UPS – Centre d'Orsay | **Arithmétique – Maîtrise**
Mathématiques | Année 2003–2004

FEUILLE D'EXERCICES n° 1

Exercice 1 – Pour quelles valeurs de $n \in \mathrm{N}$ la fraction $\dfrac{2n^7+1}{3n^3+2}$ est-elle réductible ? [1163 *est premier*]

Exercice 2 – Quelle est la périodicité de la fonction $\varphi : \mathrm{N} \to \mathbb{Z}/7\mathbb{Z}$ définie par $\varphi(n) = 3^n + n$? Trouver toutes les solutions de l'équation $\varphi(n) = 0$ [*utiliser le Lemme Chinois*]

★ **Exercice 3** – Montrer que pour tout entier $n > 1$, on a $n \nmid 2^n - 1$.

Exercice 4 – [*Test de Fermat et Critère de Korselt 1899*] Montrer que $a^N \equiv a \pmod{N}$ pour tout entier a si et seulement si N est sans facteur carré et $p-1$ divise $N-1$ pour tout p facteur premier de N. [*Un tel N est appelé* nombre de Carmichael *s'il n'est pas premier. On sait qu'il en existe une infinité (Alford, Granville, Pomerance, 1994).*] Montrer qu'un nombre de Carmichael a au moins 3 facteurs premiers.

Exercice 5 – [*Test de Miller-Rabin, 1977*] Soit N un entier impair dont on se demande s'il est premier. On pose

$$e := v_2(N-1), \quad q := (N-1)/2^e.$$

Soit a un entier dans $]1, N[$. On dit que N est *pseudo-premier* (de Miller-Rabin) pour la base a si

$$a^q \equiv 1 \pmod{N}$$

ou s'il existe $0 \leqslant i < e$ tel que

$$a^{q2^i} \equiv -1 \pmod{N}.$$

a) Montrer que si N n'est pas pseudo-premier pour une base a, alors il est composé. Dans ce cas a est appelé *témoin* (de non-primalité).

★★ **b)** Montrer que si N est composé alors il est pseudo-premier pour au plus 1/4 des bases a. [*Soit* $N = \prod p^{f_p}$ *ayant* ω *facteurs premiers, travailler dans* $(\mathbb{Z}/N\mathbb{Z})^* \sim \oplus(\mathbb{Z}/(p-1)p^{f_p-1}, +)$ *et montrer que le nombre de bases pour lesquelles* N *est pseudo-premier est*

$$\left(1 + \frac{2^{\omega \min_p v_2(p-1)} - 1}{2^\omega - 1}\right) \prod_{p|N} (q, p-1).$$

Discuter suivant que $\omega = 1$, $\omega > 2$, *ou* $\omega = 2$. *Pour ce dernier cas, on peut conclure sauf si* $p-1 \mid N-1$ *pour chaque* $p \mid N$ *et* N *est sans facteur carré. Finir en utilisant l'exercice précédent.*]

Exercice 6 – Montrer que pour $m \neq n$ des entiers, les nombres $F_m = 2^{2^m} + 1$ et $F_n = 2^{2^n} + 1$ sont premiers entre eux [F_n *est appelé le* n*-ième nombre de Fermat*]. En déduire que l'ensemble des nombres premiers est infini. Quelle minoration de $\pi(N) := \mathrm{card}\{\, p \leqslant N \ :\ p \text{ premier}\}$ fournit cette méthode ?
Montrer que si $n > 1$, l'écriture décimale de F_n se termine par 7.

Exercice 7 – Pour tout entier positif k, montrer qu'il existe $n \in \mathrm{N}$ tel que l'ensemble $n, n+1, \ldots, n+k-1$ ne contienne aucun nombre premier. Que dire de $\limsup\limits_{n\to+\infty} (p_{n+1} - p_n)$ où p_n désigne le n-ième nombre premier ?

Exercice 8 – [*Théorème de Wilson 1770*] Montrer que $p \geqslant 2$ est premier si et seulement si

$$(p-1)! \equiv -1 \pmod{p}.$$

Ce test est-il praticable ?

Exercice 9 – [*Théorème de Wolstenholme 1862*] Soit $p > 3$ un nombre premier. Montrer l'égalité

$$\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \pmod{p^2}$$

[*évaluer* $\prod_{i=1}^{p-1}(X-i)$ *en* p *ou exprimer* $(p-i)^{-1}$ *en fonction de* i^{-1} *(modulo* p^2*)*]

★ **Exercice 10** – Soit $P \in \mathbb{Z}[X]$ un polynôme non constant, montrer qu'il existe une infinité de nombres premiers p tels que l'équation $P(x) \equiv 0 \pmod{p}$ ait au moins une solution. [*Généraliser la preuve d'Euclide sur l'existence d'une infinité de nombres premiers.*]

Exercice 11 – Soient d un entier, $d > 0$, et $c \in \mathbb{F}_p$. Etudier l'existence et le nombre de solutions dans $\mathbb{F}_p$ de l'équation $x^d = c$.

