

# ARITHMÉTIQUE

(corrigés)

## Exercice 1

1. C'est vrai :

$$\mathcal{D}(45) = \{-45, -30, -15, -9, -3, -1, 1, 3, 9, 15, 30, 45\}$$

2. C'est faux : par exemple  $18 \equiv 1 [17]$  alors que 18 est pair.

3. C'est faux. On a  $2 \mid 2$  mais  $2 \times 2$  ne divise pas 2.

**Remarque :** dans la propriété du cours,  $a$  et  $b$  sont premiers entre eux.

4. C'est faux. Par exemple, 8 divise  $4 \times 2$  mais 8 ne divise ni 4 ni 2.

5. C'est faux.

En effet, un entier  $n \in \mathbb{Z}$  est divisible par 7 si et seulement s'il existe  $k \in \mathbb{Z}$  tel que  $n = 7k$ . Il s'agit de compter les entiers naturels  $k$  tels que  $1 \leq 7k \leq 1000$ . Or :

$$\forall k \in \mathbb{N}, \quad 1 \leq 7k \leq 1000 \iff \frac{1}{7} \leq k \leq \frac{1000}{7} \iff 1 \leq k \leq \left\lfloor \frac{1000}{7} \right\rfloor$$

Or  $\left\lfloor \frac{1000}{7} \right\rfloor = 142$ . Il y a donc 142 multiples de 7 dans l'intervalle  $\llbracket 1, 1000 \rrbracket$ .

6. C'est faux. Par exemple, 16 divise  $4^2$  mais 16 ne divise pas 4.

7. C'est faux. Par exemple  $4^2 \equiv 1 [15]$  mais 15 ne divise ni 3 ni 5.

8. C'est vrai. En effet, si  $4a \equiv 4b [21]$ , alors 21 divise  $4(a-b)$ . Or 21 et 4 sont premiers entre eux donc (d'après le lemme de Gauss) 21 divise  $a-b$ . Autrement dit,  $a \equiv b [21]$ .

## Exercice 2

1. On propose deux méthodes.

### ★ Première méthode :

Soit  $n \in \mathbb{N}$ . On a :

$$3^{2n} - 1 = 9^n - 1^n = (9 - 1) \sum_{k=0}^{n-1} 9^k = 8 \times \underbrace{\sum_{k=0}^{n-1} 9^k}_{\in \mathbb{N}}$$

donc 8 divise  $3^{2n} - 1$ .

### ★ Deuxième méthode :

On a  $9 \equiv 1 [8]$  donc  $3^{2n} = 9^n \equiv 1^n \equiv 1 [8]$ . Donc  $3^{2n} - 1 \equiv 0 [8]$ . Autrement dit, 8 divise  $3^{2n} - 1$ .

Finalement :

pour tout entier naturel  $n$ , l'entier  $3^{2n} - 1$  est divisible par 8

2. On a  $4^2 \equiv 1 [15]$  donc :

$$4^{1001} = (4^2)^{500} \times 4 \equiv 4 [15]$$

donc  $4^{1001} + 11 \equiv 4 + 11 \equiv 0 [15]$ . Ainsi :

$$15 \mid 4^{1001} + 11$$

3. On a  $2^5 = 32 \equiv -1 [11]$ . Or  $123 = 60 \times 5 + 3$  donc :

$$2^{123} = 2^{24 \times 5 + 3} = (2^5)^{60} \times 8 \equiv (-1)^{24} \times 8 \equiv 8 [11]$$

On a  $3^2 \equiv -2 [11]$  donc :

$$3^{121} = 3^{2 \times 60 + 1} = (3^2)^{60} \times 3 \equiv (-2)^{60} \times 3 \equiv 3 \times 2^{60} [11]$$

Or :

$$2^{60} = (2^5)^{12} \equiv 1^{12} \equiv 1 [11]$$

Ainsi,  $3^{121} \equiv 3 [11]$  puis  $2^{123} + 3^{121} \equiv 8 + 3 \equiv 0 [11]$ . Finalement :

$$11 \mid 2^{123} + 3^{121}$$

4. On a  $3^3 = 27 \equiv 1 [13]$  et  $5^2 = 25 \equiv -1 [16]$  donc :

$$3^{126} = 3^{42 \times 3} = (3^3)^{42} \equiv 1 [13]$$

et :

$$5^{126} = (5^2)^{63} \equiv (-1)^{63} \equiv -1 [13]$$

Ainsi :

$$3^{126} + 5^{126} \equiv 0 [13]$$

Autrement dit :

$3^{126} + 5^{126}$  est un multiple de 13

5. (a) Comme 5 est un nombre premier qui ne divise pas 1357, on a  $1357^4 \equiv 1 [5]$  (d'après le petit théorème de Fermat). Ainsi :

$$1357^{2013} = 1357^{4 \times 503 + 1} = (1357^4)^{503} \times 1357 \equiv 1357 \equiv 2 [5]$$

