TD 15 : Arithmétique des entiers

▶ Divisibilité, calculs en congruences

Exercice 15.1 Montrer que pour tout $n \in \mathbf{N}$, F

1. $7 \mid 3^{2n+1} + 2^{n+2}$
2. $16 \mid 5^n - 1 - 4n$
3. $6 \mid n(n+2)(7n-5)$

Exercice 15.2 Trouver le reste de la division euclidienne de 100^{1000} par 13. F

Exercice 15.3 En raisonnant modulo 3, montrer que l'équation $x^4 = 3y^2 - 25$, $(x, y) \in \mathbf{N}^2$ ne possède pas de solution. PD

Exercice 15.4 Montrer qu'un entier dont l'écriture en base 10 est la répétition de deux groupes de trois chiffres identiques (comme 817 817) est divisible par 7, par 11 et par 13. D'ailleurs, que vaut le produit $7 \times 11 \times 13$? PD

Exercice 15.5 En utilisant des congruences modulo 3, déterminer tous les nombres premiers p tels que $p^2 + 2$ soit également premier. PD

Exercice 15.6 Déterminer le dernier chiffre de l'écriture décimale de $7^{3^{11^{17}}}$. AD

Exercice 15.7 (Oral Centrale) PD
Pour $n \in \mathbf{N}^*$, on note N le nombre de diviseurs positifs de n et P leur produit. Quelle relation existe-t-il entre n, N et P ?

Exercice 15.8 (Oral ENS) TD
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.

▶ PGCD, PPCM

Exercice 15.9 Pour chacun des couples (a, b) suivants, déterminer $a \wedge b$, $a \vee b$ et une relation de Bézout. F

1. $(51, 438)$
2. $(720, 1320)$
3. $(151, 77)$

Exercice 15.10 Équations $ax + by = c$ PD

1. On s'intéresse dans cette question à l'équation $18x + 25y = 1$, d'inconnue $(x, y) \in \mathbf{Z}^2$.
   (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 $k \in \mathbf{Z}$ 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 15.11 Soient $(a, b, c) \in \mathbf{Z}^3$, tels que a et b soient premiers entre eux. Montrer que $a \wedge (bc) = a \wedge c$. PD

Exercice 15.12 AD

1. Montrer que si r est le reste de la division euclidienne de a par b, alors $2^r - 1$ est le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$.
2. Montrer que le PGCD de $2^a - 1$ et $2^b - 1$ est $2^{a \wedge b} - 1$.

Exercice 15.13 AD

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

Exercice 15.14 Soient $(a, b) \in \mathbf{Z}^2$ et soit $n \in \mathbf{N}^*$. Montrer que $(a \wedge b)^n = a^n \wedge b^n$. PD

Exercice 15.15 (Banque CCP, exercice 95) PD

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

(b) Déterminer toutes les solutions de $(\mathscr{S})$.

Exercice 15.16 Soit $a \in \mathbf{N}^*$, et soit $(F_n)_n$ une suite d'entiers naturels tels que $\forall n \in \mathbf{N}$, $F_{n+2} = aF_{n+1} + F_n$. PD
Montrer que pour tout $n \in \mathbf{N}$, $F_{n+1} \wedge F_n = F_0 \wedge F_1$.

Exercice 15.17 Une réciproque de Bézout PD
Soient a et b deux entiers non nuls, et soit $d \in \mathbf{N}$ un diviseur commun de a et de b. Montrer que s'il existe deux entiers $(u, v) \in \mathbf{Z}^2$ tels que $au + bv = d$, alors $d = a \wedge b$.

Exercice 15.18 Retour sur les racines $n^{\text{èmes}}$ de l'unité AD
Montrer que pour $a, b \in \mathbf{N}^*$, $\mathbf{U}_a \cap \mathbf{U}_b = \mathbf{U}_{a\wedge b}$.

▶ Nombres premiers et décomposition primaire

Exercice 15.19 Soit $n \geqslant 3$. Montrer qu'il n'existe aucun nombre premier entre $n! + 2$ et $n! + n$. F
En déduire 1000 entiers consécutifs sans aucun nombre premier.