Exercice 12 – Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. Pour tout entier n on note $\rho(n)$ le nombre de solutions dans $\mathbb{Z}/n\mathbb{Z}$ de l'équation $P(x) = 0$.

a) Montrer que si $(m, n) = 1$ on a $\rho(mn) = \rho(m)\rho(n)$.

b) Soit p un nombre premier, on suppose qu'il existe $x_1 \in \mathbb{F}_p$ tel que $P(x_1) \equiv 0 \pmod{p}$ et $P'(x_1) \not\equiv 0 \pmod{p}$. Montrer que, pour tout $k \geqslant 1$, il existe un unique $x_k \in \mathbb{Z}/p^k\mathbb{Z}$ tel que $P(x_k) \equiv 0 \pmod{p^k}$ et $x_k \equiv x_l \pmod{p^l}$ pour tout $l \leqslant k$.

c) Si les racines de P dans $\mathbb{F}_p$ sont simples pour tout $p \mid n$, montrer que

$$\rho(n) \leqslant (\deg P)^{\omega(n)}$$

où $\omega(n)$ est le nombre de facteurs premiers de n.

Exercice 13 – [*Théorème de Chevalley-Warning, 1936*] Soit un polynôme P de $\mathbb{F}_p[x_1,\dots,x_n]$ de degré d. On note N le nombre de solutions de l'équation $P(x_1,\dots,x_n)=0$ dans $\mathbb{F}_p^n$. Le but de l'exercice est de montrer que si $d<n$ on a la congruence $N\equiv 0 \pmod p$.

a) Calculer pour tout $h\in \mathrm{N}$ la somme $S_p(h)=\sum_{x\in\mathbb{F}_p} x^h$ où l'on a posé $x^0=1$.

b) Montrer que

$$N\equiv \sum_{\mathbf{x}\in\mathbb{F}_p^n}(1-P(x_1,\dots,x_n)^{p-1}) \pmod p.$$

c) Montrer enfin que, lorsque $j_1,\dots,j_n\in \mathrm{N}$ sont des entiers qui vérifient

$$j_1+\cdots+j_n<n(p-1),$$

on a

$$\sum_{\mathbf{x}\in\mathbb{F}_p^n} x_1^{j_1}\dots x_n^{j_n}=0,$$

puis conclure.

d) Soit P homogène de degré $0<d<n$. Montrer que P admet une solution dans $\mathbb{F}_p^n$ différente de $(0,\dots,0)$.

e) On considère maintenant que $P=x_1^d+\cdots+x_n^d$ avec $d<n$. Montrer que, lorsque $p\nmid d$, l'équation $P(\mathbf{x})\equiv 0 \pmod{p^k}$ admet une solution non triviale dans $(\mathbb{Z}/p^k\mathbb{Z})^n$ pour tout entier k.

Exercice 14 – Soient $P\in\mathbb{Z}[X]$ un polynôme non constant, n un entier non nul et ψ un caractère du groupe additif $\mathbb{Z}/n\mathbb{Z}$. On considère la somme d'exponentielles

$$S_P(\psi;n):=\sum_{x\in\mathbb{Z}/n\mathbb{Z}}\psi(P(x)).$$

a) Montrer que pour $(m,n)=1$ on a la relation

$$S_P(\psi;mn)=S_P(\psi_1;m)S_P(\psi_2;n)$$

où ψ_1 et ψ_2 sont des caractères modulo m et n que l'on précisera en fonction de ψ.

b) On suppose que $n=p>2$, que ψ est non trivial, et que P est de degré 2. Montrer que $|S_P(\psi,n)|=n^{1/2}$

c) On considère maintenant le cas $n=p^\gamma$ avec $\gamma=2\alpha$ ou $2\alpha+1$ et $\alpha>0$. On suppose de plus que ψ est d'ordre n (Que se passe-t-il dans le cas contraire ?). Majorer $|S_P(\psi,n)|$ en fonction de $n^{1/2}$, du nombre de racines de P' dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ et du nombre de racines de P'' dans $\mathbb{Z}/p\mathbb{Z}$. [*on pourra faire la décomposition suivante de la variable x, suivant les cas : $x=x'+p^\alpha y$ ou $x=x'+p^\alpha(y+pz)$.*]

Exercice supplémentaire : soit F un corps ; F^* est un groupe abélien, en particulier un $\mathbb{Z}$-module. On pose

$$K_2F = F^* \otimes_{\mathbb{Z}} F^* \Big/ \{x \otimes (1-x), x \neq 0, 1\}\,.$$

C'est aussi un $\mathbb{Z}$-module, en particulier un groupe abélien (noté additivement, de neutre 0). On note $\{x, y\}$ la projection canonique de $x \otimes y$ dans K_2F.

a) Montrer que $\{x, -x\} = 0$ pour tout $x \neq 0$. [*considérer* $\left\{\frac{1}{x}, 1 - \frac{1}{x}\right\}$]

b) En déduire que $2\{x, x\} = 0$.

★ **c)** Montrer que si F est fini[1], alors $K_2F = \{0\}$ [F^* *est cyclique ; distinguer suivant que* -1 *est ou non un carré dans* F]

[1]On montre que $K_2\mathbb{Q}$ n'est pas de type fini [il est isomorphe a $(\mathbb{Z}/4\mathbb{Z})^* \oplus \bigoplus_{p>2}(\mathbb{Z}/p\mathbb{Z})^*$]. Si F n'est pas dénombrable, K_2F non plus.