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 $\mathbb{Z}$.

> 1. On montre que $2n^2 - n - 6 = (n+3)(2n-7) + 15$. Donc cette fraction est entier si, et seulement si, $n+3 \mid 15$. Les entiers pour lesquels cette fraction est entière sont donc ceux de la forme $n = 15k - 3$.
> 2. S'il existe $p, q \in \mathbb{Z}$ tels que $21n - 3 = 4q$ et $15n - 2 = 4p$, on obtient $1 = 20(q-p)$, ce qui est impossible.

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).

1. Calculons les carrés modulo 11.

$a \mod 11$	0	1	2	3	4	5	6	7	8	9	10
$a^2 \mod 11$	0	1	4	9	5	3	3	5	9	4	1

Ainsi, la liste des carrés *modulo* 11 est

$$\{0, 1, 3, 4, 5, 9\}.$$

2. Soit $(x, y, z) \in \mathbb{Z}^3$. On suppose que

$$x^2 + y^2 = 11z^2.$$

Alors,

$$x^2 + y^2 \equiv 0 \mod 11.$$

Or, on sait d'après la première question que, *modulo* 11, les carrés sont $\{0, 1, 3, 4, 5, 9\}$. Regardons quelles peuvent être les valeurs *modulo* 11 de $x^2 + y^2$:

	0	1	3	4	5	9
0	0	1	3	4	5	9
1	1	2	4	5	6	10
3	3	4	6	7	8	1
4	4	5	7	8	9	2
5	5	6	8	9	10	3
9	9	10	1	2	3	7

Ainsi, comme $x^2 + y^2 \equiv 0 \mod 11$, il suit

$$x^2 \equiv 0 \mod 11 \quad \text{et} \quad y^2 \equiv 0 \mod 11.$$

Donc, d'après la première question,

$$x \equiv 0 \mod 11 \quad \text{et} \quad y \equiv 0 \mod 11.$$

Ainsi, $11 \mid x$ et $11 \mid y$, ce qui donne :

$$11^2 \mid x^2 + y^2$$

puis :

$$11^2 \mid 11z^2$$

soit :

$$11 \mid z^2$$

et finalement :

$$11 \mid z.$$

On conclut qu'on dispose de $(x', y', z') \in \mathbb{Z}^3$ tels que $x = 11x'$, $y = 11y'$ et $z = 11z'$. Mais comme $x^2 + y^2 = 11z^2$, on obtient après simplification par 11^2 :

$$x'^2 + y'^2 = 11z'^2.$$

3. Procédons par analyse-synthèse.

   - **Analyse.** Supposons que l'équation (E) admette au moins une solution (a, b, c) différente de $(0, 0, 0)$. Alors, nécessairement, $c \neq 0$. En effet, dans le cas contraire, comme $a^2 + b^2 = 0$, nous aurions $a = b = 0$ et la solution serait nulle. Soit

   $$\Gamma = \left\{ |z| : \exists (x, y) \in \mathbb{Z}^2 \setminus \{(0, 0\}, x^2 + y^2 = 11z^2 \right\}.$$

   – Γ est une partie de $\mathbb{N}^*$,
   – Γ est non vide car contient $|c|$.

   Ainsi, Γ admet un plus petit élément, nommons-le z_0. On dispose alors de $(x_0, y_0) \in \mathbb{Z}^2$ tel que $x_0^2 + y_0^2 = 11z_0^2$. D'après ce qu'on a montré, dans la question 2, on dispose de $(x_1, y_1, z_1) \in \mathbb{Z}^3$ tel que

   $$(x_0, y_0, z_0) = 11(x_1, y_1, z_1)$$

   et

   $$x_1^2 + y_1^2 = 11z_1^2.$$

   Ainsi, (x_1, y_1, z_1) est une solution et $0 < |z_1| < |z_0|$, ce qui est impossible.
   On conclut que la seule solution possible de l'équation (E) est $(0, 0, 0)$.

   - **Synthèse.** Réciproquement, $(0, 0, 0)$ est bien solution de (E) puisque $0^2 + 0^2 = 11 \cdot 0^2$.

