maximum de f, alors on a $D_{(x_0,y_0)}f = 0$. Autrement dit, (x_0,y_0) satisfait au système d'équations

$$\begin{cases}(1-2x_0)(1-x_0y_0) + x_0y_0(1-x_0) = 0, \\ (1-2y_0)(1-x_0y_0) + x_0y_0(1-y_0) = 0.\end{cases}$$

La différence de ces deux équations donne $(x_0-y_0)(2-x_0y_0) = 0$, d'où $x_0 = y_0$. Un calcul direct donne alors $x_0 = y_0 = (\sqrt{5}-1)/2$. D'où le résultat.

8) D'après 1) et 7), on a

$$0 < d_n^2|I_n| = |A_n + B_n\zeta(2)| < \Big(\frac{\sqrt{5}-1}{2}\Big)^{5n} 3^{2n}\zeta(2)$$

pour n suffisamment grand. Comme

$$9 \times \Big(\frac{\sqrt{5}-1}{2}\Big)^5 < \frac{5}{6},$$

on obtient le résultat.

9) Le nombre $\zeta(2)$ est irrationnel car sinon

$$\inf_{\substack{(a,b)\in\mathbb{Z}^2 \\ a\zeta(2)+b\neq 0}} |a\zeta(2)+b|$$

est strictement positif. Cela contradit 8).