Arithmétique – Partie 4 : Congruences

Exercice 1.

Simplifier les expressions suivantes (sans calculatrice). Par exemple "simplifier 72 [7]" signifie "trouver n entre 0 et 6 tel que $72 \equiv n\,[7]$" ; la réponse est $n = 2$.

— $45\,[7]$, $39\,[7]$, $45+39\,[7]$, $45 \times 39\,[7]$, $45^2\,[7]$, $39^3\,[7]$.

— $1052\,[22]$, $2384\,[22]$, $2384-1052\,[22]$, $1052^2 \times 2384\,[22]$.

Exercice 2.

1. Calculer 2^{500} modulo 13 (utiliser le petit théorème de Fermat).
2. Calculer 1000^{123} modulo 17.
3. Calculer 3^{1234} modulo 15 (attention on ne peut pas appliquer le petit théorème de Fermat, étudier d'abord 3^k modulo 15 pour les petites valeurs de k).

Exercice 3.

Les deux premières questions reprennent un exercice précédent et montrent l'efficacité des congruences pour les calculs.

1. Soit $n = p^2$ le carré d'un entier. Déterminer les valeurs possibles de n modulo 4.
2. Montrer que si n est un entier naturel somme de deux carrés d'entiers alors n modulo 4 n'est jamais égal à 3.
3. Soit $n = p^2$ le carré d'un entier. Déterminer les valeurs possibles de n modulo 8.
4. Montrer que si n est un entier naturel somme de trois carrés d'entiers alors n modulo 8 n'est jamais égal à 7.

Exercice 4.

1. Montrer que $p = 101$ est un nombre premier.
2. Soit a un entier avec $1 \leqslant a < p$. Montrer que $\mathrm{pgcd}(a, p) = 1$.
3. Écrire le théorème de Bézout pour le pgcd précédent ; en déduire qu'il existe $u \in \mathbb{Z}$ tel que $au \equiv 1\,[p]$. *Un tel u s'appelle un **inverse** de a modulo p.*
4. Trouver un inverse de $a = 15$ modulo $p = 101$.
5. Trouver une solution de l'équation d'inconnue x (un entier) : $15x \equiv 7\,[101]$.
6. Reprendre tout l'exercice avec $p = 103$.

Exercice 5.

Les **nombres de Fermat** F_n sont les entiers définis pour $n \in \mathbb{N}$ par

$$F_n = 2^{2^n} + 1$$

1. Montrer que pour tout entier naturel n, on a $F_{n+1} = (F_n - 1)^2 + 1$.

2. Démontrer que pour $n \geqslant 2$, l'écriture décimale des nombres de Fermat (F_n) se termine par le chiffre 7.