M13 - TD n°2

Arithmétique — Congruences

Exercice 1

Résoudre dans $\mathbb{Z}$ le système d'équations $\begin{cases} x \equiv 2 \ mod\ 7 \\ x \equiv 1 \ mod\ 8 \\ x \equiv 3 \ mod\ 9 \end{cases}$

Exercice 2

On note $x = x_\ell \cdots x_0$ $(= x_\ell 10^\ell + \cdots + 10c_1 + c_0)$ l'écriture décimale d'un entier $x \in \mathbb{N}$.
1. Montrer la « **règle de 11** » : $x \equiv (-1)^\ell x_\ell + \cdots + (-1)^i x_i \cdots - x_1 + x_0$ (mod 11).
2. Calculer le reste de la division euclidienne de 641489 et 42813617 par 3, 9 et 11.

Exercice 3

1. Démontrer que le nombre $4^{12} + 2^6$ est un multiple de 13.
2. Quel est le reste de la division euclidienne de 2992^{217} par 5 ?
3. Montrer que $11 | 2^{123} + 3^{121}$.

Exercice 4

1. Montrer que pour tout $n \in \mathbb{Z}$, $169 \nmid n^2 + 20n + 74$.
2. Montrer que pour tout $n \in \mathbb{N}$, $9 | 2^{2n} + 15n - 1$.

Exercice 5

1. Dans $\mathbb{Z}/641\mathbb{Z}$, calculer successivement $\overline{2}^4 + \overline{5}^4$, $\overline{2}^7.(-\overline{5})$, $\overline{2}^{28}.\overline{5}^4$, $\overline{2}^{32} (= \overline{2}^{28}.\overline{2}^4)$ et $\overline{2}^{32} + 1$.
2. [Euler] Sans utiliser de calculatrice, démontrer que 641 divise $F_5 = 2^{32}+1 = 4294967297$.
(On a, en fait, $F_5 = 2^{32} + 1 = 4294967297 = 641.6700417$, où les deux facteurs sont premiers. Personne n'a jamais réussi à trouver un nombre de Fermat *F_n premier avec $n \geq 5$.)*

Exercice 6

1. Ecrire la table de multiplication des anneaux $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.
2. Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ et dans $\mathbb{Z}/6\mathbb{Z}$ les équations et le système suivant :
(*i*) $\overline{5}x + \overline{4} = \overline{-1}$.
(*ii*) $\overline{3}x + \overline{4} = \overline{0}$.
(*iii*) $\overline{2}x + \overline{2} = \overline{0}$.
(*iv*) $(\mathcal{S})$ $\begin{cases} \overline{3}x & + & \overline{2}y & = & \overline{1} \\ \overline{2}x & + & \overline{4}y & = & \overline{3} \end{cases}$
Justifier algébriquement la nature différente des résultats.

Exercice 7

Si $a \in \mathbb{Z}$, on notera $\overline{a}$ la classe de a modulo 61.
a) Déterminer l'ensemble des couples $(u, v) \in \mathbb{Z}^2$ solutions de $61u + 50v = 1$.
b) Quel est l'inverse de $\overline{50}$ dans le groupe multiplicatif $\left(\mathbb{Z}/61\mathbb{Z}\right)^*$?
c) Quel est l'ordre de $\overline{50}$ dans le groupe multiplicatif $\left(\mathbb{Z}/61\mathbb{Z}\right)^*$?
d) Déterminer le reste de 6150^{2002} modulo 61.

Exercice 8

Soit $p \geq 2$ un nombre premier.
1. Montrer que l'équation $x^2 = \bar{1}$ a exactement deux solutions dans $\mathbb{Z}/p\mathbb{Z}$ et qu'il s'agit de $\bar{1}$ et $\overline{-1}$.
2. Montrer que $(p-1)! \equiv -1 \mod p$ (théorème de Wilson). *Indication : On pourra regrouper chaque élément du produit avec son inverse.*
3. Montrer réciproquement que si $n \geq 2$ est un entier tel que $(n-1)! \equiv -1 \mod n$ alors n est premier.

Exercice 9

On se place dans $\mathbb{Z}/17\mathbb{Z}$.
1. Calculer l'inverse de $\bar{5}$.
2. Exactement la moitié des éléments de $\mathbb{Z}/17\mathbb{Z}^* := \mathbb{Z}/17\mathbb{Z} \setminus \{\bar{0}\}$ sont des carrés. Lesquels ?
3. Dans $\mathbb{Z}/17\mathbb{Z}$, résoudre l'équation $\bar{x}^2 + \bar{2} = \bar{0}$, puis $\bar{5}\bar{x}^2 + \overline{10} = \bar{0}$.
4. Pour quelles valeurs de $x \in \mathbb{Z}$ le nombre $5x^2 + 10$ est-il divisible par 17 ?

Exercice 10

Lagrange *a démontré qu'un entier positif peut toujours s'écrire comme une somme d'au plus quatre carrés. Le but de cet exercice est de démontrer que certains entiers ne peuvent pas s'écrire comme une somme de trois carrés ou moins.*

1. Déterminer l'ensemble $\{\bar{x}^2 + \bar{y}^2 + \bar{z}^2 \quad | \quad \bar{x}, \bar{y} \text{ et } \bar{z} \in \mathbb{Z}/8\mathbb{Z}\} \subset \mathbb{Z}/8\mathbb{Z}$.
2. Donner l'exemple d'une progression arithmétique infinie d'entiers positifs ne pouvant pas s'écrire comme une somme de trois carrés ou moins.

Gauss *a déterminé sous quelles conditions un entier positif $n \in \mathbb{N}$ ne peut pas être écrit comme une somme de trois carrés ou moins ; lorsque n est impair, c'est le cas si, et seulement si, $n \equiv 7 \pmod 8$.*

Exercice 11

Euler *a déterminé quels entiers positifs peuvent s'écrire comme une somme de deux carrés ou moins.*

1. Démontrer que lorsque $n \equiv 3 \pmod 4$, n ne peut pas s'écrire comme une somme de deux carrés ou moins.
2. Supposons que $n \equiv 3 \pmod 4$. Quels sont les exposants α pour lesquels n^α peut s'écrire comme une somme de deux carrés ou moins ?
3. Soient $n := a^2 + b^2$ et $m := c^2 + d^2$ deux entiers positifs pouvant s'écrire comme une somme de deux carrés ou moins. Démontrer que leur produit $m\,n$ peut également s'écrire comme une somme de deux carrés ou moins.
Indication : Calculer de deux façons différentes $|(a+bi)(c+di)|^2$.

Euler *a démontré que lorsque $n \in \mathbb{N}$ est un nombre premier impair, n peut s'écrire comme une somme de deux carrés si, et seulement si, $n \equiv 1 \pmod 4$.*

Exercice 12

1. Calculer $\varphi(15)$.
2. Dresser la table de Cayley de $(\mathbb{Z}/15\mathbb{Z})^\times$.
3. Calculer l'ordre de tout élément de $(\mathbb{Z}/15\mathbb{Z})^\times$. Le groupe $(\mathbb{Z}/15\mathbb{Z})^\times$ est-il cyclique ?
4. Mêmes questions pour $n = 10$, $n = 18$ et $n = 16$.
(Deux des quatre groupes sont cycliques.)