Donc :

le reste de la division euclidienne de  $1357^{2013}$  par 5 est 2

- (b) On a  $3^3 = 27 \equiv 2 [25]$  donc  $(3^3)^7 \equiv 2^7 \equiv 3 [25]$  car  $2^7 = 128$ . Ainsi,  $3^{21} \equiv 3 [25]$ . Donc 25 divise  $3^{21} - 3 = 3(3^{20} - 1)$ . Or  $3 \wedge 25 = 1$  donc 25 divise  $3^{20} - 1$ . Autrement dit,  $3^{20} \equiv 1 [25]$ . Donc :

$$3^{1289} = 3^{19 \times 20 + 9} = (3^{20})^{19} \times 3^9 \equiv 3^9 [25] \\ \equiv 2^3 [25]$$

Ainsi :

le reste de la division euclidienne de  $3^{1289}$  par 25 est 8

- (c) Comme 13 est un nombre premier ne divisant pas 49, on sait d'après le petit théorème de Fermat que  $49^{12} \equiv 1 [13]$ . On a alors :

$$49^{90021} = 49^{12 \times 7501 + 9} = (49^{12})^{7501} \times 49^9 \equiv 49^9 [13]$$

Or  $49 \equiv -3 [13]$  donc  $49^9 \equiv -3^9 [13]$  et  $3^3 = 27 \equiv 1 [13]$  donc  $3^9 \equiv 1 [13]$ . Finalement :

$$49^{90021} \equiv -1 \equiv 12 [13]$$

Ainsi :

le reste de la division euclidienne de  $49^{90021}$  par 13 est 12

### Exercice 3

Soit  $n \in \mathbb{N}$ . On remarque que :

$$3(14n + 3) + (-2)(21n + 4) = 1$$

D'après le théorème de Bézout, les entiers  $14n + 3$  et  $21n + 4$  sont premiers entre eux. Autrement dit :

la fraction  $f = \frac{21n + 4}{14n + 3}$  est irréductible

### Exercice 4

On raisonne par analyse-synthèse.

★ **Analyse** : supposons que l'équation proposée admette une solution rationnelle  $x \in \mathbb{Q}$ . Il existe alors  $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$  tel que  $x = \frac{p}{q}$  et tel que  $p \wedge q = 1$  (on peut supposer que la fraction est sous forme irréductible). Par hypothèse sur  $x$ , on a :

$$x^3 + x^2 + 2x + 1 = 0 \quad i.e. \quad \frac{p^3}{q^3} + \frac{p^2}{q^2} + \frac{2p}{q} + 1 = 0$$

En multipliant par  $q^3$ , on obtient :

$$p^3 + p^2q + 2pq^2 + q^3 = 0$$

- On a  $p(p^2 + pq + 2q^2) = -q^3$  donc  $p \mid q^3$ . Or  $p \wedge q = 1$  donc  $p = \pm 1$ .
- De même, on a  $q(q^2 + 2pq + p^2) = -p^3$  donc  $q \mid p^3$ . Comme  $q \geq 1$  et  $p \wedge q = 1$ , on a nécessairement  $q = 1$ .

On vient de montrer que si  $x$  est une solution rationnelle de l'équation, alors nécessairement  $x = -1$  ou  $x = 1$ .

★ **Synthèse** : on constate que ni  $-1$  ni  $1$  n'est solution de l'équation.

Finalement :

l'équation n'admet pas de solution rationnelle

### Exercice 5

1. Soit  $n \in \mathbb{Z}$ . On a  $7n - 5 \equiv n + 1 [6]$  donc :

$$n(n + 2)(7n - 5) \equiv n(n + 1)(n + 2) [6]$$

Ainsi,  $6 \mid n(n + 2)(7n - 5)$  si et seulement si  $6 \mid n(n + 1)(n + 2)$ . Or  $n, n + 1$  et  $n + 2$  sont trois entiers consécutifs donc l'un d'entre eux est un multiple de 3. De plus, l'un de ces entiers est nécessairement pair. Comme  $2 \wedge 3 = 1$ , on a  $6 \mid n(n + 1)(n + 2)$ . Finalement :

$$\forall n \in \mathbb{Z}, \quad 6 \mid n(n + 2)(7n - 5)$$

2. On raisonne par analyse-synthèse.

★ **Analyse** : soit  $n \in \mathbb{Z}$ . On suppose que  $n + 1 \mid n + 7$ . Comme  $n + 1 \mid n + 1$ , on a aussi  $n + 1 \mid (n + 7) - (n + 1)$  i.e.  $n + 1 \mid 6$ . On en déduit que :

$$n + 1 \in \{-6, -3, -2, -1, 1, 2, 3, 6\} \quad i.e. \quad n \in \{-7, -4, -3, -2, 0, 1, 2, 5\}$$

★ **Synthèse** : pour chaque entier  $n \in \{-7, -4, -3, -2, 0, 1, 2, 5\}$ , on vérifie que  $n + 1 \mid n + 7$ .

