

Exercice 1 On pose $\sum_{k=1}^n \frac{1}{k} = \frac{a_n}{b_n}$ avec $a_n \wedge b_n = 1$, pour $n \in \mathbb{N}^*$.

Montrer que si n est premier $n > 2$ alors n divise a_{n-1} .

Exercice 2 Déterminer selon $n \in \mathbb{N}$ le reste de la division euclidienne par 7 de

$$A = 851^{3n} + 851^{2n} + 851^n + 2.$$

Exercice 3 Montrer que: $\forall n \in \mathbb{N} : 6 \mid 5n^3 + n$ et $7 \mid 3^{2n+1} + 2^{n+2}$.

Exercice 4 Montrer qu'il y a une infinité de nombres premiers de la forme $4k - 1$ avec $k \in \mathbb{N}$.

Exercice 5 Soient $x \in \mathbb{N} \setminus \{0; 1\}$, $p, q \in \mathbb{N}^*$ et $d = p \wedge q$.

Montrer que : $(x^p - 1) \wedge (x^q - 1) = (x^d - 1)$.

Exercice 6 Soit $k \in \mathbb{N}^*$, montrer que si $2^k + 1$ est premier alors k est une puissance de 2. Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$.

Montrer que si $n \neq m$ alors $F_n \wedge F_m = 1$.

Exercice 7 Montrer que si $n \in \mathbb{N}$ est somme de deux carrés d'entiers alors le reste de la division euclidienne de n par 4 est différent de 3.

Exercice 8

1. Soient a, b , et c des entiers relatifs tels que $(a, b) \neq (0, 0)$, montrer que pour que l'équation

$$ax + by = c$$

ait une solution (x, y) en entiers relatifs x et y , il faut et il suffit que le $pgcd$ de a et b divise c .

2. Résoudre en entiers relatifs les équations suivantes:

$$7x - 9y = 1; \quad 7x - 9y = 6; \quad 11x + 17y = 5; \quad 11x + 56y = 12.$$

Exercice 9 Trouver une CNS pour que $ax + b \equiv 0 \pmod n$ ait une solution.

1. Soit $p \in \mathbb{Z}$ un nombre premier. Montrer que si $a \in \mathbb{Z}$ n'est pas congru à 0 modulo p alors p ne divise pas a et donc $pgcd(a, p) = 1$.
2. Soit $a \in \mathbb{Z}$ non congru à 0 modulo p avec p premier. Montrer qu'il existe $u \in \mathbb{Z}$ non congru à 0 modulo p vérifiant $au \equiv 1[p]$. (Remarquer que cela donne un inverse de a modulo p).

3. Montrer que si p n'est pas premier, il existe des éléments $a, u \in \mathbb{Z}$ non nuls modulo p tels que $au \equiv 0[p]$.

Exercice 10 Dans tout cet exercice, p désigne un nombre premier.

PARTIE I:

1. Montrer que : $\forall k \in \llbracket 1, p-1 \rrbracket : p$ divise \mathbb{C}_p^k .

2. En déduire que :

(a) $\forall n, m \in \mathbb{N} : (n+m)^p \equiv n^p + m^p \pmod p$.

(b) $\forall n \in \mathbb{Z} : n^p \equiv n \pmod p$, et en particulier si $p \wedge n = 1$ alors $n^{p-1} \equiv 1 \pmod p$.

PARTIE II:

Pour tout $A \in \mathbb{N}$, on note $(A \pmod p)$ le reste de la division euclidienne de A par p . Un entier $x \in \llbracket 1, p-1 \rrbracket$ est appelé une *racine primitive modulo p* lorsqu'on a:

$$\{(x^k \pmod p), \text{ pour } k \in \mathbb{N}\} = \llbracket 1, p-1 \rrbracket.$$

1. On prend dans cette question $p = 7$. Déterminer les racines primitives modulo 7.

On admet désormais que, quel que soit le nombre premier p , il existe au moins une racine primitive modulo p . Dans la suite, on désigne par g une racine primitive modulo p .

2. Soit $b \equiv a \pmod{p-1}$. Montrer que $(g^b \pmod p) = (g^a \pmod p)$.

- (a) Soit $A \in \llbracket 1, p-1 \rrbracket$. Justifier l'existence et l'unicité d'un entier $a \in \llbracket 0, p-2 \rrbracket$ tel que $A = (g^a \pmod p)$.

a est appelé *logarithme de base g modulo p* de A ; on le note $\ell(A)$, on a donc:

$$\ell(A) = a \iff \begin{cases} a \in \llbracket 0, p-2 \rrbracket, \\ (g^a \pmod p) = A. \end{cases}$$

- (b) Dans cette question, on prend $p = 7, A = 2, g = 5$. Déterminer $\ell(A)$.

3. Dans cette question, on se place dans le cas $p = 113, g = 55$ et on donne $\ell(2) = 60$ et $\ell(3) = 5$. Trouver $\ell(54)$.