Université Joseph Fourier
Master1, mathématiques

Algèbre 1, devoir surveillé
du 6 décembre 2004, 13h30-15h30

Document autorisé : une feuille A4 manuscrite

I

Soient p un nombre premier tel que $p \equiv 3 \bmod 4$, et a un inversible modulo p. Montrer que a est une racine primitive si et seulement si $-a$ est d'ordre $(p-1)/2$.

II

Soit p un nombre premier impair, distinct de 3 et 7. Caractériser chacune des propriétés suivantes en terme de la classe de congruence de p modulo un entier convenable :

a) p est un carré modulo 21;

b) 21 est un carré modulo p.

III

Soient n, $b \in \mathbb{N}$ vérifiant : b est impair et $b < 2^n$. On pose $N = b\,2^n + 1$. On suppose qu'il existe a entier premier à N qui vérifie : $a^{(N-1)/2} \equiv -1 \bmod N$.

1. Soit p un facteur premier de N. Quelles sont les classes modulo p de $a^{b\,2^{n-1}}$ et $a^{b\,2^n}$?

2. Soit d le pgcd de $p-1$ et $b\,2^n$. Montrer que $a^d \equiv 1 \bmod p$.

3. Écrivons $d = b'\,2^{n'}$, où b' est impair. Déduire de 1. et 2. que $n' = n$.

4. Si N est décomposable, montrer qu'il admet un facteur premier $p < 2^n$.

5. Déduire de ce qui précède que N est premier.

IV

On considère l'anneau $A = \mathbb{Z}[i]$ des entiers de Gauss. On note $N : z \mapsto |z|^2$, application multiplicative de A dans $\mathbb{N}$. On rappelle que (A, N) est euclidien et on admettra qu'un élément z de A est inversible si et seulement si $N(z) = 1$.

T.S.V.P.

Soit alors p un nombre premier tel qu'il existe $x \in \mathbb{Z}$ vérifiant $x^2 \equiv -1 \bmod p$. Dans la suite on fixe un tel x.

1. Avec le cours, donner un critère simple pour qu'un nombre premier vérifie la propriété de p.

2. Montrer que l'idéal (p) de A n'est pas premier.

3. Montrer que $d = \mathrm{pgcd}_A(x+i, p)$ (qui est défini modulo $A^\times$), n'est ni 1 ni p. Si $d = a + ib$ avec $a, b \in \mathbb{Z}$, montrer que $p = a^2 + b^2$.

4. L'écriture $p = a^2 + b^2$, où a, $b \in \mathbb{Z}$, détermine–t–elle la paire $\{a^2, b^2\}$ de manière unique?

5. On prend $p = 397$, et on donne $63^2 = 3969 \equiv -1 \bmod p$. Déterminer le pgcd dans A de $63 + i$ et 397. Vérifier qu'on obtient $397 = a^2 + b^2$.