   L'ensemble des solutions de l'équation (E) est donc $\{(0, 0, 0)\}$.

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 ?

On a $P^2 = \left(\prod_{d|n} d \right)^2$. Mais à chaque diviseur d de n correspond un autre diviseur, qui est $\frac{n}{d}$. Plus précisément, notons D_n l'ensemble des diviseurs positifs de n, et soit $\varphi_n : D_n \to D_n$ l'application définie par $\varphi_n(d) = \frac{n}{d}$. Alors $\varphi_n \circ \varphi_n = \mathrm{id}_{D_n}$, et donc φ_n est une bijection de D_n sur lui-même, égale à sa propre bijection réciproque. En particulier :

$$\prod_{d|n} d = \prod_{d|n} \frac{n}{d}$$

et donc :

$$P^2 = \prod_{d|n} d \prod_{d|n} \frac{n}{d} = \prod_{d|n} n = n^N.$$

Puisque P est positif, en passant à la racine, on en déduit que $P = n^{N/2}$.

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 $(a, b) \in \mathbb{Z}^2$.

1. Commençons par le cas où a et b sont premiers entre eux. Puisque $a \vee b = ab$, il s'agit donc de prouver que $(a + b) \wedge (ab) = 1$.

   Or $a + b$ est premier avec a, puisqu'un diviseur commun de $a + b$ et a doit diviser b, et donc doit diviser $a \wedge b = 1$. De même, $a + b$ est premier avec b. Et donc $a + b$ est premier avec ab.

   Alternative. Supposons qu'il existe un nombre premier p divisant $(a + b) \wedge ab$. Alors p divise a ou p divise b (on utilise ici que p est premier). Mais si $p \mid a$ et $p \mid a + b$, alors $p \mid b$, donc $p \mid a \wedge b = 1$.

   Et de même, si $p \mid b$, alors $p \mid a$ et donc $p \mid 1$.

   Or aucun nombre premier ne divise 1, donc $(a + b) \wedge (ab)$ n'a pas de diviseur premier, ce qui n'est possible que si il est égal à 1 .

   Dans le cas général, notons $d = a \wedge b$, et soient a', b' premiers entre eux tels que $a = da'$ et $b = db'$. Alors :

$$\begin{aligned}(a + b) \wedge (a \vee b) &= \left[d\left(a' + b\right)'\right] \wedge \left[(da') \vee (db')\right] = d\left[(a' + b') \wedge (a' \vee b')\right] \\ &= d \times 1 = d = a \wedge b.\end{aligned}$$

2. Nommons $(\mathscr{S})$ le système de l'énoncé.

   Si (a, b) est une solution de $(\mathscr{S})$, alors $a \wedge b = (a + b) \wedge (a \vee b) = 144 \wedge 420 = 12$. Donc il existe a' et b' premiers entre eux tels que $a = 12a'$ et $b = 12b'$. Et alors (a, b) est solution du système $(\mathscr{S})$ si, et seulement si, il existe deux entiers a', b' premiers entre eux tels que :

$$(a,b) = (12a', 12b'), \text{ avec } (a,b') \text{ solution de } \begin{cases} a'+b' = 12 \\ a'b' = 35 \end{cases} \quad (\mathscr{S}').$$

Ce système se résout de manière classique : les solutions sont les couples (x,y) tels que $\{x,y\}$ est l'ensemble des racines de $X^2 - 12X + 35$. Le discriminant de ce polynôme vaut $\Delta = 144 - 4\times 35 = 4$. Donc les deux racines en sont $\frac{12+\sqrt{4}}{2} = 7$ et $\frac{12-\sqrt{4}}{2} = 5$.

Ainsi, les couples de réels (a',b') solutions du système $(\mathscr{S}')$ sont $(5,7)$ et $(7,5)$. Et donc les solutions au système $(\mathscr{S})$ de départ sont $(12\times 5, 12\times 7) = (60,84)$ et $(84,60)$.

