UNIVERSITÉ DE RENNES 1

Algèbre générale de base

TD

Feuille d'exercices 7

Exercice 1

Évaluez les symboles de Legendre suivants :

$$\left(\frac{71}{73}\right), \left(\frac{14}{23}\right), \left(\frac{37}{61}\right).$$

Exercice 2

1. Soit $p > 2$ un nombre premier. Montrez que le polynôme $aX^2 + bX + c$ admet des racines dans $\mathbb{F}_p$ ssi $\Delta = b^2 - 4ac$ est un résidu quadratique modulo p.
2. Résoudre $3X^2 + 6X + 5 \equiv 0 \; mod \; 89$

Exercice 3

Soit $p \geqslant 3$ premier. Montrez que $\left(\frac{5}{p}\right) = +1$ ssi $p = 1, 9, 11, \text{ou } 19 \, mod \, 20$.

Exercice 4

Si $p = 2^k + 1$ est premier, montrez que tout entier a qui est non-résidu quadratique mod p est une racine primitive de p (càd un générateur de $\mathbb{F}_p^\times$).

Exercice 5

1. Soit n un entier non multiple de 3. Montrez que $4n^2 + 3$ possède un facteur premier congru à 7 modulo 12.
2. Montrez qu'il existe un nombre infini de nombres premiers congru à 7 modulo 12.

Exercice 6

Soit n impair et $n = p_1^{e_1}...p_k^{e_k}$ sa décomposition en facteurs premiers. On montre que a tel que $(a, n) = 1$ est un carré modulo n ssi il est un carré modulo p_i pour tout $i \in \{1, .., k\}$.

1. Montrez que a est un carré modulo n ssi il est un carré modulo $p_i^{e_i}$ pour tout $i \in \{1, .., k\}$.
2. Supposons $n = p^e$. Montrez que a est un carré modulo p^e ssi a est un carré modulo p.
3. Est-ce que 13 est un carré modulo $1127 (= 49 \times 23)$?

Remarque : Plus généralement, si $n = 2^{e_0} p_1^{e_1}...p_k^{e_k}$, et $(a, n) = 1$, on peut montrer que a est un carré modulo n ssi les deux conditions suivantes sont vérifiées :

— Pour $i \in \{1, .., k\}$, $\left(\frac{a}{p_i}\right) = 1$.

— Si $e_0 = 2$ alors $a \equiv 1\,[4]$, et si $e_0 \geqslant 3$, alors $a \equiv 1\,[8]$.