Finalement :

l'ensemble des entiers  $n \in \mathbb{Z}$  tels que  $n + 1 \mid n + 7$  est  $\{-7, -4, -3, -2, 0, 1, 2, 5\}$

3. Soit  $n \in \mathbb{Z}$ . On a :

$$n^2 + (n+1)^2 + (n+3)^2 = 3n^2 + 8n + 10 \equiv 3n^2 + 8n [10]$$

Ainsi :

$$\begin{aligned} 10 \mid n^2 + (n+1)^2 + (n+3)^2 &\iff 10 \mid 3n^2 + 8n \\ &\iff 2 \mid 3n^2 + 8n \text{ et } 5 \mid 3n^2 + 8n \end{aligned}$$

car 2 et 5 sont premiers entre eux. Or  $8n$  est pair donc :

$$\begin{aligned} 2 \mid 3n^2 + 8n &\iff 2 \mid 3n^2 \iff 2 \mid n^2 \quad (\text{car } 2 \wedge 3 = 1, \text{ lemme de Gauss}) \\ &\iff 2 \mid n \quad (\text{car } 2 \in \mathcal{P}) \end{aligned}$$

Par ailleurs  $3n^2 + 8n \equiv 3n^2 + 3n [5]$  donc :

$$\begin{aligned} 5 \mid 3n^2 + 8n &\iff 5 \mid 3n(n+1) \\ &\iff 3 \mid n(n+1) \quad (\text{car } 3 \wedge 5 = 1, \text{ lemme de Gauss}) \\ &\iff 5 \mid n \text{ ou } 5 \mid n+1 \quad (\text{car } 5 \in \mathcal{P}) \end{aligned}$$

Ainsi :

$$\begin{aligned} 10 \mid n^2 + (n+1)^2 + (n+3)^2 &\iff 2 \mid n \text{ et } (5 \mid n \text{ ou } 5 \mid n+1) \\ &\iff (2 \mid n \text{ et } 5 \mid n) \text{ ou } (2 \mid n \text{ et } 5 \mid n+1) \\ &\iff 10 \mid n \text{ ou } (n+1 \text{ impair et } 5 \mid n+1) \end{aligned}$$

car 2 et 5 sont premiers entre eux. Or les entiers impairs multiples de 5 sont de la forme  $5(2k+1)$  où  $k \in \mathbb{Z}$ . Ainsi, l'ensemble des solutions est :

$$\boxed{\{10k \mid k \in \mathbb{Z}\} \cup \{10k+4 \mid k \in \mathbb{Z}\}}$$

## Exercice 6

1. Par définition de  $a_0, a_1, \dots, a_r$ , on a  $n = \sum_{k=0}^r a_k 10^k$ . Pour tout  $k \in \llbracket 2, r \rrbracket$ , on a :

$$10^k = 4 \times 25 \times 10^{k-2}$$

donc  $4 \mid a_k 10^k$ . Ainsi,  $n \equiv a_0 + 10a_1 [4]$ . On en déduit que :

$$\boxed{4 \text{ divise } n \text{ si et seulement si } n \text{ divise } a_0 + 10a_1},$$

ce qu'il fallait démontrer.

2. Comme  $10 \equiv 1 [3]$ , on a :

$$\forall k \in \llbracket 0, r \rrbracket, \quad 10^k \equiv 1 [3] \quad \text{et donc} \quad a_k 10^k \equiv a_k [3]$$

Ainsi,  $n \equiv \sum_{k=0}^r a_k [3]$  donc :

$$\boxed{3 \text{ divise } n \text{ si et seulement si } 3 \text{ divise } \sum_{k=0}^r a_k}$$

Le même résultat est valable pour la divisibilité par 9 (puisque  $10 \equiv 1 [9]$ ).

3. On a  $10 \equiv -1 [11]$  donc (même raisonnement que précédemment) :

$$n \equiv \sum_{k=0}^r (-1)^k [11]$$

Ainsi :

$$\boxed{11 \text{ divise } n \text{ si et seulement si } 11 \text{ divise } \sum_{k=0}^r (-1)^k a_k}$$

**Exercice 7** Soient  $x, y \in \mathbb{Z}$ . On raisonne par double implication.

- ★ Supposons que  $x$  et  $y$  soient divisibles par 7. On a  $x \equiv 0 [7]$  donc  $x^2 \equiv 0 [7]$ . De la même façon, on a aussi  $y^2 \equiv 0 [7]$  et donc  $x^2 + y^2 \equiv 0 [7]$ . Autrement dit, 7 divise  $x^2 + y^2$ .
- ★ Supposons que  $7 \mid x^2 + y^2$ . Montrons que  $x$  et  $y$  sont divisibles par 7. Le reste, dans la division euclidienne de  $x$  par 7 est un entier de  $\llbracket 0, 6 \rrbracket$ . Donc  $x^2$  est congru à l'un des carrés de ces entiers modulo 7. Or  $3^2 \equiv 2 [7]$ ,  $4^2 \equiv 2 [7]$ ,  $5^2 \equiv 4 [7]$  et  $6^2 \equiv 1 [7]$ . Ainsi, le reste dans la division euclidienne de  $x^2$  par 7 vaut 0 (ceci ne se produit que si  $x$  est un multiple de 7) 1, 2 ou 4. Il en est de même pour  $y^2$ . Or :

$$\forall k, \ell \in \{0, 1, 2, 4\}, \quad k + \ell \equiv 0 [7] \iff k = \ell = 0$$

On en déduit que si  $x^2 + y^2 \equiv 0 [7]$ , alors  $x \equiv y \equiv 0 [7]$ .

