Feuille d'exercices n°8

Exercice 1 Déterminer le pgcd et une relation de Bézout pour les éléments $3+i$ et $1+3i$ dans $\mathbf{Z}[i]$.

Exercice 2 Soit K un corps.

1. Soit $P \in K[X]$ de degré 2 ou 3. Montrer que P est irréductible si et seulement si P n'a pas de racine dans K.
2. Quels sont les polynômes irréductibles de degré 2 de $\mathbf{Z}/2\mathbf{Z}[X]$?
3. En déduire un critère pour qu'un polynôme de degré ≤ 5 de $\mathbf{Z}/2\mathbf{Z}[X]$ soit irréductible.
4. *Application :* montrer que $P = X^5+X^3+1$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 3 Soit p un nombre premier.

1. On suppose $p \equiv 3 \pmod 4$. En utilisant le fait que -1 n'est pas un carré modulo p, montrer que l'équation $x^2 + y^2 = p$ n'admet pas de solution dans $\mathbf{Q}^2$.
2. Montrer que l'équation $x^2+y^2 = 1$ admet une infinité de solutions dans $\mathbf{Q}^2$ (on pourra paramétrer le cercle par des fonctions rationnelles).
3. En déduire que si $p = 2$ ou $p \equiv 1 \pmod 4$, l'équation $x^2 + y^2 = p$ admet une infinité de solutions dans $\mathbf{Q}^2$.
4. Montrer que l'équation $x^2 + y^2 + z^2 = 7$ n'a pas de solutions dans $\mathbf{Q}^3$.

Exercice 4 Le but de cet exercice est de montrer que l'équation $y^2 = x^3+7$ n'admet pas de solution dans $\mathbf{Z}^2$. Par l'absurde, on suppose qu'il existe une solution (x, y).

1. Montrer que y est pair.
2. Montrer que $x \equiv 1 \pmod 4$ et $x \geq 1$.
3. En déduire qu'il existe p premier $\equiv 3 \pmod 4$ divisant $x + 2$.
4. Montrer que $x + 2$ divise $y^2 + 1$ et conclure.

Remarque : on peut montrer, mais c'est plus difficile, que cette équation n'a pas de solution dans $\mathbf{Q}^2$.

Exercice 5 Soit $a, b, m \in \mathbf{Z}$.

1. Montrer que la congruence $ax \equiv b \pmod{m}$ a une solution dans $\mathbf{Z}$ si et seulement si $\text{pgcd}(a, m)$ divise b.
2. Déterminer la solution générale en fonction d'une solution particulière.
3. Résoudre la congruence $8x \equiv 6 \pmod{50}$.

Exercice 6 Déterminer les solutions de l'équation $x^2 \equiv 9$ dans $\mathbf{Z}/35\mathbf{Z}$.

Exercice 7

1. Déterminer un générateur de $(\mathbf{Z}/17\mathbf{Z})^*$.
2. En déduire les solutions de $x^4 \equiv 1 \pmod{17}$.
3. Combien y a-t-il de puissances quatrièmes dans $(\mathbf{Z}/17\mathbf{Z})^*$?

Exercice 8 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 9 Le but de cet exercice est de montrer que pour tout $m \geq 1$, il existe une infinité de nombres premiers congrus à 1 modulo m.

1. Soit p un nombre premier $\neq 3$. Montrer que si p divise $a^2 + a + 1$ avec $a \in \mathbf{Z}$, alors a est d'ordre 3 dans $(\mathbf{Z}/p\mathbf{Z})^*$.
2. En déduire le résultat pour $m = 3$.
3. Soit p premier et $m \geq 1$ non divisible par p. Montrer que $X^m - \overline{1} \in \mathbf{Z}/p\mathbf{Z}[X]$ n'a pas de racine double dans $\mathbf{Z}/p\mathbf{Z}$.
4. On suppose 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.
5. En déduire le résultat.

Exercice 10 (Un cas particulier du lemme de Hensel) Soit p un nombre premier impair. Soit $a \in \mathbf{Z}$ tel que la classe de $a \pmod{p}$ est un carré non nul dans $\mathbf{Z}/p\mathbf{Z}$.

1. Montrer que pour tout $n \geq 1$, la congruence $x^2 \equiv a \pmod{p^n}$ admet (au moins) une solution dans $\mathbf{Z}$.
2. Montrer que cette congruence a exactement deux solutions dans $\mathbf{Z}/p^n\mathbf{Z}$.

Exercice 11 Soit $k \geq 1$. Montrer qu'il existe un entier naturel n de k chiffres tel que l'écriture décimale de n^2 se termine par n. En trouver pour $k \leq 3$.