Alternative. On peut également remarquer que $35 = 5\times 7 = 35\times 1$ sont les seules décompositions de 35 en produit de deux entiers, et que seule la première décomposition conduit à une somme égale à 12.

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.

1. Il s'agit de prouver que le seul facteur premier de n est 2.

   Écrivons $n = 2^m q$ avec q impair. Une telle écriture est toujours possible : puisque si $m = v_2(n)$, alors $n = 2^{v_2(n)} q$, avec $q \wedge 2 = 1$, c'est-à-dire q impair. Alors $2^n = (2^{2^m})^q$, et donc

   $$2^n + 1 = \left(2^{2^m}\right)^q - (-1)^q = \left(2^{2^m} + 1\right) \left(\sum_{k=0}^{q-1} 2^{2^m k} (-1)^{q-1-k} \right)$$

   Nous avons alors là une factorisation de $2^n + 1$, qui est premier. Donc $2^{2^m} + 1 = 1$ ou $2^{2^m} + 1 = 2^n + 1$. Le premier cas est clairement impossible, donc $2^{2m} + 1 = 2^n + 1$, donc $n = 2^m$.

2. (a) Prouvons le résultat par récurrence sur n.

   Init. On a $F_1 = 2^2 + 1 = 5 = 3 + 2 = \left(2^{2^0} + 1\right) + 2 = F_0 + 2$. Donc la récurrence est bien initialisée.

   Hér. Soit $n \in \mathbb{N}$. Supposons que $F_{n+1} = F_0 F_1 \cdots F_n + 2$. Alors $F_{n+2} = 2^{2^{n+2}} + 1$, et donc

   $$F_{n+2} - 1 = 2^{2^{n+2}} = 2^{2^{n+1} \times 2} = \left(2^{2^{n+1}}\right)^2 = (F_{n+1} - 1)^2 = F_{n+1}^2 - 2F_{n+1} + 1$$

   Soit encore $F_{n+2} = F_{n+1}^2 - 2F_{n+1} + 2 = F_{n+1}(F_{n+1} - 2) + 2$. Mais par hypothèse de récurrence, $F_{n+1} = F_0 F_1 \cdots F_n + 2$, et donc

   $$F_{n+2} = F_{n+1}(F_0 F_1 \cdots F_n + 2 - 2) + 2 = F_0 \cdots F_{n+1} + 2.$$

   Donc par le principe de récurrence, pour tout $n \in \mathbb{N}$, $F_{n+1} = F_0 \cdots F_n + 2$.

   (b) Supposons que $m < n$. Alors $F_n = F_0 \cdots F_m \cdots F_{n-1} + 2$. Si d est un diviseur positif commun à F_n et F_m, c'est donc un diviseur de $2 = F_n - F_m (F_0 \cdots F_{m-1} F_{m+1} \cdots F_{n-1})$. Donc $d = 1$ ou $d = 2$. Or, F_n et F_m sont impairs, donc ne peuvent avoir 2 comme diviseur. On en déduit que 1 est l'unique diviseur commun à F_n et à F_m, de sorte que F_n et F_m sont premiers entre eux.

   Remarque. On peut retrouver de cette manière qu'il existe une infinité de nombres premiers. En effet, pour tout $n \in \mathbb{N}$, il existe au moins un diviseur premier p_n de F_n. Et ces nombres premiers sont tous distincts puisque les entiers F_n sont premiers entre eux deux à deux. On a donc de cette manière exhiber une infinité de nombres premiers.

Le saviez-vous ?

Les premiers nombres de Fermat sont $F_0 = 2^{2^0} + 1 = 3, F_1 = 5$, $F_2 = 17, F_3 = 257$ et $F_4 = 65537$. Ces nombres sont tous premiers. On a alors $F_5 = 4294967\,297$, dont il est difficile de savoir sans ordinateur s'il est ou non premier... Fermat a conjecturé que les F_n étaient tous premiers. Il a fallu attendre Euler pour savoir que $641 \mid F_5$, qui n'est donc pas premier.

