Agrégation ENS Lyon
2008/2009

Anneaux, corps, polynômes et fractions rationnelles (4)

Exercice 1. Déterminer le PGCD et une relation de Bézout pour les entiers suivants : $(21, 34)$; $(220, 284)$; $(314, 159)$; $(10; 142857)$; $(10, 12, 15)$; $(2^n - 1, 2^n + 1)$ avec $n \geq 1$.

Exercice 2. Résoudre la congruence $6x \equiv 3 \pmod{15}$.

Exercice 3. Résoudre les problèmes suivants du *Liber Abaci* de Fibonacci (1202).

a) *"Il y a un nombre qui, divisé par 2, ou 3, ou 4, ou 5, ou 6, a toujours un reste de 1, et il est divisible par 7. Quel est ce nombre ?"*

b) "Il y a aussi un nombre qui, divisé par 2, a un reste de 1 ; divisé par 3, a un reste de 2 ; divisé par 4, a un reste de 3, et ainsi de suite jusqu'à 10 ; quand le nombre est divisé par 10, il a un reste de 9 ; le nombre est divisible par 11. Quel est-il ?"

Exercice 4. Résoudre le système de congruences

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 4 \pmod{9} \\ x \equiv 3 \pmod{5}. \end{cases}$$

Exercice 5. Soit $a, b, m \in \mathbf{Z}$. Montrer que la congruence $ax \equiv b \pmod{m}$ a une solution dans $\mathbf{Z}$ si et seulement si $\mathrm{PGCD}(a, m)$ divise b.

Exercice 6.

a) Soit $(x_0, y_0) \in \mathbf{Z}^2$ une solution de $ax + by = c$. Montrer que la solution générale de l'équation est donnée par $x = x_0 + tb/d$ et $y = y_0 - ta/d$ avec $d = \mathrm{PGCD}(a, b)$ et $t \in \mathbf{Z}$.

b) Déterminer de même la solution générale de la congruence $ax \equiv b \pmod{m}$ lorsque $\mathrm{PGCD}(a, m)$ divise b.

Exercice 7. Soit $a, b \geq 1$. Posons $d = \mathrm{PGCD}(a, b)$ et $m = \mathrm{PPCM}(a, b)$. Montrer les identités $\phi(a)\phi(b) = \phi(d)\phi(m)$ et $\phi(ab)\phi(d) = d\phi(a)\phi(b)$, où ϕ est l'indicatrice d'Euler.

Exercice 8. Soit n un entier ≥ 1. Montrer que n possède un nombre impair de diviseurs positifs si et seulement si n est un carré parfait.

Exercice 9.

a) Soit m un entier impair. Montrer que les groupes $(\mathbf{Z}/m\mathbf{Z})^*$ et $(\mathbf{Z}/2m\mathbf{Z})^*$ sont isomorphes.

b) Trouver deux entiers impairs distincts m et n tels que $(\mathbf{Z}/m\mathbf{Z})^*$ et $(\mathbf{Z}/n\mathbf{Z})^*$ soient isomorphes.

Exercice 10. Montrer que les nombres de Fermat $F_n = 2^{2^n} + 1$ $(n \geq 0)$ sont deux à deux premiers entre eux. En déduire qu'il existe une infinité de nombres premiers.

Exercice 11.

a) Montrer que $1 + \frac{1}{2} + \cdots + \frac{1}{n} \notin \mathbf{Z}$ dès que $n \geq 2$.

b) Montrer que tout p premier ≥ 3 divise le numérateur de $1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$.

c) Si p est premier ≥ 5, alors p^2 divise le numérateur de $1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$.

Exercice 12.

a) Pour tout n impair, montrer $n^2 \equiv 1 \pmod 8$.

b) Pour tout n non divisible par 3, montrer $n^2 \equiv 1 \pmod 3$.

c) Pour tout $n \in \mathbf{Z}$, montrer $n^5 \equiv n \pmod{30}$ et $n^7 \equiv n \pmod{42}$.

Exercice 13. Résoudre la congruence $x^2 \equiv 1 \pmod{10^n}$ pour $n = 1, 2, 3$.

Exercice 14.

a) Déterminer un générateur de $(\mathbf{Z}/17\mathbf{Z})^*$.

b) En déduire les solutions de $x^4 \equiv 1 \pmod{17}$.

c) Résoudre de même $x^3 \equiv 1 \pmod{19}$.

Exercice 15. Montrer que $3x^2 + 2 = y^2$ n'a pas de solution dans $\mathbf{Z}^2$, puis dans $\mathbf{Q}^2$.

Exercice 16. Montrer que $7x^3 + 2 = y^3$ n'a pas de solution dans $\mathbf{Z}^2$, puis dans $\mathbf{Q}^2$.

Exercice 17. Le but de cet exercice est d'établir que l'équation $y^2 = x^3 + 7$ n'a pas de solution $x, y \in \mathbf{Z}$.

(a) Montrer que x est nécessairement impair.

(b) Montrer qu'il existe p premier $\equiv 3 \pmod 4$ divisant $x^2 - 2x + 4$.

(c) Conclure en remarquant que $x^3 + 8 = (x + 2)(x^2 - 2x + 4)$.

Exercice 18. **(Lemme de Hensel)** Soit p un nombre premier et $P \in \mathbf{Z}[X]$. On suppose qu'il existe $x_1 \in \mathbf{Z}$ tel que $P(x_1) \equiv 0 \pmod p$ et $P'(x_1) \not\equiv 0 \pmod p$.

