Master1, mathématiques
Algèbre 1

Devoir surveillé du 2 décembre 2003

Durée: 2 heures
Document autorisé: une feuille A4 manuscrite

1. Pour certaines valeurs de l'entier p, on considère l'équation en entiers $\mathbf{E}(p)$: $x^2 + 5y^2 = pz^2$. On note $\overline{\mathbf{E}_p}$ l'équation $x^2 + 5y^2 = \overline{0}$ considérée dans $\mathbb{Z}/p\mathbb{Z}$.

a) On prend $p = 11$. Montrer que l'équation $\overline{\mathbf{E}_{11}}$ a pour unique solution $(\overline{0}, \overline{0})$.

On note $\mathcal{N}$ l'ensemble des nombres premiers p pour lesquels -5 *n'est pas* un carré modulo p.

b) On suppose que $p \in \mathcal{N}$. Résoudre l'équation $\overline{\mathbf{E}_p}$. Montrer que l'équation $\mathbf{E}(p)$ a pour unique solution le triplet $(0, 0, 0)$.

c) Caractériser en terme de congruence les nombres premiers p qui sont dans $\mathcal{N}$.

2. L'anneau quotient $A = \mathbb{Z}[i]/(3 + i)$ est-il intègre?
Montrer que la classe de 7 dans A est inversible et déterminer son inverse.

3. Soit p un nombre premier impair. On note G le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ et on se donne une classe n de G qui *n'est pas* un carré modulo p. Soit $a \in G$ un carré modulo p. Le but de l'exercice est de trouver une racine carrée de a, c'est–à–dire un élément y de G tel que $y^2 = a$. Pour cela on écrit $p - 1 = 2^s t$ où t est impair, et on note $b = n^t$.

a) Déterminer l'ordre de b dans G. Décrire en fonction de b le sous–groupe de G formé des éléments x tels que $x^{2^{s-1}} = 1$.

b) On pose $r = a^{(t+1)/2}$. Montrer que $(a^{-1}r^2)^{2^{s-1}} = 1$.

c) Déduire de a) et b) qu'il existe $j \in [0, \cdots, 2^{s-1} - 1]$ tel que $(rb^j)^2 = a$.

d) Appliquer ce qui précède pour trouver une racine carrée de $\overline{2}$ dans $\mathbb{Z}/41\mathbb{Z}$.

4. Soit p un nombre premier impair tel que $q = 2p - 1$ soit premier. On pose $n = pq$.

a) Calculer le nombre de classes d'entiers b modulo n telles que $b^{n-1} \equiv 1 \bmod n$.

b) Dénombrer: les classes d'entiers b modulo q qui vérifient $b^{(p-1)/2} \equiv 1 \bmod q$, celles qui vérifient $b^{p-1} \equiv 1 \bmod q$, enfin celles qui vérifient $b^{(p-1)/2} \equiv -1 \bmod q$.

c) Déterminer la proportion de témoins d'Euler dans $(\mathbb{Z}/n\mathbb{Z})^\times$ (les *témoins d'Euler* sont les classes d'entiers b modulo n qui vérifient $b^{(n-1)/2} \not\equiv (\frac{b}{n}) \bmod n$).

*****