À l'heure actuelle, on ne connaît pas d'autres nombres de Fermat premiers autres que F_0, F_1, F_2, F_3, F_4. Et on ne sait pas s'il en existe d'autres ou non. Des travaux de Boklan et Conway de mai 2016 estiment cependant la probabilité d'un autre nombre premier à moins d'un sur un milliard.

Ces nombres premiers apparaissent dans un résultat surprenant du à Wantzel : on peut construire un polygone régulier à n côtés uniquement à l'aide d'un compas et d'une règle non graduée si et seulement si n est de la forme une puissance de 2 fois un produit de nombres premiers de Fermat distincts. Par exemple on peut tracer à la règle et au compas un polygone à $6, 15 \text{ou} 68 = 2^2 \times 17$ côtés, mais pas un polygone à $25 = 5^2$ ou à 11 côtés.

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 $M_{11} = 23 \times 89$.

1. Supposons $n \mid m$. On dispose alors de $k \in \mathbb{N}$ tel que $m = kn$. Il vient :
$$\begin{aligned} a^m - 1 &= a^{kn} - 1 \\ &= (a^n)^k - 1^k \\ &= (a^n - 1) \sum_{p=0}^{k-1} (a^n)^p \\ &= (a^n - 1) \sum_{p=0}^{k-1} a^{np}, \end{aligned}$$
ce qui prouve que $(a^n - 1) \mid (a^m - 1)$.

   Supposons réciproquement que $(a^n - 1) \mid (a^m - 1)$. Effectuons la division euclidienne de m par n : cela nous fourni un couple $(q, r) \in \mathbb{N}^2$ tel que $m = qn + r$ et $r < n$. Écrivons alors :
$$\begin{aligned} a^m - 1 &= a^{qn+r} - 1 \\ &= a^{qn+r} - a^r + a^r - 1 \\ &= a^r(a^{qn} - 1) + a^r - 1 \end{aligned}$$
   Par hypothèse, $(a^n - 1) \mid (a^m - 1)$ et, comme on l'a vu dans la démonstration du sens direct, $(a^n - 1) \mid (a^{qn} - 1)$. Il suit que $(a^n - 1) \mid (a^r - 1)$.

   Mais, comme $r < n$ et $a > 1$, on a aussi $a^r - 1 < a^n - 1$. On en déduit que $a^r - 1 = 0$, c'est-à-dire $r = 0$. Ainsi, $n \mid m$.

2. La factorisation classique donne
$$a^n - 1 = a^n - 1^n = (a - 1)\left(a^{n-1} + a^{n-2} + \cdots + 1\right).$$
   Supposons $a > 2$ Alors $a - 1 \geq 2$. De plus, puisque $n \geq 2$, le deuxième facteur, qui comporte n termes tous entiers naturels non nuls, est plus grand que 2. Il existe donc dans

ce cas une factorisation de $a^n - 1$ en deux entiers strictement plus grand que 1. On en conclut que, si $a^n - 1$ est premier, alors $a = 2$.

Supposons maintenant $2^n - 1$ premier. Soit d un diviseur de n. On dispose alors d'un $p \in \mathbb{N}^*$ tel que $n = d\,p$, et

$$2^{pd} - 1 = (2^d)^p - 1 = (2^d - 1)\,(1 + 2^d + 2^{2d} + \cdots + 2^{(p-1)d}).$$

$2^d - 1$ divise $2^n - 1$. D'où, puisque ce dernier nombre est premier, $2^d - 1 = 1$ ou $2^n - 1$, et donc $d = 1$ ou $d = n$. Ainsi, puisque par ailleurs $n \geq 2$, n est premier.

Le saviez-vous ?

