Fiche de TD 3

Exercice 1

i) Montrer que 7 divise $3^{512} - 2^{256}$ et 13 divise $2^{70} + 3^{70}$.

ii) Quel est le reste de la division euclidienne de $2222^{3333} + 3333^{2222}$ par 5?

Exercice 2

Quel est le dernier chiffre de l'écriture de $7^{7^{7^7}}$ en base 3, en base 7 et en base 10?

Exercice 3

Vérifier que $400\,000\,000\,000\,000\,000\,081$ est divisible par 13.

Exercice 4

Pour a, b, c entiers impairs, calculer $(a+b+c)^2$ et $a^2+b^2+c^2$ modulo 8, puis $ab+bc+ca$ modulo 4. En supposant de plus que $ab+bc+ca \geq 0$, démontrer que $\sqrt{ab+bc+ca} \notin \mathbf{Q}$.

[*On pourra faire la liste des carrés modulo* 8.]

Exercice 5

En utilisant des congruences modulo un entier bien choisi, montrer que les équations suivantes n'ont pas de solutions entières:

$$i)\, 7x - 4y^3 = 1 \qquad ii)\, x^3 + y^3 + z^3 - 9t = 4 \qquad iii)\, x^2 + xy + 2y^2 = 7003$$

[*Pour iii) compléter le carré modulo* 7.]

Exercice 6

Résoudre dans $\mathbf{Z}$ les équations suivantes:

$$i) 12x + 14 \equiv 0[8], \qquad ii) 12x + 14 \equiv 0[37].$$

Exercice 7

Résoudre dans $\mathbf{Z}$ les équations suivantes:

$$i)\, x^2 \equiv 4[35], \qquad ii) \begin{cases} x \equiv 13[19] \\ x \equiv 6[12] \end{cases} \qquad iii) \begin{cases} x \equiv 3[17] \\ x \equiv 4[11] \\ x \equiv 5[6] \end{cases}$$

Exercice 8 (Extrait du partiel d'automne 2022)

i) Résoudre dans $\mathbf{Z}$

$$\begin{cases} x \equiv 0[4] \\ x \equiv 1[25] \end{cases}$$

ii) En déduire les deux derniers chiffres de $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (2022 fois) en écriture décimale.

Exercice 9

i) Faire la liste des inversibles (multiplicatifs) des anneaux $\mathbf{Z}/5\mathbf{Z}$ et $\mathbf{Z}/8\mathbf{Z}$ et déterminer leurs inverses.

ii) Quel est l'inverse de $\overline{16}$ dans $\mathbf{Z}/37\mathbf{Z}$?

Exercice 10 (Une preuve du petit théorème de Fermat)

Soit p un nombre premier et $a \in \mathbf{Z}$ non multiple de p.

i) Montrer que l'application

$$\psi : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} : \overline{x} \mapsto \overline{a}\,\overline{x}$$

est une bijection.

ii) En considérant le produit $\psi(\overline{1}) \cdots \psi(\overline{p-1})$ montrer que $a^{p-1} \equiv 1[p]$.

Exercice 11 (Le théorème de Wilson)

Soit p un nombre premier.

i) On considère les polynômes suivants à coefficients dans le corps $\mathbf{Z}/p\mathbf{Z}$:

$$P = (X - \overline{p-1})(X - \overline{p-2}) \cdots (X - \overline{2})(X - \overline{1}) \quad \text{et} \quad Q = X^{p-1} - \overline{1}.$$

Montrer que $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ sont racines de Q. En déduire que $P = Q$.

ii) En déduire que $(p-1)! \equiv -1[p]$.

iii) Réciproquement, soit $n \geq 2$ un entier tel que

$$(n-1)! \equiv -1[n].$$

Montrer que n est premier.

Exercice 12 (Diviseurs d'un entier)

On note $d(n)$ le nombre de diviseurs de l'entier $n > 0$. Montrer que

$$\Pi_{d|n} d = n^{\frac{d(n)}{2}}.$$

[*Se servir de la factorisation primaire de* n.]

Exercice 13 (Extrait du partiel d'automne 2022)

i) Faire la liste des nombres premiers $\leq \sqrt{641}$.

ii) Justifier que 641 est un nombre premier.

Exercice 14 (Nombres de Fermat)

1. Soit $k \in \mathbf{N}^\star$.

Montrer que si $2^k + 1$ est un nombre premier, alors il existe $n \in \mathbf{N}$ tel que $k = 2^n$.

[*Ecrire* $k = 2^n(2m+1)$ *et factoriser* $x^{2m+1} + 1$]

On note $F_n = 2^{2^n} + 1, n \in \mathbf{N}$ (les nombres de Fermat).

2. Montrer que pour tout $n, m \in \mathbf{N}$, $m > 0$, F_n divise $F_{m+n} - 2$. En déduire pgcd (F_n, F_{n+m}) [*Penser à Bézout*].

3. Proposer une preuve de l'assertion - *Il existe une infinité de nombres premiers* -

4.
i) Montrer que F_0, F_1, F_2, F_3 sont premiers.
ii) Soit p premier tel que $p \mid F_4$, montrer que $p = 1 \bmod 32$.

[*Commencer par observer ceci: soit* $P = \{l \in \mathbf{N}^\star, 2^l \equiv 1[p]\}$ *et* $n = min(P)$. *Alors,* $l \in P \Leftrightarrow n|l$.]

iii) En déduire que $F_4 = 65537$ est premier.

iv) Montrer que $641 \mid F_5$. F_5 n'est donc pas premier.

Exercice 15

i) Montrer qu'il y a une infinité de nombres premiers de la forme $4k - 1, k \in \mathbf{N}$.
[*Par l'absurde en se servant de l'entier* $n = 4p_1 \cdots p_N - 1$ *où* $p_1, \ldots, p_N$ *sont les nombres premiers congrus à* -1 *modulo* 4.]

ii)
- Soit p un nombre premier impair. On suppose qu'il existe un entier x tel que $x^2 \equiv -1[p]$. Montrer que $p \equiv 1[4]$.

- Montrer qu'il y a une infinité de nombres premiers de la forme $4k + 1, k \in \mathbf{N}$.
[*Par l'absurde en se servant de l'entier* $n = 4(p_1 \cdots p_N)^2 + 1$ *où* $p_1, \ldots, p_N$ *sont les nombres premiers congrus à* 1 *modulo* 4.]