UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille de TD 5

Exercice 1

Évaluez les symboles de Legendre suivants :

$$a = \left(\frac{71}{73}\right),\ b = \left(\frac{-219}{383}\right),\ c = \left(\frac{3658}{12703}\right).$$

Exercice 2

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.

Exercice 3

Déterminez si les congruences suivantes ont une solution.

1 $X^2 \equiv 219\ mod\ 419$,

2 $3X^2 + 6X + 5 \equiv 0\ mod\ 89$,

3 $2X^2 + 5X - 9 \equiv 0\ mod\ 101$.

Exercice 4

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

Exercice 5

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 6

Symbole de Jacobi

1 Soient a, b deux entiers tels que $(a, b) = 1$, et $b > 2$ est impair. Si $b = p_1 ... p_k$, on définit le *symbole de Jacobi*:

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right) ... \left(\frac{a}{p_k}\right),$$

où les $\left(\frac{a}{p_i}\right)$ sont les symboles de Legendre.

Évaluez les symboles de Jacobi suivants :

$$a = \left(\frac{21}{221}\right),\ b = \left(\frac{215}{253}\right),\ c = \left(\frac{631}{1099}\right).$$

2 Montrez que si a est résidu quadratique mod b, alors $\left(\frac{a}{b}\right) = +1$, mais que la réciproque est fausse.

Exercice 7

Soit $p > 2$ un premier. On pose pour $a \in \mathbf{Z}$,

$$g_a = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{ak},$$

où $\zeta = e^{2i\pi/p}$.

1 Montrez que $g_0 = 0$.

2 Montrez que

$$g_a = \left(\frac{a}{p}\right) g_1.$$

3 Montrez que

$$g_1^2 = (-1)^{(p-1)/2} p.$$

Indication : On pourra calculer de deux façons différentes la somme

$$S = \sum_{a=1}^{p-1} g_a g_{-a}.$$

Exercice 8

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.