Les nombres $M_p = 2^p - 1$ avec p premiers sont appelés nombres de Mersenne, du nom du mathématicien français du XVII^e siècle Marin Mersenne.
Mersenne avait montré que M_p est premier pour $p = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 127$, oubliant au passage $p = 61, 89, 109$. Et que $M_{11} = 2047 = 23 \times 87$ ne l'était pas. La réciproque du résultat démontré dans cette question est donc fausse.
Il existe un test de primalité efficace pour les nombres de Mersenne, le test de primalité de Lucas-Lehmer. De ce fait, les plus grands nombres premiers connus sont des nombres de Mersenne (le plus grand étant $M_{82589933}$). Les nombres de Mersenne premiers sont pourtant rares : seulement 51 sont connus début 2022.
On ne sait pas s'il existe une infinité de nombres de Mersenne premiers. On ne sait pas davantage s'il existe une infinité de nombres de Mersenne non premiers.

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.

Le nombre $A = 4p_1 \ldots p_N - 1$ est impair. Ainsi ses diviseurs premiers sont de la forme $4n-1$ ou $4n+1$. Supposons que ce nombre n'admet aucun diviseur premier de la forme $4n-1$, alors tous ces diviseurs premiers sont de la forme $4n+1$. Mais alors il serait lui même de la forme $4n+1$ (en remarquant que $(4p+1)(4q+1) = 4(4pq+p+q)+1$). Or ceci est impossible, puisqu'alors

$$4p_1 \ldots p_N - 1 = 4n + 1 \quad \Leftrightarrow \quad 4(p_1 \ldots p_N - n) = 2$$

et 4 diviserait 2.
Donc A a au moins un diviseur premier de la forme $4n-1$, par exemple p_1. Or ceci est impossible également car sinon p_1 diviserait $4p_1 \ldots p_N - A = 1$.
Ainsi l'hypothèse de départ était absurde, et on a bien démontré l'existence d'une infinité de nombres premiers de la forme $4n - 1$.

Remarque. On peut montrer qu'il y a également une infinité de nombres premiers de la forme $4n - 1$, mais la preuve est plus difficile.

Exercice 12.19 (★★)

En remarquant que $561 = 3 \times 11 \times 17$, montrer que :

$$\forall a \in \mathbb{Z}, \quad a \wedge 561 = 1 \Rightarrow a^{560} \equiv 1\,[561].$$

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.

1. Puisque e est premier avec $(p-1)(q-1)$, il existe $u, v \in \mathbb{Z}$ tels que :
$$eu + (p-1)(q-1)v = 1.$$
D'où en prenant la congruence modulo $(p-1)(q-1)$, $eu \equiv 1\,[(p-1)(q-1)]$. Et si on note d le reste de la division euclidienne de u par $(p-1)(q-1)$, alors $d \geq 0$ et :
$$ed \equiv 1\,[(p-1)(q-1)].$$
2. Soit $x \in \mathbb{Z}$. Si x est divisible par p ou par q, le résultat est évident. Supposons dans la suite que p et q ne divisent pas x.
Puisque $ed \equiv 1\,[(p-1)(q-1)]$, il existe $k \in \mathbb{N}$ tel que $ed = 1 + k(p-1)(q-1)$ (car e et d sont positifs). Par le petit théorème de Fermat :
$$x^{p-1} \equiv 1\,[p], \quad \text{et donc} \quad x^{ed} \equiv x^{1+k(p-1)(q-1)} \equiv x \times \left(x^{p-1}\right)^{k(q-1)} \equiv x \times 1\,[p].$$
De même, $x^{ed} \equiv x\,[q]$. Ainsi p et q divisent $x^{ed} - x$, et puisqu'ils sont premiers entre eux (ce sont des nombres premiers distincts), $p \times q$ divise $x^{ed} - x$. Ce qui se récrit $x^{ed} \equiv x[n]$.

Le saviez-vous ?
Voici le principe du chiffrement RSA. Bob veut envoyer un message confidentiel $M \in \mathbb{N}$ à Alice. Pour cela :

1. Alice choisit deux nombres premiers p et q de grande taille. Elle note $n = pq > M$ le produit de ces deux nombres.
2. Alice choisit ensuite un autre entier e tel que e et $(p-1)(q-1)$ soient premiers entre eux. Alors on sait (par la formule de Bezout) qu'il existe un entier $d \in \mathbb{N}$ tel que $ed \equiv 1[(p-1)(q-1)]$.
3. Alice rend publique la clef (e, n), dont Bob aura besoin pour coder le message, et elle garde secret le nombre d qui est nécessaire au décryptage (les autres entiers ne servent plus).
4. Bob code son message M en $T \equiv M^e[n]$, qu'il transmet à Alice.
5. Alice, qui a reçu le message codé T, peut retrouver M par la formule $M \equiv T^d[n]$.