Finalement :

$$\boxed{x^2 + y^2 \text{ est divisible par 7 si et seulement si } x \text{ et } y \text{ sont divisibles par 7}}$$

**Exercice 8** Soit  $p \in \mathcal{P} \setminus \{2, 3\}$ . On a  $p^2 - 1 = (p-1)(p+1)$ .

- ★ Le nombre premier  $p$  est impair (car  $p \neq 2$ ) donc  $p-1$  et  $p+1$  sont deux entiers pairs consécutifs. L'un des deux est donc un multiple de 4. On en déduit que  $8 \mid p^2 - 1$ .

★ Comme  $p$  est un nombre premier différent de 3, il existe un entier naturel  $k$  tel que  $p = 3k + 1$  ou  $p = 3k + 2$  (si  $p$  était un multiple de 3 différent de 3, alors  $p$  ne serait pas un nombre premier).

— Si  $p = 3k + 1$ , alors  $p - 1$  est un multiple de 3 et donc  $3 \mid p^2 - 1$ .

— Si  $p = 3k + 2$ , alors  $p + 1 = 3(k + 1)$  est un multiple de 3 donc  $3 \mid p^2 - 1$ .

Dans les deux cas,  $3 \mid p^2 - 1$ .

Finalement,  $p^2 - 1$  est divisible par 3 et par 8. Or 3 et 8 sont premiers entre eux donc  $3 \times 8 \mid p^2 - 1$ . Ainsi :

$$\boxed{p^2 - 1 \text{ est divisible par } 24}$$

**Exercice 9** Soient  $n \in \mathbb{N}^*$  et  $a, b \in \mathbb{Z}$ . On suppose que  $a \equiv b[n]$ . Montrons que  $n^2 \mid a^n - b^n$ . On a :

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

Comme  $a \equiv b[n]$ , on a (par compatibilité de la relation de congruence avec l'exponentiation positive entière) :

$$\forall k \in \llbracket 0, n-1 \rrbracket, \quad a^k \equiv b^k[n]$$

La relation de congruence est compatible également avec la multiplication donc :

$$\forall k \in \llbracket 0, n-1 \rrbracket, \quad a^k b^{n-1-k} \equiv b^{n-1}[n]$$

puis (en utilisant cette fois la compatibilité avec l'addition) :

$$\sum_{k=0}^{n-1} a^k b^{n-1-k} \equiv \sum_{k=0}^{n-1} b^{n-1} \equiv n b^{n-1} \equiv 0[n]$$

Ainsi,  $n \mid \sum_{k=0}^{n-1} a^k b^{n-1-k}$  et  $n \mid a - b$  par hypothèse donc :

$$n^2 \mid (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k} \quad i.e. \quad n^2 \mid a^n - b^n$$

Finalement :

$$\boxed{a^n \equiv b^n[n^2]}$$

**Exercice 10** Soient  $a \in \mathbb{Z} \setminus (2\mathbb{Z})$  et  $n \in \mathbb{N}$ . Montrons que  $a^{2^n} \equiv 1[2^{n+1}]$  en utilisant un raisonnement par récurrence.

★ Comme  $a$  est impair, l'entier  $a^{2^0} - 1 = a - 1$  est pair donc  $2 \mid a - 1$ . La relation de congruence est donc vraie pour  $n = 0$ .

★ Soit  $n \in \mathbb{N}$ . On suppose que  $a^{2^n} \equiv 1[2^{n+1}]$ . Montrons que  $a^{2^{n+1}} \equiv 1[2^{n+2}]$ . On a :

$$a^{2^{n+1}} - 1 = a^{2^n \times 2} - 1 = (a^{2^n})^2 - 1^2 = (a^{2^n} - 1)(a^{2^n} + 1)$$

Par hypothèse, on sait que  $2^{n+1} \mid a^{2^n} - 1$ . De plus,  $a^{2^n}$  est impair car  $a$  est impair (en effet, un entier  $k$  est impair si et seulement si  $k \equiv 1[2]$  et, dans ce cas, on a  $k^\alpha \equiv 1[2]$  pour tout  $\alpha \in \mathbb{N}$ ). Ainsi,  $a^{2^n} + 1$  est pair donc  $2 \mid a^{2^n} + 1$ . Finalement :

$$2^{n+1} \times 2 \mid (a^{2^n} - 1)(a^{2^n} + 1) \quad i.e. \quad 2^{n+2} \mid a^{2^{n+1}} - 1$$

Autrement dit,  $a^{2^{n+2}} \equiv 1[2^{n+2}]$ .

Par principe de récurrence simple, on peut conclure que :

$$\boxed{\forall n \in \mathbb{N}, \quad a^{2^n} \equiv 1[2^{n+1}]}$$

**Exercice 11** Soit  $n \in \mathbb{Z}$ . On utilise l'algorithme d'Euclide étendu pour déterminer le PGCD des entiers  $n^3 + n^2 + 1$  et  $n^2 - n + 1$ .

★ On a  $n^3 + n^2 + 1 = (n + 2)(n^2 - n + 1) + n - 1$ .

★ Ensuite,  $n^2 - n + 1 = n(n - 1) + 1$ .

★ Et enfin  $n - 1 = 1 \times (n - 1) + 0$ .

