TD12

Arithmétique dans $\mathbb{Z}$

Diviseurs

Exercice 12.1 (★)

Montrer que pour tout $n \in \mathbb{N}$,

1. $17 \mid 2^{6n+3} + 3^{4n+2}$;
2. $7 \mid 3^{2n+1} + 2^{n+2}$;
3. $676 \mid 27^{n+1} - 26n - 27$;
4. $6 \mid n(n+2)(7n-5)$.

Exercice 12.2 (★★)

1. Déterminer les $n \in \mathbb{N}$ pour lesquels $\dfrac{2n^2 - n - 6}{n+3} \in \mathbb{Z}$.
2. Soit $n \in \mathbb{Z}$. Montrer que $\dfrac{21n-3}{4}$ et $\dfrac{15n-2}{4}$ ne sont pas simultanément dans $\mathbb{Z}$.

Exercice 12.3 (★★)

1. Trouver le reste de la division euclidienne de 100^{1000} par 13.
2. Déterminer le dernier chiffre de l'écriture décimale de $7^{3^{11^{17}}}$.

Exercice 12.4 (★★ - Numérotation en base $b \geq 2$ - ✍)

1. Démontrer que tout entier $a \in \mathbb{N}^*$ s'écrit de manière unique sous la forme
$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$$
où $n \in \mathbb{N}$ et $0 \leq a_i \leq b-1$, $a_n \neq 0$. On l'appelle *l'écriture de l'entier a dans la base b.*
2. (a) Trouver la base b dans laquelle on a $14 \times 41 = 1224$.
   (b) Trouver en base 10 les entiers qui s'écrivent simultanément sous les formes suivantes : $\overline{xyz}$ en base 7 et $\overline{zyx}$ en base 11.
3. En notant que $7 \times 11 \times 13 = 1001$, déterminer un critère de divisibilité d'un entier $n = \overline{a_n \cdots a_2 a_1 a_0}$ par $7, 11$ ou 13 faisant intervenir la somme $\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$.

Exercice 12.5 (★★ - Une équation diophantienne)

On s'intéresse à l'équation
$$x^2 + y^2 = 11z^2 \tag{E}$$
d'inconnue $(x, y, z) \in \mathbb{Z}^3$.

1. Donner la liste des carrés *modulo* 11.
2. Soit $(x, y, z) \in \mathbb{Z}^3$ une solution de l'équation (E). Montrer qu'il existe $(x', y', z') \in \mathbb{Z}^3$ tel que $(x, y, z) = 11(x', y', z')$ et $x'^2 + y'^2 = 11z'^2$.
3. Résoudre l'équation (E).

Exercice 12.6 (★★★)

Pour $n \in \mathbb{N}^*$, on note N le nombre de diviseurs positifs de n et P leur produit. Quelle relation existe-t-il entre n, N et P ?

PGCD et PPCM

Exercice 12.7 (★)

Pour chacun des couples (a, b) suivants, déterminer $a \wedge b$, $a \vee b$ et une relation de Bézout.

(i) $(51, 438)$; | (ii) $(720, 1320)$; | (iii) $(151, 77)$.

Exercice 12.8 (★★)

On considère trois entiers naturels n, p, q avec $n \geq 2$ et $q > 0$.

1. Montrer que si r est le reste de la division euclidienne de p par q, alors $n^r - 1$ est le reste de la division euclidienne de $n^p - 1$ par $n^q - 1$.
2. En déduire $(n^p - 1) \wedge (n^q - 1)$ en fonction de n et $p \wedge q$.

Exercice 12.9 (★★)

Chercher les couples d'entiers (a, b) tels que $a \wedge b = 42$ et $a \vee b = 1680$.

Exercice 12.10 (★★)

1. Montrer que pour a, b entiers, $(a + b) \wedge (a \vee b) = a \wedge b$.
2. Résoudre le système $\begin{cases} a + b = 144 \\ a \vee b = 420 \end{cases}$ d'inconnues $(a, b) \in \mathbb{Z}^2$.

Exercice 12.11 (★★)

Soient $(a, b) \in \mathbb{Z}^2$ et soit $n \in \mathbb{N}^*$. Montrer que $(a \wedge b)^n = a^n \wedge b^n$.

Exercice 12.12 (★★)

Montrer que pour $a, b \in \mathbb{N}^*$, $\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{a \wedge b}$.

Exercice 12.13 (★★ - Équations diophantiennes $ax + by = c$ - ✍)

1. On s'intéresse dans cette question à l'équation $18x + 25y = 1$, d'inconnue $(x, y) \in \mathbb{Z}^2$.
   (a) Déterminer une solution particulière (x_0, y_0).
   (b) Montrer que si (x, y) est solution, on a alors $18\,(x - x_0) = 25\,(y_0 - y)$, puis qu'il existe $k \in \mathbb{Z}$ tel que $x = 25k + x_0$.
   (c) En déduire toutes les solutions de l'équation.
2. Résoudre les équations $9x + 15y = 3$, $42x + 45y = 6$ et $12x + 30y = 15$.

Exercice 12.14 (★★ - Banque CCP)

1. Soient $(a, b) \in \mathbb{N}^2$ premiers entre eux, et soit $c \in \mathbb{N}$. Prouver que : $(a \mid c \text{ et } b \mid c) \Leftrightarrow ab \mid c$.
2. On considère le système $(\mathscr{S})$: $\begin{cases} x \equiv 6\,[17] \\ x \equiv 4\,[15] \end{cases}$ d'inconnue $x \in \mathbb{Z}$.
   (a) Déterminer une solution particulière x_0 de $(\mathscr{S})$.
   (b) Déterminer toutes les solutions de $(\mathscr{S})$.