Supposons que Carl souhaite déchiffrer le message T sans avoir la clef de déchiffrage d (seulement en possession d'Alice). Il dispose pour cela de T, n, e. Pour obtenir d, Carl a besoin de $p-1$ et $q-1$, ou encore p et q. Il doit donc factoriser n.

Et c'est sur ce point que réside la sûreté du code RSA, sur la fonction à sens unique $f : (p, q) \in \mathbb{P} \times \mathbb{P} \mapsto p \cdot q \in \mathbb{N}$. On a en effet des algorithmes performants pour calculer $p \cdot q$ même pour des grands nombres. Mais pour $n \in \mathbb{N}$ produit de deux grands nombres premiers p et q, on ne sait pas déterminer p et q facilement (c'est-à-dire en un temps raisonnable). La méthode du crible d'Eratosthène va demander un temps exponentiel et est donc inapplicable. D'autres techniques plus

efficaces existent, mais elles ont une complexité exponentielle ou sous-exponentielle au mieux, et restent donc très lentes.

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 N le nombre de diviseurs positifs de n et $\sigma(n)$ leur somme.

1. Déterminer N.
2. Montrer que si m et n sont premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$.
3. 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!.

1. Par propriété de la valuation p-adique :

$$v_p(n!) = v_p\left(\prod_{k=1}^{n} k\right) = \sum_{k=1}^{n} v_p(k).$$

En écrivant ensuite, pour tout $k \in [\![1, n]\!]$, $v_p(k) = \displaystyle\sum_{j=1}^{v_p(k)} 1$, la somme devient :

$$v_p(n!) = \sum_{k=1}^{n} \left(\sum_{j=1}^{v_p(k)} 1 \right),$$

où il y a autant de termes que de facteurs p dans $n!$.

L'idée est à présent d'intervertir les symboles de sommation, comme dans une somme triangulaire. On peut sommer dans les deux ordres suivants :

- soit comme dans cette dernière somme, en regardant, pour chaque $k \leq n$, combien de fois k est divisible par p ;

- soit en regardant, pour chaque $\ell \geq 1$, combien de fois p^ℓ divise au moins une fois chacun des entiers $k \leq n$.
  Remarquons que, pour ℓ suffisamment grand (strictement plus grand que $\lfloor \log_p(n) \rfloor$), $p^\ell > n$ et il ne divisera donc aucun entier inférieur à n. Ainsi, $v_p(k) \leq \lfloor \log_p(n) \rfloor$ pour tout $k \in [\![1, n]\!]$.

Poursuivons notre calcul :

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{n} \left(\sum_{\ell=1}^{v_p(k)} 1 \right) = \sum_{\substack{(k,\ell) \in [\![1,n]\!] \times \mathbb{N}^* \\ 1 \leq \ell \leq v_p(k)}} 1 \\ &= \sum_{\ell=1}^{\lfloor \log_p(n) \rfloor} \left(\sum_{\substack{1 \leq k \leq n \\ v_p(k) \geq \ell}} 1 \right). \end{aligned}$$

Soit ℓ un entier vérifiant $1 \leq \ell \leq \lfloor \log_p(n) \rfloor$. Alors, la somme $\displaystyle\sum_{\substack{1 \leq k \leq n \\ v_p(k) \geq \ell}} 1$ est égale au nombre d'entiers de $[\![1, n]\!]$ divisibles au moins ℓ fois par p, c'est-à-dire le nombre de multiples de p^ℓ dans $[\![1, n]\!]$, à savoir $\left\lfloor \frac{n}{p^\ell} \right\rfloor$.