Le dernier reste non nul obtenu est égal à 1 donc  $(n^3 + n^2 + 1) \wedge (n^2 - n + 1) = 1$ . Donc :

$$\boxed{\text{pour tout } n \in \mathbb{Z}, \text{ les entiers } n^3 + n^2 + 1 \text{ et } n^2 - n + 1 \text{ sont premiers entre eux}}$$

**Exercice 12** Soient  $a, b \in \mathbb{N}^*$  tels que  $a \wedge b = 1$ . Montrons que  $(a + b) \wedge ab = 1$ .

★ Posons  $d = (a + b) \wedge a$ . On a  $d \mid a + b$  et  $d \mid a$  donc  $d \mid (a + b) - a$  i.e.  $d \mid b$ . Ainsi,  $d \mid a \wedge b$ , i.e.  $d \mid 1$ . Or  $d \geq 1$  donc  $d = 1$ . Ainsi,  $(a + b) \wedge a = 1$ .

★ De la même manière,  $(a + b) \wedge b = 1$ .

★ Comme  $(a + b) \wedge a = (a + b) \wedge b = 1$ , on a aussi  $(a + b) \wedge ab = 1$  (propriété de cours).

Finalement :

$$\boxed{(a + b) \wedge ab = 1}$$

**Exercice 13**

1. Soit  $n \in \mathbb{N}$ . On a :

$$2 \times (n + 1) + (-1) \times (2n + 1) = 1$$

donc, d'après le théorème de Bézout,  $(n + 1) \wedge (2n + 1) = 1$ . Ainsi :

pour tout entier naturel  $n$ , les nombres  $n + 1$  et  $2n + 1$  sont premiers entre eux

### Autre méthode :

Soit  $n \in \mathbb{N}$ . On pose  $d = (n + 1) \wedge (2n + 1)$ . On a  $d \mid n + 1$  et  $d \mid 2n + 1$  donc  $d \mid 2(n + 1) - (2n + 1)$ , i.e.  $d \mid 1$  donc  $d = \pm 1$ . Mais  $d \geq 0$  (par définition du PGCD) donc  $d = 1$ . Ainsi  $(n + 1) \wedge (2n + 1) = 1$ .

2. Soit  $n \in \mathbb{N}$ . On a :

$$\binom{2n+1}{n+1} = \frac{(2n+1)!}{(n+1)!(2n+1-n-1)!} = \frac{2n+1}{n+1} \times \frac{(2n)!}{n!n!} = \frac{2n+1}{n+1} \binom{2n}{n}$$

donc :

$$(n+1) \binom{2n+1}{n+1} = (2n+1) \binom{2n}{n}$$

Ainsi,  $n+1 \mid (2n+1) \binom{2n}{n}$ . Comme  $(n+1) \wedge (2n+1) = 1$ , on déduit du lemme de Gauss que  $n+1 \mid \binom{2n}{n}$ . Finalement :

$$\forall n \in \mathbb{N}, \quad n+1 \mid \binom{2n}{n}$$

### Exercice 14

Soit  $p \in \mathcal{P}$ .

1. Soit  $k \in \llbracket 1, p-1 \rrbracket$ . D'après la formule sans nom (à savoir redémontrer), on a :

$$\underbrace{k}_{\in \mathbb{N}} \binom{p}{k} = p \underbrace{\binom{p-1}{k-1}}_{\in \mathbb{N}}$$

Ainsi,  $p \mid k \binom{p}{k}$ . Or  $p$  est un nombre premier et  $1 \leq k < p$  donc  $p \wedge k = 1$ . D'après le lemme de Gauss, on peut conclure que :

$$p \mid \binom{p}{k}$$

2. On utilise un raisonnement par récurrence finie (et la formule du triangle de Pascal).

★ On a  $\binom{p-1}{0} = 1 \equiv 1[p]$ . La propriété est donc vraie au rang  $k = 0$ .

★ Soit  $k \in \llbracket 0, p-2 \rrbracket$ . On suppose que  $\binom{p-1}{k} \equiv (-1)^k [p]$ . Montrons que

$\binom{p-1}{k+1} \equiv (-1)^{k+1} [p]$ . D'après la formule du triangle de Pascal, on a :

$$\binom{p-1}{k} + \binom{p-1}{k+1} = \binom{p}{k+1} \quad \text{i.e.} \quad \binom{p-1}{k+1} = \binom{p}{k+1} - \binom{p-1}{k}$$

Comme  $k+1 \in \llbracket 1, p-1 \rrbracket$ , on a  $\binom{p}{k+1} \equiv 0[p]$  (d'après la question 1.). De

plus  $\binom{p-1}{k} \equiv (-1)^k [p]$  par hypothèse de récurrence donc :

$$\binom{p-1}{k+1} \equiv 0 - (-1)^k \equiv (-1)^{k+1} [p]$$

Par principe de récurrence simple, on peut conclure que :

$$\forall k \in \llbracket 0, p-1 \rrbracket, \quad \binom{p-1}{k} \equiv (-1)^k [p]$$

### Exercice 15

Soient  $a, b \in \mathbb{N} \setminus \{0, 1\}$ . On suppose que  $a \wedge b = 1$ . Montrons que  $\frac{\ln(a)}{\ln(b)} \in \mathbb{R} \setminus \mathbb{Q}$  en raisonnant par l'absurde. Supposons que  $\frac{\ln(a)}{\ln(b)} \in \mathbb{Q}$ . Comme  $a$  et  $b$

sont supérieurs ou égaux à 2, on a  $\frac{\ln(a)}{\ln(b)} \in \mathbb{Q}_+^*$  donc il existe  $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$  tels que