Exercice 12.15 (★★★)
Résoudre dans $\mathbb{Z}$ le système : $\begin{cases} x \equiv 2\,[7] \\ x \equiv 3\,[5] \\ x \equiv 7\,[9] \end{cases}$.
On commencera par établir une relation de Bezout pour 5×9, 7×9, 7×5.

Nombres premiers

Exercice 12.16 (★★ - Nombres de Fermat)

1. Soit $n \in \mathbb{N}^*$. Montrer que si $2^n + 1$ est premier, alors il existe $m \in \mathbb{N}$ tel que $n = 2^m$.
2. On note à présent $F_n = 2^{2^n} + 1$ (qu'on appelle $n^{\text{ème}}$ nombre de Fermat).
   (a) Montrer que pour tout $n \in \mathbb{N}$, $F_{n+1} = F_0 F_1 \cdots F_n + 2$.
   (b) En déduire que pour (m, n) distincts, F_m et F_n sont premiers entre eux.

Exercice 12.17 (★★ - Nombres de Mersenne)

1. Soient un entier $a \geq 2$, et $(m, n) \in \mathbb{N}^2$. Montrer que :
$$n \mid m \Leftrightarrow (a^n - 1) \mid (a^m - 1).$$
On pourra utiliser les résultats de l'Exercice 12.8.
2. Soit $(a, n) \in \mathbb{N}^2$ vérifiant $a \geq 2$ et $n \geq 2$. Montrer que si $a^n - 1$ est premier, alors n est premier et $a = 2$.
Les nombres $M_p = 2^p - 1$ *où* $p \in \mathbb{P}$ *sont appelés nombres de Mersenne. Tous ne sont pas premiers, par exemple* $M_{11} = 23 \times 89$.

Exercice 12.18 (★★ - Infinité de nombres premiers de la forme $4n - 1$)
On suppose qu'il existe un nombre fini N d'entiers premiers de la forme $4n - 1$ où $n \geq 1$. On les note $p_1, \ldots, p_N$, et on forme le nombre $P = 4p_1 \ldots p_N - 1$.
Montrer que P admet nécessairement un diviseur premier de la forme $4n - 1$, et en déduire une contradiction. Conclure.

Exercice 12.19 (★★)
En remarquant que $561 = 3 \times 11 \times 17$, montrer que :
$$\forall n \in \mathbb{Z}, \quad a \wedge 561 = 1 \Rightarrow a^{560} \equiv 1\,[561].$$
Que pensez-vous de la réciproque du petit théorème de Fermat ?

Exercice 12.20 (★★ - Chiffrement RSA)
Soient p et q deux nombres premiers distincts, $n = pq$ et e un entier naturel premier avec $(p-1)(q-1)$.

1. Justifier qu'il existe un entier $d \geq 0$ tel que $ed \equiv 1\,[(p-1)(q-1)]$.
2. Montrer que $x^{ed} \equiv x\,[n]$ pour tout entier x.

Exercice 12.21 (★)
Déterminer les entiers $b \in \mathbb{N}^*$ tels que $\text{ppcm}(28, b) = 140$.

Exercice 12.22 (★)
Soient $a, n \in \mathbb{N}^*$, soit p un nombre premier. Montrer que $p | a^n \Rightarrow p^n | a^n$.

Exercice 12.23 (★★)
Soient $a, b, c, k \in \mathbb{N}^*$ tels que $ab = c^k$ et $\text{pgcd}(a, b) = 1$. Montrer qu'il existe $\alpha, \beta \in \mathbb{N}^*$ tels que $a = \alpha^k$ et $b = \beta^k$.

Exercice 12.24 (★★)
Pour tout $n \in \mathbb{N}^*$, on note $\sigma(n)$ la somme des diviseurs positifs de n.

1. Montrer que si m et n sont premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$.
2. Calculer $\sigma(n)$ pour tout $n \in \mathbb{N}^*$.

Exercice 12.25 (★★)
Trouver $n \in \mathbb{N}^*$ sachant que le produit de ses diviseurs positifs est 45^{42}.

Exercice 12.26 (★★ - Formule de Legendre)
1. Montrer que pour tous $p \in \mathbb{P}$ et $n \in \mathbb{N}$: $\quad v_p(n!) = \displaystyle\sum_{k=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor$.
2. En déduire le nombre de zéros à la fin de $1000000!$.

Exercice 12.27 (★★★ - Théorème de Wilson - ✍)
1. Soit p un nombre premier.
   (a) Montrer que $\forall x \in [\![1, p-1]\!]$, $\exists! y \in [\![1, p-1]\!]$ tel que $xy \equiv 1\,[p]$.
   (b) En déduire que $(p-1)! \equiv -1\,[p]$.
2. Soit $n \in \mathbb{N}^*$, tel que $(n-1)! \equiv -1\,[n]$. Montrer que n est premier.

On a donc prouvé que $p \in \mathbb{N}^*$ est premier si, et seulement si, $(p-1)! \equiv -1\,[p]$.

Exercice 12.28 (★★★★ - Oral ENS)
Montrer qu'il existe un multiple de 2019 dont l'écriture décimale ne comporte que le chiffre 3.
Indication : le nombre premier 673 *divise* 2019.