Substituons dans la somme.

$$\sum_{\substack{1 \leq k \leq n \\ v_p(k) \geq \ell}} 1 = \left\lfloor \frac{n}{p^\ell} \right\rfloor.$$

On en déduit :

$$v_p(n!) = \sum_{k=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Remarque. Cette dernière expression se récrit :

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

étant bien entendu qu'il s'agit d'une somme finie, les termes devenant nuls à partir d'un certain rang.

2. Le nombre de zéros à la fin d'un nombre $N \in \mathbb{N}^*$ vaut $v_{10}(N) = \max\{k \in \mathbb{N}^* : 10^k \text{ divise } n\}$.

Mise en garde.

Il faut se garder d'utiliser directement la formule obtenue à la question précédente. En effet, elle utilise l'égalité :

$$v_p(ab) = v_p(a) + v_p(b)$$

qui n'est valable que pour p premier, fausse sinon (prendre par exemple $p = 6$, $a = 3$ et $b = 2$).

On s'en sort ici en remarquant que $v_{10}(N) = \max(v_2(N), v_5(N))$. Pour notre nombre $N = (10^6)!$, il est intuitivement clair que $v_2(N) \geq v_5(N)$. On peut le montrer en utilisant la formule qu'on vient de démontrer, et la croissance de la partie entière :

$$v_5((10^6)!) = \sum_{k=1}^{\lfloor \log_5(10^6) \rfloor} \left\lfloor \frac{10^6}{5^k} \right\rfloor \leq \sum_{k=1}^{\lfloor \log_5(10^6) \rfloor} \left\lfloor \frac{10^6}{2^k} \right\rfloor \leq \sum_{k=1}^{\lfloor \log_2(10^6) \rfloor} \left\lfloor \frac{10^6}{2^k} \right\rfloor = v_2((10^6)!).$$

Ainsi, $v_{10}(N) = v_5(N)$ qu'il nous reste à calculer avec la formule obtenue à la question précédente.

Posons $n = 10^6$. On cherche $v_{10}(n!) = v_5(n!)$. Pour cela, calculons les $v_k = \left\lfloor \frac{n}{5^k} \right\rfloor$ pour tout $k \in \mathbb{N}$. Il vient $v_1 = 200\,000$, $v_2 = 40\,000$, $v_3 = 8\,000$, $v_4 = 1\,600$, $v_5 = 320$, $v_6 = 64$, $v_7 = \left\lfloor \frac{64}{5} \right\rfloor = 12$, $v_8 = \left\lfloor \frac{64}{25} \right\rfloor = 2$ et, pour tout $k \geq 9$, $v_k = \left\lfloor \frac{10^6}{5^k} \right\rfloor = \left\lfloor \frac{64}{5^{k-6}} \right\rfloor = 0$.

Le nombre de zéros cherché est donc

$$200\,000 + 40\,000 + 8\,000 + 1\,600 + 320 + 64 + 12 + 2 = 249\,998.$$

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, $(p-1)! \equiv -1\,[p]$.

1. (a) Soit $x \in [\![1, p-1]\!]$. Puisque p est premier et ne divise pas x, x et p sont premiers entre eux. Et donc par le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tels que $xu + pv = 1$.

   Remarquons que u ne peut être divisible par p, faute de quoi 1 serait lui aussi divisible par p, ce qui est absurde. Notons alors $u = ap + b$ la division euclidienne de u par p, de sorte que $1 \leq b \leq p-1$. Il vient donc $xu + pv = xb + p(ax + v) = 1$ et par conséquent $xu \equiv 1\,[p]$. Ceci prouve donc l'existence demandée.

   Passons à l'unicité, et supposons qu'il existe deux entiers y_1 et y_2 dans $[\![1, p-1]\!]$ tels que $xy_1 \equiv xy_2\,[p]$. Alors $x(y_1 - y_2) \equiv 0\,[p]$ et donc est divisible par p. Puisque x est premier avec p, par le lemme de Gauss, on a donc $p \mid (y_1 - y_2)$. Or, $-(p-2) \leq y_1 - y_2 \leq p-2$, et le seul nombre divisible par p dans $[\![-(p-2), (p-2)]\!]$ est 0 . Donc $y_1 = y_2$.