$\frac{\ln(a)}{\ln(b)} = \frac{p}{q}$ . Ainsi,  $q \ln(a) = p \ln(b)$  i.e.  $\ln(a^q) = \ln(b^p)$ . En en déduit que  $a^q = b^p$ . Comme  $q \geq 1$ , on a  $a \mid b^p = b \times b^{p-1}$ . Or  $a \wedge b = 1$  donc  $a \mid b^{p-1}$  (lemme de Gauss). En itérant le raisonnement, on obtient que  $a \mid b^{p-p} = 1$ , ce qui est absurde car  $a \geq 2$ . Finalement :

$$\frac{\ln(a)}{\ln(b)} \in \mathbb{R} \setminus \mathbb{Q}$$

### Exercice 16

**Exercice 17** Soient  $a, b \in \mathbb{N}^*$ . Montrons que  $\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{a \wedge b}$  en raisonnant par double inclusion.

★ Montrons que  $\mathbb{U}_{a \wedge b} \subset \mathbb{U}_a \cap \mathbb{U}_b$ . Soit  $z \in \mathbb{U}_{a \wedge b}$ . Alors  $z^{a \wedge b} = 1$ . Comme  $a \wedge b \mid a$ , il existe  $k \in \mathbb{N}$  tel que  $a = k(a \wedge b)$ . Ainsi :

$$z^a = z^{k(a \wedge b)} = (z^{a \wedge b})^k = 1^k = 1$$

De la même façon,  $z^b = 1$ . Donc  $z \in \mathbb{U}_a \cap \mathbb{U}_b$ . Finalement, on a l'inclusion  $\mathbb{U}_{a \wedge b} \subset \mathbb{U}_a \cap \mathbb{U}_b$ .

★ D'après la relation de Bézout, il existe  $k, \ell \in \mathbb{Z}$  tels que :

$$ak + b\ell = a \wedge b$$

Montrons que  $\mathbb{U}_a \cap \mathbb{U}_b \subset \mathbb{U}_{a \wedge b}$ . Soit  $z \in \mathbb{U}_a \cap \mathbb{U}_b$ . D'après les propriétés de l'exponentiation entière dans  $\mathbb{C}$ , on a :

$$z^{a \wedge b} = z^{ak+b\ell} = z^{ak} z^{b\ell} = (z^a)^k (z^b)^\ell = 1^k 1^\ell = 1 \quad (\text{car } z \in \mathbb{U}_a \cap \mathbb{U}_b)$$

Ainsi,  $z \in \mathbb{U}_{a \wedge b}$ . Finalement,  $\mathbb{U}_a \cap \mathbb{U}_b \subset \mathbb{U}_{a \wedge b}$ .

Par double inclusion, on peut conclure que :

$$\boxed{\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{a \wedge b}}$$

**Exercice 18** Soient  $a, b \in \mathbb{Z}$  et  $n \in \mathbb{N}$ .

1. On suppose que  $a^2$  divise  $b^2$ . Alors :

$$\forall p \in \mathcal{P}, \quad v_p(a^2) \leq v_p(b^2)$$

*i.e.* (d'après les propriétés sur les valuations  $p$ -adiques) :

$$\forall p \in \mathcal{P}, \quad 2v_p(a) \leq 2v_p(b) \quad \text{i.e.} \quad v_p(a) \leq v_p(b)$$

Autrement dit,  $a \mid b$ . Ainsi :

$$\boxed{\text{si } a^2 \text{ divise } b^2, \text{ alors } a \text{ divise } b}$$

2. On sait que :

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$$

donc :

$$(a \wedge b)^n = \prod_{p \in \mathcal{P}} p^{n \min(v_p(a), v_p(b))}$$

Or :

$$\begin{aligned} \forall p \in \mathcal{P}, \quad n \min(v_p(a), v_p(b)) &= \min(nv_p(a), nv_p(b)) \\ &= \min(v_p(a^n), v_p(b^n)) \end{aligned}$$

Ainsi :

$$\boxed{(a \wedge b)^n = \prod_{p \in \mathcal{P}} p^{\min(v_p(a^n), v_p(b^n))} = a^n \wedge b^n}$$

**Exercice 19** Soient  $a, b \in \mathbb{N}^*$  et  $k \in \mathbb{N} \setminus \{0, 1\}$ . On suppose que  $a \wedge b = 1$  et qu'il existe  $c \in \mathbb{N}$  tel que  $ab = c^k$ . Soit  $p \in \mathcal{P}$ . On a :

$$v_p(ab) = v_p(c^k) \quad \text{i.e.} \quad v_p(a) + v_p(b) = kv_p(c)$$

Comme  $a$  et  $b$  sont premiers entre eux,  $p$  ne peut pas être un diviseur de  $a$  et de  $b$ . On a donc  $v_p(a) = 0$  ou  $v_p(b) = 0$ . Dans tous les cas,  $v_p(a)$  et  $v_p(b)$  sont des multiples de  $k$ . On en déduit qu'il existe des familles  $(\alpha_p)_{p \in \mathcal{P}}$  et  $(\beta_p)_{p \in \mathcal{P}}$  telles que :

$$\forall p \in \mathcal{P}, \quad v_p(a) = k\alpha_p \quad \text{et} \quad v_p(b) = k\beta_p$$

