UNIVERSITÉ DE RENNES 1

Théorie des nombres

Interrogation 1

Durée : 1h
Les notes de cours et de TD sont autorisées. Les calculatrices sont autorisées. Les téléphones sont interdits.

Exercice 1

Trouver tous les générateurs de $\mathbb{F}_{11}^{\times}$.

Exercice 2

Calculer les symboles de Jacobi suivants. (Chaque étape du calcul devra être justifiée).

1. $\left(\frac{58}{77}\right)$
2. $\left(\frac{19}{41}\right)$
3. $\left(\frac{77}{91}\right)$
4. $\left(\frac{28}{59}\right)$

Exercice 3

1. Soient p un nombre premier impair et un entier $n \geqslant 1$. Soit $a \in \mathbb{Z}$ un entier premier à p. On suppose qu'il existe un entier x tel que $x^2 \equiv a \pmod{p^n}$. Montrer qu'il existe un $u \in \mathbb{Z}$ tel que $(x + p^n u)^2 \equiv a \pmod{p^{n+1}}$.
2. En déduire que a est un carré modulo p^n si et seulement si $\left(\frac{a}{p}\right) = 1$.
3. Montrer de même que si a est un entier impair et si $n \geqslant 3$, alors a est un carré modulo 2^n si et seulement si $a \equiv 1 \pmod{8}$. (Indication : on pourra chercher u tel que $(x + 2^{n-1}u)^2 \equiv a \pmod{2^{n+1}}$).
4. Soit $N \geqslant 1$ un entier, et soit a un entier premier à N. Notons $N = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ la décomposition de N en produit de facteurs premiers, avec $p_1 < \cdots < p_m$ premiers et des entiers $\alpha_1, \dots, \alpha_m > 0$. Montrer que les deux propriétés suivantes sont équivalentes :

(i) a est un carré modulo N ;

(ii) pour tout $i \in \{1, \dots, m\}$,

$$\begin{cases} a \equiv 1 \pmod 4 & \text{si } p_i = 2 \text{ et } \alpha_i = 2 \\ a \equiv 1 \pmod 8 & \text{si } p_i = 2 \text{ et } \alpha_i \geqslant 3 \\ \left(\frac{a}{p_i}\right) = 1 & \text{si } p_i > 2. \end{cases}$$