   Nous avons donc prouvé qu'il existe un unique $y \in [\![1, p-1]\!]$ tel que $xy \equiv 1\,[p]$.

   (b) Rappelons que $(p-1)! = \prod_{k=1}^{p-1} k$. L'idée est de regrouper chacun des termes k de ce produit avec son inverse modulo p, c'est-à-dire avec l'unique élément y de $[\![1, p-1]\!]$ tel que $ky \equiv 1\,[p]$.

   Toutefois, ce regroupement ne sera pas possible lorsque k est égal à son inverse modulo p. En effet, chacun des éléments de $[\![1, p-1]\!]$ n'apparaît qu'une seule fois dans $(p-1)!$. Autrement dit, les termes qu'on ne pourra simplifier avec leur inverse sont les k tels que $k^2 \equiv 1\,[p]$. Mais

   $$k^2 \equiv 1\,[p] \Leftrightarrow k^2 - 1 \equiv 0\,[p] \Leftrightarrow p \mid k^2 - 1.$$

Puisque $k^2-1=(k+1)(k-1)$, alors p divise k^2-1 si, et seulement si, $p \mid k-1$ ou $p \mid k+1$. Pour $k \in [\![1, p-1]\!]$, ceci n'est possible que dans deux cas : $k=1$ et $k=p-1$.

Ainsi, après avoir regroupé les termes deux à deux lorsque c'était possible, il vient :

$$(p-1)! \equiv 1 \times (p-1) \equiv p-1 \equiv -1\,[p].$$

2. Supposons que $(n-1)! \equiv -1\,[n]$. Alors il existe $k \in \mathbb{Z}$ tel que $(n-1)! = -1+kn \Leftrightarrow kn-(n-1)!=1$. Par le théorème de Bézout, n et $(n-1)$! sont premiers entre eux. En particulier, aucun des entiers de $[\![2, n-1]\!]$, qui sont des diviseurs de $(n-1)!$, ne divise n. Et donc les seuls diviseurs positifs de n sont 1 et n : n est premier.

   Remarque. On obtient ici un nouveau test de primalité : n est premier si, et seulement si, $(n-1)! \equiv -1\,[n]$. Il n'est cependant pas utilisable en pratique, le calcul de $(n-1)!\,[n]$ le rendant inefficient.

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.

Notons qu'un nombre N a une écriture décimale ne comportant que des 3 si, et seulement si, il existe $n \in \mathbb{N}$ tel que

$$N = \sum_{k=0}^{n} 3 \times 10^k = 3 \sum_{k=0}^{n} 10^k = 3\frac{10^{n+1}-1}{10-1} = \frac{10^{n+1}-1}{3}.$$

On a $2019 = 3 \times 673$, qui est donc la décomposition de 2019 en produit de facteurs premiers. Par le petit théorème de Fermat, $10^{672} \equiv 1\ [673]$, de sorte que 673 divise $10^{672}-1$. Mais 9 est premier avec 673, et donc par le lemme de Gauss, puisque 673 divise $10^{672}-1 = 9\frac{10^{672}-1}{9}$, 673 divise $\frac{10^{672}-1}{9}$. Et donc $\frac{10^{672}-1}{9}$ est un multiple de 673. En multipliant par 3, $\frac{10^{672}-1}{3}$ est un multiple de 2019, dont tous les chiffres de l'écriture décimale valent 3.

Remarque. Notons que nous n'avons pas nécessairement trouvé le plus petit multiple de 2019 dont l'écriture ne contient que des 3 . De fait, une recherche avec `Python` prouve que $\frac{10^{224}-1}{3}$ est déjà un multiple de 2019. Ceci vient du fait que le petit théorème de Fermat, s'il nous garantit que $a^{p-1} \equiv 1\,[p]$, ne nous dit pas que $p-1$ soit le plus petit entier k tel que $a^k \equiv 1\,[p]$. De fait, ici, $10^{224} \equiv 1\,[673]$.