Exercice 15.20 Montrer que pour tout entier $n \in \mathbf{N}^*$, $4n^3 + 6n^2 + 4n + 1$ n'est pas premier. F

Exercice 15.21 Nombres de Fermat AD

1. Soit $n \in \mathbf{N}^*$. Montrer que si $2^n + 1$ est premier, alors il existe $m \in \mathbf{N}$ 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 $n \in \mathbf{N}$, $F_{n+1} = F_0F_1 \cdots F_n + 2$.
   (b) En déduire que pour (m, n) distincts, F_m et F_n sont premiers entre eux.

Exercice 15.22 Inégalité ultramétrique PD
Soit p un nombre premier et soit $(a, b) \in \mathbf{N}^* \times \mathbf{N}^*$. Montrer que $v_p(a+b) \geqslant \min(v_p(a), v_p(b))$. Prouver que si $v_p(a) \neq v_p(b)$, alors cette inégalité est en fait une égalité.

Exercice 15.23 En utilisant le petit théorème de Fermat, prouver que pour tout $a \in \mathbf{Z}$, $a^{13} \equiv a \quad [2730]$. AD

Exercice 15.24 Soient p, q deux nombres premiers distincts. Prouver que $p^{q-1} + q^{p-1} \equiv 1 \ [pq]$. AD

Exercice 15.25 Montrer que la suite $(2^n - 3)_n$ contient une infinité de termes divisibles par 5, une infinité de termes divisibles par 13, mais aucun divisible par 5×13. D

Exercice 15.26 Soit $n \in \mathbf{N}^*$, soit $d(n)$ le nombre de diviseurs positifs de n, et soient $p_1, \ldots, p_k$ les facteurs premiers de n. Exprimer $d(n)$ en fonction des $v_{p_i}(n)$, $i \in [\![1, k]\!]$. PD

Exercice 15.27 Soit $n \in \mathbf{N}^*$ et soient a, b deux entiers premiers entre eux. PD
On suppose que le produit ab est une puissance $n^{\text{ème}}$, c'est-à-dire qu'il existe $c \in \mathbf{Z}$ tel que $ab = c^n$.
Montrer que a et b sont déjà eux-mêmes des puissances $n^{\text{èmes}}$.

Exercice 15.28 Autour de la valuation p-adique d'une factorielle AD
Montrer qu'il existe $n \in \mathbf{N}$ tel que $100! = 2^{97}(2n + 1)$.

Exercice 15.29 Pour $n \in \mathbf{N}^*$, on pose $u_n = \left\lfloor (1 + \sqrt{3})^{2n+1} \right\rfloor$. D

1. Prouver que $u_n = (1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1}$.
2. Déterminer la valuation 2-adique de u_n

Exercice 15.30 Théorème de Wilson D

1. Soit p un nombre premier.
   (a) Montrer que $\forall x \in [\![1, p-1]\!]$, $\exists! y \in [\![1, p-1]\!]$ tel que $xy \equiv 1 \quad [p]$.
   (b) En déduire que $(p-1)! \equiv -1 \quad [p]$.
2. Soit $n \in \mathbf{N}^*$, tel que $(n-1)! \equiv -1 \quad [n]$. Montrer que n est premier.

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

Exercice 15.31 Théorème de Kürschák (Oral ENS) TD
Déterminer pour quels entiers $n \geqslant m \geqslant 1$ le nombre $H_{m,n} = \sum_{k=m}^{n} \frac{1}{k}$ est un entier.
Indication : utiliser les valuations 2-adiques des entiers $k \in [\![m, n]\!]$.

Exercice 15.32 Ordre d'un élément dans $\mathbf{Z}/n\mathbf{Z}$ D
Soit $n \in \mathbf{N}^*$. On se place dans le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$.

1. Montrer que $\mathbf{Z}/n\mathbf{Z} = \langle \overline{1} \rangle$, le sous-groupe engendré par la classe de congruence de 1.
2. Soit $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$. Montrer que $d = n \wedge a$ ne dépend pas du choix d'un représentant de $\overline{a}$, et que $\langle \overline{a} \rangle = \langle \overline{d} \rangle$. Quel est le cardinal de $\langle \overline{a} \rangle$?

