MAT 2440 : Théorie des nombres

Logarithme discret

Exercice 1 Donner l'ordre de $2, 4, 7, 8, 11, 13, 14$ modulo 15. Est-ce qu'il existe des racines primitives modulo 15 ?

Exercice 2 Trouver toutes les racines primitives modulo 17 et calculer 11×13 modulo 17 par les logarithmes discrets.

Exercice 3 Chercher les n tels que $8^{2006} \equiv 8^n \mod 27$.

Exercice 4 Sachant que 2 est racine primitive modulo 29,

1. trouver toutes les racines primitives modulo 29,
2. déterminer si la congruence $x^7 \equiv 2 \mod 29$ a une solution,
3. montrer que, pour tout entier n, la congruence $x^3 \equiv n \mod 29$ a une solution.

Exercice 5 Soit $p = 4t + 1$ un nombre premier. Montrer que a est une racine primitive modulo p si et seulement si $-a$ est une racine primitive modulo p.

Exercice 6 Donner les solutions de

1. $x^3 \equiv 1 \mod 19$,
2. $x^4 \equiv 1 \mod 17$.

Exercice 7 Résoudre $1 + x + \ldots + x^6 \equiv 0 \mod 29$.

Exercice 8 Soit p un nombre premier impair.

1. Montrer que, si a un entier d'ordre $n > 1$ modulo p, alors

$$a^{n-1} + a^{n-2} + \ldots + 1 \equiv 0 \mod p.$$

2. Montrer que, si a est d'ordre 3 modulo p, alors $a + 1$ est d'ordre 6 modulo p.