Ainsi :

$$a = \prod_{p \in \mathcal{P}} p^{k\alpha_p} = \left( \prod_{p \in \mathcal{P}} p^{\alpha_p} \right)^k \quad \text{et} \quad b = \left( \prod_{p \in \mathcal{P}} p^{\beta_p} \right)^k$$

Finalement :

$$\boxed{a \text{ et } b \text{ sont des puissances } k^e \text{ d'entiers}}$$

**Exercice 20** Soit  $n \in \mathbb{N} \setminus \{0, 1\}$ . Montrons que  $p_{n+1} < p_1 \cdots p_n$ . Posons  $P = p_1 \cdots p_n - 1$ . L'entier  $P$  est supérieur ou égal à 2 (en fait,  $P \geq p_1 p_2 - 1 = 5$ ) donc il admet un facteur premier (d'après le cours) noté  $p$ .

- ★ Comme aucun des nombres  $p_1, \dots, p_n$  ne divise  $P$ , on a  $p > p_n$ . Il existe donc un entier  $k \geq n+1$  tel que  $p = p_k$ .
- ★ Comme  $p_k \mid P$ , on a  $p_k \leq P$ , *i.e.*  $p_k \leq p_1 \cdots p_n - 1$  donc  $p_k < p_1 \cdots p_n$ .
- ★ La suite  $(p_\ell)_{\ell \geq 1}$  est croissante et  $k \geq n+1$  donc  $p_{n+1} \leq p_k < p_1 \cdots p_n$ .

Ainsi :

$$\boxed{\forall n \in \mathbb{N} \setminus \{0, 1\}, \quad p_{n+1} < p_1 \cdots p_n}$$

**Exercice 21** Soient  $a, n \in \mathbb{N} \setminus \{0, 1\}$ . On suppose que  $a^n - 1 \in \mathcal{P}$ .

1. On raisonne par l'absurde : supposons que  $a \neq 2$ , *i.e.* que  $a \geq 3$ . On a :

$$a^n - 1 = a^n - 1^n = (a - 1) \sum_{k=0}^{n-1} a^k$$

Comme  $a \geq 3$ , on a  $a - 1 \geq 2$  et (puisque  $n \geq 2$ ) :

$$\sum_{k=0}^{n-1} a^k \geq \sum_{k=0}^1 3^k = 1 + 3 = 4$$

La factorisation précédente montre donc que  $a^n - 1$  n'est pas un nombre premier, ce qui est exclu. Ainsi :

si  $a^n - 1$  est un nombre premier, alors  $a = 2$

2. À nouveau, raisonnons par l'absurde en supposant que  $n$  n'est pas un nombre premier. Il existe alors deux entiers  $k, \ell$  supérieurs ou égaux à 2 tels que  $n = k\ell$ . Alors :

$$2^n - 1 = 2^{k\ell} - 1 = (2^k)^\ell - 1^\ell = (2^k - 1) \sum_{j=0}^{\ell-1} 2^{kj}$$

Or  $2^k - 1 \geq 3$  (car  $k \geq 2$ ) et :

$$\sum_{j=0}^{\ell-1} 2^{kj} \geq 1 + 2^k \geq 5$$

Ainsi,  $2^n - 1$  n'est pas un nombre premier, ce qui est absurde. Finalement :

si  $2^n - 1$  est un nombre premier, alors  $n$  est un nombre premier

## Exercice 22

1. Soit  $n \in \mathbb{N}^*$ . On suppose que  $2^n + 1 \in \mathcal{P}$ . Montrons que  $n$  est une puissance de 2. Raisonnons par l'absurde en supposant que  $n$  n'est pas une puissance de 2. Il existe donc  $k \in \mathbb{N}$  et  $\ell \in \mathbb{N}^*$  tels que  $n = 2^k(2\ell + 1)$ . On a :

$$2^n + 1 = (2^{2^k})^{2\ell+1} - (-1)^{2\ell+1} = (2^{2^k} + 1) \sum_{j=0}^{2\ell} 2^{j2^k} (-1)^{2\ell-j}$$

Comme  $2\ell + 1 > 1$  (car  $\ell \geq 1$ ), on a  $1 < 2^k < 2^k(2\ell + 1) = n$  donc :

$$1 < 2^{2^k} + 1 < 2^n + 1$$

Ainsi,  $2^{2^k} + 1$  est un diviseur de  $2^n + 1$  différent de 1 et de  $2^n + 1$ , ce qui est absurde car  $2^n + 1$  est un nombre premier. Ainsi :

si  $2^n + 1$  est un nombre premier, alors  $n$  est une puissance de 2

2. (a) On procède par récurrence.