CORRECTION DES EXERCICES DU TD 15

SOLUTION DE L'EXERCICE 15.1

1. Raisonnons modulo 7 :

$$\begin{aligned} 3^{2n+1} + 2^{n+2} &\equiv 9^n \times 3 + 4 \times 2^n \pmod 7 \\ &\equiv 2^n \times 3 + 4 \times 2^n \pmod 7 \\ &\equiv 2^n (3+4) \pmod 7 \\ &\equiv 2^n \times 7 \equiv 0 \pmod 7. \end{aligned}$$

Et donc $3^{2n+1} + 2^{n+2}$ est divisible par 7.

> **Méthode**
> Montrer qu'un entier est divisible par n, c'est prouver qu'il est congru à 0 modulo n.
> Ceci est souvent plus facile à prouver grâce aux propriétés des congruences.

2. Commençons par calculer les premières puissances de 5 modulo 16 :

$5^2 = 25 \equiv 9 \pmod{16}$, $5^3 \equiv 5^2 \cdot 5 \equiv 45 \equiv 12 \equiv -3 \pmod{16}$, $5^4 \equiv -3 \cdot 5 \equiv 1 \pmod{16}$.

Et donc les puissances suivantes sont faciles

$5^5 \equiv 5^4 \cdot 5 \equiv 5 \pmod{16}$, $5^6 \equiv 5^4 \cdot 5^2 \equiv 9 \pmod{16}$, $5^7 \equiv 5^4 \cdot 5^3 \equiv -3 \pmod{16}$, ...

Et donc pour tout $k \in \mathbf{N}$,

$5^{4k} \equiv 1 \pmod{16}$, $5^{4k+1} \equiv 5 \pmod{16}$, $5^{4k+2} \equiv 9 \pmod{16}$, $5^{4k+3} \equiv -3 \pmod{16}$.

Mais en même temps, on a

$$\begin{aligned} 1 + 4(4k) &\equiv 1 \pmod{16}, \quad 1 + 4(4k+1) \equiv 5 \pmod{16} \\ 1 + 4(4k+2) &\equiv 9 \pmod{16}, \quad 1 + 4(4k+3) \equiv 13 \equiv -3 \pmod{16}. \end{aligned}$$

Dans tous les cas, pour tout $n \in \mathbf{N}$, $5^n \equiv 1 + 4n \pmod{16}$ de sorte que $5^n - 1 - 4n \equiv 0 \pmod{16}$ et donc est divisible par 16.

> **Méthode**
> Une fois qu'on a : $5^4 \equiv 1$, alors pour $n = 4q + r$, on aura
> $$5^n \equiv \left(5^4\right)^q 5^r \equiv 5^r.$$
> Il suffit donc d'obtenir la division euclidienne de n par 4.

> **Autrement dit**
> La classe de congruence de $1 + 4n$ modulo 16, tout comme celle de 5^n, de dépend que de la classe de congruence de n modulo 4.

3. Distinguons plusieurs cas, suivant la classe de congruence de n modulo 6.
Si $n \equiv 0 \pmod 6$, alors $n(n+2)(7n-5) \equiv 0 \pmod 6$.
Si $n \equiv 1 \pmod 6$, alors $n(n+2)(7n-5) \equiv 1 \cdot 3 \cdot (7-5) \equiv 6 \equiv 0 \pmod 6$.
Si $n \equiv 2 \pmod 6$, alors $n(n+2)(7n-5) \equiv 2 \cdot 4 \cdot 9 \equiv 0 \pmod 6$.
Si $n \equiv 3 \pmod 6$, alors $n(n+2)(7n-5) \equiv 3 \cdot 5 \cdot 16 \equiv 15 \cdot 16 \equiv 3 \cdot 4 \equiv 0 \pmod 6$.
Si $n \equiv 4 \pmod 6$, alors $n+2 \equiv 0 \pmod 6$, donc $n(n+2)(7n-5) \equiv 0 \pmod 6$.
Enfin, si $n \equiv 5 \pmod 6$, alors $n(n+2)(7n-5) \equiv 5 \cdot 7 \cdot 30 \equiv 0 \pmod 6$.
Donc dans tous les cas, $n(n+2)(7n-5) \equiv 0 \pmod 6$, donc $6 \mid n(n+2)(7n-5)$.