(a) Montrer qu'il existe une suite d'entiers $(x_n)_{n\geq 2}$ telle que $P(x_n) \equiv 0 \pmod{p^n}$ et $x_{n+1} \equiv x_n \pmod{p^n}$ pour tout $n \geq 1$.

(b) Montrer que si deux suites (x_n) et (y_n) vérifient les conditions ci-dessus alors $x_n \equiv y_n \pmod{p^n}$ pour tout n.

(c) *Application.* On suppose p impair. Soit $a \in \mathbf{Z}$ tel que la classe de a dans $\mathbf{Z}/p\mathbf{Z}$ est un carré non nul. Pour tout $n \geq 1$, montrer que la congruence $x^2 \equiv a \pmod{p^n}$ possède exactement deux solutions dans $\mathbf{Z}/p^n\mathbf{Z}$.

Exercice 19.

a) Montrer que 2 est associé à un carré dans $\mathbf{Z}[i]$.

b) Montrer que 3 est associé à un carré dans $\mathbf{Z}[j]$ avec $j = e^{2i\pi/3}$.

c) En utilisant la fonction $|\cdot|^2$, montrer que $\mathbf{Z}[i]^* = \{\pm 1, \pm i\}$ et $\mathbf{Z}[j]^* = \{\pm 1, \pm j, \pm j^2\}$.

Exercice 20. Soient $x, y, z \in \mathbf{Z}[j]$ tels que $x^3 + y^3 = z^3$. Montrer que $1 - j$ divise xyz.

Exercice 21. Soit p premier. Montrer que si l'ordre de a dans $(\mathbf{Z}/p\mathbf{Z})^*$ est 3, alors l'ordre de $a + 1$ est 6.

Exercice 22.

a) Montrer que si p premier divise $x^2 + 1$ avec $x \in \mathbf{Z}$, alors $p = 2$ ou $p \equiv 1 \pmod 4$ (utiliser le petit théorème de Fermat). En déduire l'existence d'une infinité de nombres premiers congrus à 1 modulo 4.

b) Montrer que si p premier divise $x^4 - x^2 + 1$ avec $x \in \mathbf{Z}$, alors $p \equiv 1 \pmod{12}$.

c) Soit $m \geq 2$ un entier et p un nombre premier ne divisant pas m. Montrer que la réduction du polynôme $X^m - 1$ n'a que des racines simples dans $\mathbf{Z}/p\mathbf{Z}$.

d) Supposons de plus que p divise $\Phi_m(a)$ avec $a \in \mathbf{Z}$, où $\Phi_m \in \mathbf{Z}[X]$ est le m-ième polynôme cyclotomique. Montrer que l'ordre de a dans $(\mathbf{Z}/p\mathbf{Z})^*$ vaut m, et en déduire que $p \equiv 1 \pmod{m}$.

e) Utiliser la question précédente pour montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo m. Cette preuve est attribuée à Euler par Dickson (*History of the Theory of Numbers, Vol. I : Divisibility and Primality*, 1919).

Exercice 23. Déterminer le polynôme minimal sur $\mathbf{Q}$ de $2\cos(2\pi/5)$ et $2\cos(2\pi/7)$ (on pourra penser aux polynômes cyclotomiques). Dans chacun des cas, déterminer les racines dans $\mathbf{C}$ et le corps de décomposition associé.

Exercice 24. Montrer que le corps de décomposition de $X^3 - 2 \in \mathbf{Q}[X]$ dans $\mathbf{C}$ est une extension de degré 6 de $\mathbf{Q}$.

Exercice 25. Construire les corps finis suivants :

(a) $\mathbf{F}_4$, $\mathbf{F}_8$ et $\mathbf{F}_{16}$;

(b) $\mathbf{F}_9$, $\mathbf{F}_{25}$ et $\mathbf{F}_{49}$.

Dans chacun des cas, on exhibera un générateur du groupe multiplicatif et on déterminera les sous-corps.

Exercice 26. Expliciter un isomorphisme entre les corps finis $\mathbf{F}_2[X]/(X^3 + X + 1)$ et $\mathbf{F}_2[Y]/(Y^3 + Y^2 + 1)$.

Exercice 27. Soit $\mathbf{F}_q$ un corps fini à $q = p^n$ éléments, où p est premier.

(a) Soit K un sous-corps de $\mathbf{F}_q$. Montrer que $\operatorname{card} K = p^d$ avec $d|n$.

(b) Soit $\varphi : \mathbf{F}_q \to \mathbf{F}_q$ défini par $\varphi(x) = x^p$. Montrer que φ est un automorphisme $\mathbf{F}_p$-linéaire du corps $\mathbf{F}_q$.

(c) Montrer que K est l'ensemble des points fixes de φ^d.

(d) Réciproquement, montrer que $K_d = \{x \in \mathbf{F}_q ; \phi^d(x) = x\}$ est un sous-corps de $\mathbf{F}_q$ de cardinal p^d.

Exercice 28. Soit $\mathbf{F}_q$ un corps fini à q éléments. En adaptant l'argument d'Euclide, montrer qu'il existe une infinité de polynômes irréductibles unitaires dans $\mathbf{F}_q[X]$.

Exercice 29. Combien le groupe $\mathbf{F}_q^*$ possède-t-il de générateurs ?

Exercice 30. Montrer que $\mathbf{F}_{p^n}^*$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{F}_p)$.