Université d'Évry Val d'Essonne 2009-2010

M54 algèbre et arithmétique

Feuille 1 — Inversibles de $\mathbf{Z}/n\mathbf{Z}$

Exercice 1. Soient a et n deux entiers. Montrer que les assertions suivantes sont équivalentes.

1. La classe $\bar{a}$ de a est inversible dans $\mathbf{Z}/n\mathbf{Z}$;
2. Il existe un entier k tel que $a^k \equiv 1 \mod n$;
3. $a^{\Phi(n)} \equiv 1 \mod n$.

Exercice 2. On décrit les groupes multiplicatifs $(\mathbf{Z}/n\mathbf{Z})^\times$ pour certaines valeurs de l'entier n.

1. Montrer que tous les éléments de $(\mathbf{Z}/5\mathbf{Z})^\times$ sont de la forme $\bar{2}^k$, $k \in \mathbf{N}$. Ce groupe est donc cyclique, trouver un autre générateur.
2. Quels sont les groupes cycliques parmi $(\mathbf{Z}/10\mathbf{Z})^\times$, $(\mathbf{Z}/12\mathbf{Z})^\times$, $(\mathbf{Z}/14\mathbf{Z})^\times$?

Exercice 3. Calculer $\Phi(8)$. Montrer qu'il existe un entier k divisant strictement $\Phi(8)$ tel que $a^k \equiv 1 \mod 8$, pour tout a premier à 8.

Exercice 4. Soit $d > 0$ un entier. Montrer que les racines de l'équation $X^d = 1$ dans $\mathbf{Z}/n\mathbf{Z}$ forment un sous-groupe (multiplicatif) de $(\mathbf{Z}/n\mathbf{Z})^\times$.

Exercice 5 (Variante du théorème de Wilson)**.** Montrer qu'un entier $n > 0$ divise $(n-1)!$ sauf si $n = 4$ ou si n est premier.

Exercice 6. Soient p un nombre premier impair et $q = \frac{p-1}{2}$. Montrer les assertions suivantes.

1. Pour tout entier x premier à p, on a $x^q \equiv \pm 1 \mod p$.
2. L'application $f\colon (\mathbf{Z}/p\mathbf{Z})^\times \to \{-1, 1\}$, qui à $\bar{x}$ associe $\bar{x}^q$, est un morphisme de groupes. Le noyau de f possède q éléments.
3. Si $\bar{x}$ est un carré dans $(\mathbf{Z}/p\mathbf{Z})^\times$ alors $f(\bar{x}) = 1$.
4. Dans le corps $(\mathbf{Z}/p\mathbf{Z})^\times$, on a $x^2 = y^2$ si et seulement si $x = \pm y$. Il existe q carrés dans $(\mathbf{Z}/p\mathbf{Z})^\times$.
5. x est un carré modulo p si et seulement si $x^q \equiv 1 \mod p$.
6. -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$.

Exercice 7 (Exemples de sommes de carrés)**.** 1. Ecrire 2, 5 et 13 comme somme de deux carrés.

2. Vérifier que $a^2 + b^2$ n'est pas congru à 3 modulo 4, quelques soient les entiers a et b. En déduire qu'un entier $n \equiv 3 \mod 4$ n'est pas la somme de deux carrés.

3. Montrer qu'on a $21 \equiv 1 \mod 4$ alors que 21 n'est pas la somme de deux carrés.

Exercice 8. Soit p un nombre premier. On note m la partie entière de $\sqrt{p}$ (soit le plus grand entier tel que $m^2 < p$).

1. Soient x un entier et $E = 0, 1, \dots, m$. En comptant le nombre d'éléments de $E \times E$, montrer qu'il existe deux couples distincts (a, b) et (a', b') tels que $ax + b \equiv a'x + b' \mod p$.
2. On suppose qu'il existe un entier x tel que $x^2 \equiv -1 \mod p$. Déduire de la question précédente qu'on a
$$(a - a')^2 + (b - b')^2 \equiv 0 \mod p \ ,$$
où $0 < (a - a')^2 < p$ et $0 < (b - b')^2 < p$, donc que p est la somme de deux carrés.
3. Conclure que p est la somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

Exercice 9. On définit la norme d'un nombre complexe $z = a + ib$ par
$$N(z) = z\bar{z} = |z|^2 = a^2 + b^2 \ .$$

1. Montrer que la norme est multiplicative : $N(zt) = N(z)N(t)$.
2. Si $m = a^2 + b^2$ et $n = c^2 + d^2$ sont sommes de deux carrés, en déduire qu'il en de même de leur produit (on pourra aussi décomposer explicitement mn en somme de deux carrés).

Exercice 10 (Théorème des deux carrés)**.**

1. Soit $n = d^2m$, où m et d sont entiers. Montrer que n est somme de deux carrés si et seulement si m est somme de deux carrés.
2. Soit n un entier dont tout facteur premier p tel que $p \equiv 3 \mod 4$ est d'exposant pair. Déduire de la question précédente et des exercices 8 et 9, que n est somme de deux carrés.
3. Soit $n = a^2 + b^2$ un entier, somme de deux carrés. Montrer que, pour tout facteur premier p de n tel que $p \equiv 3 \mod 4$, p divise a et b. (Sinon -1 serait un carré modulo p.) En déduire que p^2 divise n et que le quotient n/p^2 est somme de deux carrés.
4. Si n est somme de deux carrés, conclure que tout facteur premier p de n tel que $p \equiv 3 \mod 4$ est d'exposant pair.