- ★ On a  $F_0 + 2 = (2^{2^0} + 1) + 2 = 5 = 2^2 + 1 = F_1$ . L'égalité est donc vraie pour  $n = 0$ .
- ★ Soit  $n \in \mathbb{N}$ . On suppose que  $F_{n+1} = F_0 \cdots F_n + 2$ . Montrons que :

$$F_{n+2} = F_0 \cdots F_n F_{n+1} + 2$$

On a (par hypothèse de récurrence) :

$$\begin{aligned} F_0 \cdots F_n F_{n+1} &= (F_{n+1} - 2)F_{n+1} = (2^{2^{n+1}} - 1)(2^{2^{n+1}} + 1) \\ &= (2^{2^{n+1}})^2 - 1 \\ &= 2^{2^{n+1} \times 2} - 1 \\ &= 2^{2^{n+2}} - 1 \\ &= F_{n+2} \end{aligned}$$

L'égalité est donc vérifiée au rang  $n + 1$ .

Par principe de récurrence simple, on peut conclure que :

$$\forall n \in \mathbb{N}, \quad F_{n+1} = F_0 \cdots F_n + 2$$

- (b) Soient  $m, n \in \mathbb{N}$  tels que  $m \neq n$ . Quitte à échanger les rôles joués par  $m$  et  $n$ , on peut supposer que  $m < n$ . D'après la question 2.(a), on a l'égalité :

$$F_n = 2 + \prod_{k=0}^{n-1} F_k$$

Raisonnons par l'absurde : supposons que  $F_n$  et  $F_m$  ne soient pas premiers entre eux. Alors il existe  $p \in \mathcal{P}$  tel que  $p \mid F_n$  et  $p \mid F_m$ . Comme  $m \leq n - 1$ , le nombre  $F_m$  est l'un des facteurs du produit  $\prod_{k=0}^{n-1} F_k$ . Ainsi,  $p \mid \prod_{k=0}^{n-1} F_k$  et  $p \mid F_n$  donc :

$$p \mid F_n - \prod_{k=0}^{n-1} F_k \quad i.e. \quad p \mid 2$$

Comme  $p$  est un nombre premier, on a  $p = 2$ . Ceci est absurde car  $F_n$  et  $F_m$  sont des entiers impairs. Ainsi :

$$\forall m, n \in \mathbb{N}, \quad m \neq n \implies F_m \wedge F_n = 1$$

## Exercice 23

1. (a) Soit  $x \in \mathbb{Z}$ . Alors :

$$\begin{aligned} x^2 \equiv 1 [n] &\iff n \mid x^2 - 1 \iff n \mid (x - 1)(x + 1) \\ &\iff n \mid x - 1 \text{ ou } n \mid x + 1 \quad (\text{car } n \in \mathcal{P}) \\ &\iff x \equiv 1 [n] \text{ ou } x \equiv -1 \equiv n - 1 [n] \\ &\iff \exists k \in \mathbb{Z}, \quad x = kn + 1 \text{ ou } x = kn + n - 1 \end{aligned}$$

Ainsi :

les solutions de l'équation dans  $\llbracket 0, n-1 \rrbracket$  sont 1 et  $n-1$ 

**Remarque :** si  $n = 2$ , cette équation a une seule solution (à savoir 1) et si  $n > 2$ , alors l'équation a exactement deux solutions.

(b) Montrons que  $(n-1)! \equiv -1 [n]$ . On a  $(n-1)! = \prod_{k=1}^{n-1} k$ .

★ Si  $n = 2$ , on a  $1! = 1 \equiv -1 [2]$  (car  $2 \mid 2$ ).

★ On suppose maintenant que  $n \in \mathcal{P} \setminus \{2\}$ . Comme  $n$  est un nombre premier, pour tout  $k \in \llbracket 1, n-1 \rrbracket$ , on a  $k \wedge n = 1$  donc (d'après le cours)  $k$  est inversible modulo  $n$ , *i.e.* :

$$\exists ! \ell \in \llbracket 1, n-1 \rrbracket, \quad k\ell \equiv 1 [n]$$

Or, d'après la question 1., les entiers 1 et  $n-1$  sont les deux seuls éléments de  $\llbracket 1, n-1 \rrbracket$  qui sont leur propre inverse. Ainsi :

$$\prod_{k=1}^{n-1} k = 1 \times (n-1) \prod_{k=2}^{n-2} k \equiv 1 \times (n-1) \times 1 \equiv -1 [n]$$

car, dans le dernier produit, on trouve les entiers  $k \in \llbracket 2, n-2 \rrbracket$  et leurs inverses  $\ell \neq k$  modulo  $n$ .

Ainsi :

si  $n$  est un nombre premier, alors  $(n-1)! \equiv -1 [n]$ 

2. On suppose que  $(n-1)! \equiv -1 [n]$ . Soit  $a \in \llbracket 1, n-1 \rrbracket$ . D'après la relation de congruence, il existe  $k \in \mathbb{Z}$  tel que :

$$(n-1)! = -1 + kn \quad \text{i.e.} \quad kn + \underbrace{(-a) \prod_{\substack{\ell=1 \\ \ell \neq a}}^{n-1} \ell}_{\in \mathbb{Z}} = 1$$

D'après le théorème de Bézout, on a  $a \wedge n = 1$ . Finalement,  $n$  est premier avec tous les entiers de  $\llbracket 1, n-1 \rrbracket$  donc les seuls diviseurs de  $n$  sont 1 et  $n$ . On conclut donc que :

 $n$  est un nombre premier