Énoncés : V. Gritsenko
Corrections : J.-F. Barraud

# Congruence

## Exercice 1

1. Trouver

$$999\cdot 1998 \mod 1999, \qquad 136^7 \mod 137, \qquad 1997\cdot 1998\cdot 1999\cdot 2000 \mod 2001.$$

2. Trouver $2792^{217} \mod 5$ et $10^{1000} \mod 13$.

[002240]

## Exercice 2

1. Examiner les carrés $a^2 \mod n$ pour $n = 3,\ 4,\ 8$.
2. Examiner $a^3 \mod 9$ et $b^4 \mod 16$.

[002241]

## Exercice 3

Passer $\mod n$ avec un module approprié et montrer que chacune des équations suivantes n'a aucune solution dans $\mathbb{Z}$ :

1. $3x^2+2=y^2$ ;
2. $x^2+y^2=n$ pour $n = 2003, 2004$ ;
3. $x^2+y^2+z^2=1999$ ;
4. $x^3+y^3+z^3=5$ ;
5. $x_1^4+x_2^4+\cdots+x_{15}^4=7936$.

[002242]

## Exercice 4

On dit que $a \mod n$ est inversible si il existe $b \mod n$ tel que $ab\equiv 1 \mod n$.

1. Trouver tous les éléments inversibles modulo 5, 6, 9, 11.
2. Trouver $\text{pgcd}(107,281)$ et sa representation linéaire en utilisant *l'algorithme d'Euclide*.
3. Trouver l'inverse de $107 \mod 281$ et l'inverse de $281 \mod 107$.
4. Montrer que $a \mod n$ est inversible ssi $a$ et $n$ sont premiers entre eux.

[002243]

## Exercice 5

Trouver toutes les solutions dans $\mathbb{Z}$ :

1. $2x+3\equiv 10 \mod 13$ ;
2. $\begin{cases} 2x+3y\equiv 5 \mod 7 \\ 5x+2y\equiv 2 \mod 7; \end{cases}$

3. $x^2+2x+14 \equiv 0 \mod 17$.

[002244]

**Exercice 6** Le petit théorème de Fermat

Soit $p$ un nombre premier et $a$ un nombre premier à $p$. Montrer que :

1. $am \equiv an \mod p$ ssi $m \equiv n \mod p$ ;
2. La suite $a,\ 2a,\ 3a,\ldots,(p-1)a \mod p$ est une permutation de la suite $1,\ 2,\ 3,\ldots,(p-1) \mod p$ ;
3. $a^{p-1} \equiv 1 \mod p$.

[002245]

**Exercice 7**

1. Examiner $7^n+11^n \mod 19$.
2. Trouver $2792^{217} \mod 5$ et $10^{1000} \mod 13$.
3. Montrer que 13 divise $2^{70}+3^{70}$ et 11 divise $2^{129}+3^{118}$.

[002246]

**Exercice 8** Théorème de Wilson

Soit $p = 2m+1$ un nombre premier. Montrer que :

1. $(p-1)! \equiv -1 \mod p$ ;
2. $(m!)^2 \equiv (-1)^{m+1} \mod p$.

[002247]

**Exercice 9**

Soit $p > 2$ un nombre premier.

1. Soit $a$ premier à $p$. Supposons que la congruence $x^2 \equiv a \mod p$ possède une solution. Montrer que $a^{(p-1)/2} \equiv 1 \mod p$.
2. La congruence $x^2 \equiv -1 \mod p$ a une solution ssi $p \equiv 1 \mod 4$.

[002248]