SOLUTION DE L'EXERCICE 15.2

Notons que $100^{1000} = 10^{2000}$. Or, $10 \equiv -3 \ [13]$.
Et donc $10^2 = (-3)^2 = 9 \equiv -4 \ [13]$, $10^3 \equiv -40 \equiv -1 \ [13]$, de sorte que $10^6 \equiv 1 [13]$.
Mais $2000 = 6 \times 333 + 2$ de sorte que

$$10^{2000} \equiv 10^{6 \times 333 + 2} \equiv 10^2 (10^6)^{333} \equiv 10^2 \equiv -4 \equiv 9 \ [13].$$

Et donc[1] le reste de la division euclidienne par 13 de 100^{1000} vaut 9.

> **Méthode**
> La question peut en fait se reformuler en «trouver la classe de 100^{1000} modulo 13», et nous allons donc raisonner modulo 13.

[1] 9 est compris entre 0 et 12, ce qui n'était pas le cas de -4.

SOLUTION DE L'EXERCICE 15.3

Soit $x \in \mathbf{Z}$. Alors on a soit $x \equiv 0 \ [3]$, soit $x \equiv 1 \ [3]$, soit $x \equiv 2 \ [3]$.
Dans le premier cas, $x^2 \equiv 0 \ [3]$, et dans les deux autres, $x^2 \equiv 1 \ [3]$.

Et alors une puissance $4^{\text{ème}}$ est aussi nécessairement congrue à 0 ou 1 modulo 3.
Or s'il existait $x, y \in \mathbf{Z}$ tels que $x^4 = 3y^2 - 25$, alors $x^4 \equiv -25 \equiv -1 \equiv 2 \ [3]$, ce qui est impossible.
Donc l'équation $x^4 = 3y^2 - 25$ ne possède pas de solution.

SOLUTION DE L'EXERCICE 15.4

Il s'agit de noter que $1000 \equiv -1 \pmod 7$, car $1000 = 143 \times 7 - 1$
Or un nombre formé de deux groupes de trois chiffres identiques est de la forme $n = 1000a + a = 1001a$, avec $a \in [\![0, 999]\!]$.
Mais alors $n \equiv 1001a \pmod 7 \equiv 0 \pmod 7$.
Comme $1001 = 7 \times 11 \times 13$, le même raisonnement est valable modulo 11 et modulo 13.

Solution de l'exercice 15.5

Notons que $p = 3$ est clairement solution car $p^2 + 2 = 11$ est premier.
De plus, $p = 2$ n'est pas solution car $p^2 + 2 = 6$ n'est pas premier.
Soit donc p un nombre premier supérieur ou égal à 5.
Alors p ne peut être divisible par 3, et donc est congru à 1 ou à 2 modulo 3.
Or, $1^2 = 1 \equiv 1$ [3] et $2^2 = 4 \equiv 1 \pmod 3$, de sorte que dans tous les cas, $p^2 + 2 \equiv 0 \pmod 3$.
Autrement dit, 3 divise $p^2 + 2$, qui ne peut donc pas être premier.
Ainsi, 3 est le seul nombre premier tel que $p^2 + 2$ soit encore premier.

Solution de l'exercice 15.6

Il s'agit donc de trouver le reste de la division euclidienne de $n = 7^{3^{11^{17}}}$ par 10, ou encore de trouver sa classe de congruence modulo 10.
On a $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 7^2 \cdot 7 \equiv 63 \equiv 3 \pmod{10}$ et $7^4 \equiv 7^3 \cdot 7 \equiv 21 \equiv 1 \pmod{10}$.
Ainsi, si $a = 4k + r$ est la division euclidienne de a par 4, alors $7^a = \left(7^4\right)^k 7^r \equiv 7^r \pmod{10}$.
Donc il s'agit ici de déterminer la classe de congruence de $3^{11^{17}}$ modulo 4.
Or $3 \equiv -1 \pmod 4$ de sorte que $3^2 \equiv 1 \pmod 4$.
Et donc $3^b \equiv 3 \pmod 4$ si b est impair et $3^b \equiv 1 \pmod 4$ si b est pair.
Puisque 11^{17} est impair, $3^{11^{17}} \equiv 3 \pmod 4$, et donc $n \equiv 7^3 \equiv 3 \pmod{10}$.
Donc le dernier chiffre de l'écriture décimale de n est un 3.

