Quelques démonstrations et arithmétique modulaire

Exercice 1

Soit $n \in \mathbb{N}$ un entier. Montrer que le carré de $2\,n + 1$ est toujours congru à 1 modulo n.

Exercice 2

Quel est le reste modulo 4 d'un nombre entier pair élevé au carré ?

Exercice 3

En utilisant les deux résultats précédents, montrer que la somme des carrés de deux nombres impairs ne peut pas être le carré d'un nombre entier.

Exercice 4

Montrer qu'il existe $n \in \mathbb{N}$ tel que $n^2 + n + 41$ n'est pas un nombre premier.

Exercice 5

Montrer qu'un nombre entier qui n'est pas premier admet au moins un facteur plus petit ou égal à sa racine carrée.

Exercice 6

Calculer :

a) $999 \cdot 1998 \pmod{1999}$

b) $136^7 \pmod{137}$

c) $1997 \cdot 1998 \cdot 1999 \cdot 2000 \pmod{2001}$

Exercice 7

Résoudre les équations suivantes.

a) $3x \equiv 7 \pmod{9}$

b) $4x \equiv 2 \pmod{5}$

c) $2x \equiv 6 \pmod{8}$

Exercice 8

Trouver le reste de la division par 13 du nombre 100^{1000}.
Trouver le reste de la division par 5 du nombre 2792^{217}.

Exercice 1

$$\forall n \in \mathbb{N},\ (2n+1)^2 \equiv 1 \pmod{n}$$

Par définition $a \equiv b \pmod{n}$ si $n \mid (a-b)$

En effet $(2n+1)^2 = 4n^2+4n+1 = n(4n+4)+1$.

Donc $(2n+1)^2 - 1 = n(4n+1)$ et $n \mid n(4n+1)$

Donc $(2n+1)^2 \equiv 1 \pmod{n}$

Exercice 2

Pour tout entier pair p, il existe $K \in \mathbb{Z}$ tel que $p = 2K$.

$p^2 = (2K)^2 = 4K^2$.

Comme $4 \mid 4K^2$, alors $4K^2 \equiv 0 \pmod{4}$ et $p^2 \equiv 0 \pmod{4}$

Exercice 3

Soit a, b deux entiers impairs. Alors, il n'existe pas $K \in \mathbb{Z}$ tel que $a^2 + b^2 = K^2$.

Posons $a = 2a_1 + 1$ et $b = 2b_1 + 1$ les deux entiers impairs.

$$a^2 + b^2 = (2a_1+1)^2 + (2b_1+1)^2 = 4a_1^2 + 4a_1 + 1 + 4b_1^2 + 4b_1 + 1$$
$$= 4(a_1^2 + b_1^2 + a_1 + b_1) + 2$$

Donc $a^2 + b^2 \equiv 2 \pmod{4}$

1°) Si a^2+b^2 est pair, alors $a^2+b^2 \equiv 0 \pmod{4}$

2°) Si a^2+b^2 est impair, alors $a^2+b^2 \equiv 1 \pmod{4}$

Comme $a^2 + b^2 \equiv 2 \pmod 4$, il est n'existe pas de $c \in \mathbb{N}$ tel que $a^2 + b^2 = c^2$ si a et b sont impairs.

Exercice 4

Il suffit de choisir $n = 41$.

Alors $41^2 + 41 + 41 = 41 \cdot 43$ qui n'est évidemment pas premier.

Exercice 5

Soit $n \in \mathbb{N}$ non premier. Alors il existe $k \in \mathbb{N}$, avec $k < \sqrt{n}$, qui divise n. On suppose que $n \geq 2$.

En effet, n n'est pas premier, il existe deux entiers a et b tels que $n = a \cdot b$, avec $1 < a \leq b < n$.

On a $a \leq b \quad | \cdot a, a > 0$

$a^2 \leq ab$

$a^2 \leq n$ et donc $a \leq \sqrt{n}$

Exercice 6

a) $999 \cdot 1998 \pmod{1999}$

- $999 \cdot 1998 \equiv 1996002$

1996002	1999
	998
r : 1000	

$999 \cdot 1998 \equiv 1000 \pmod{1999}$

- $999 \cdot 1998 \equiv (-1000) \cdot (-1) \equiv 1000 \pmod{1999}$

b) $136^7 \pmod{137}$

$136^7 \equiv (-1)^7 \equiv -1 \equiv 136 \pmod{137}$

c) $1997 \cdot 1998 \cdot 1999 \cdot 2000 \pmod{2001}$

$(-4) \cdot (-3) \cdot (-2) \cdot (-1) \equiv 24 \pmod{2001}$

Exercice 7

a) $3x \equiv 7 \pmod 9$

Comme $3 \mid 9$ et que $3 \nmid 7$ alors l'équation n'a pas de solution.

b) $4x \equiv 2 \pmod 5$

$4 \cdot 4 \equiv 1 \pmod 5$

Donc 4 est l'inverse de 4 mod 5.

$4 \cdot 4x \equiv 4 \cdot 2 \pmod 5$

$x \equiv 3 \pmod 5$

c) $2x \equiv 6 \pmod 8$

$2 \mid 6$ et $2 \mid 8$

Cherchons les solutions de

$x \equiv 3 \pmod 4$

On a :

$$\begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 7 \pmod 8 \end{cases}$$

Exercice 8

$100^{1000} \equiv 9^{1000} \pmod{13}$

$1000 = 512 + 256 + 128 + 64 + 32 + 8$

$9^1 \equiv 9 \pmod{13}$

$9^2 \equiv 81 \equiv 3 \pmod{13}$

$9^4 \equiv 3^2 \equiv 9 \pmod{13}$

$9^8 \equiv 9^2 \equiv 3 \pmod{13}$

$9^{16} \equiv 9 \pmod{13}$

...

Ainsi $9^{1000} \equiv (9^2)^{500} \equiv 3^{500} \equiv (9^2)^{125} \equiv 3^{125} \pmod{13}$

$\equiv 3 \cdot 3^{124} \equiv 3 \cdot (9^2)^{31} \equiv 3 \cdot 3^{31} \pmod{13}$

$\equiv 3 \cdot 3^3 \cdot (9^2)^7 \equiv 3 \cdot 3^3 \cdot 3^7 \pmod{13}$

$\equiv 3^{11} \equiv 3^3 \cdot 3^8 \equiv 3^3 \cdot (9^2)^2 \equiv 3^5 \pmod{13}$

$\equiv 3 \cdot 9^2 \equiv 3 \cdot 3 \equiv 9 \pmod{13}$

Donc $100^{1000} \equiv 9 \pmod{13}$

$2792 \equiv 2 \pmod{5}$.

On calcule $2^{217} \pmod{5}$

$2^1 \equiv 2 \pmod{5}$

$2^2 \equiv 4 \pmod{5}$

$2^4 \equiv 1 \pmod{5}$

Donc $2^{217} \equiv (2^4)^{54} \cdot 2$

$217 = 4 \cdot 54 + 1$

Donc $2^{217} \equiv 2 \pmod 5$

et ainsi $2792^{217} \equiv 2 \pmod 5$