Solution de l'exercice 15.7

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 $P = n^{N/2}$.

> **Remarque**
> Notons qu'avec nos notations, N est le cardinal de D_n.

Solution de l'exercice 15.8

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

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

> **Remarque**
> $n + 1$ est le nombre de chiffres de l'écriture décimale de N.

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.

> **Nbe de chiffres**
> Comme mentionné plus tôt, ce nombre est celui dont l'écriture décimale contient 672 fois le chiffre 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].

SOLUTION DE L'EXERCICE 15.9

Il s'agit d'appliquer (bêtement) l'algorithme d'Euclide étendu.

1. $51 \wedge 438 = 3 = 43 \times 51 - 5 \times 438$. On a alors $51 \vee 438 = \dfrac{51 \times 438}{3} = 7446$.

2. $720 \wedge 1320 = 120 = 2 \times 720 - 1320$. On a donc $720 \vee 1320 = 7920$.

3. $77 \wedge 151 = 1 = 51 \times 77 - 26 \times 151$. Et donc $77 \vee 151 = 11\,627$.

SOLUTION DE L'EXERCICE 15.10

Notons que $18x + 25y = 1$ est une équation de droite $(\mathscr{D})$. Résoudre cette équation, c'est donc trouver tous les points à coordonnées entières situées sur $\mathscr{D}$.

1.a. Déterminer une solution particulière, c'est trouver une relation de Bézout pour le couple $(18, 25)$. L'algorithme d'Euclide étendu nous fournit alors $18 \times 7 + 25 \times (-5) = 1$.
Donc $(7, -5)$ est solution.

1.b. L'équation s'écrit alors

$$18x + 25y = 18x_0 + 25y_0 \Leftrightarrow 18(x - x_0) = 25(y_0 - y).$$

Et alors, si (x, y) est une solution, 25 divise $18(x - x_0)$. Étant premier à 18, par le lemme de Gauss, il divise $x - x_0$: il existe $k \in \mathbf{Z}$ tel que $x = 25k + x_0$.

1.c. Si (x, y) est solution, alors il existe $k \in \mathbf{Z}$ tel que $x = 25k + x_0$, alors $18k = y_0 - y$, donc $y = y_0 - 18k$.
Inversement, pour $k \in \mathbf{Z}$, alors $(25k + x_0, y_0 - 18k)$ est solution puisque

$$18(25k + x_0) + 25(y_0 - 18k) = 18x_0 + 25y_0 = 1.$$

Donc l'ensemble des solutions est $\{(25k + 7, -5 - 18k),\ k \in \mathbf{Z}\}$.

2. L'équation $9x + 15y = 3$ est équivalente à l'équation $3x + 5y = 1$, où 3 et 5 sont premiers entre eux, et donc il est possible d'appliquer la même méthode que précédemment.
Notons qu'une solution particulière s'obtient sans faire appel à l'algorithme d'Euclide étendu : $3 \times 2 + 5 \times (-1) = 1$.
Donc $(2, -1)$ est solution particulière.
Et alors sur le même principe, on prouve que les solutions de $3x + 5y = 1$ sont les $(2+5k, -1-3k)$, $k \in \mathbf{Z}$, et donc les solutions de $9x+15y = 3$ sont les $(6+15k, -2-9k)$, $k \in \mathbf{Z}$.

Là encore, nous pouvons simplifier un peu, et diviser l'équation par $42 \wedge 45 = 3$. On obtient alors l'équation $14x + 15y = 2$.
Mais $15 - 14 = 1$, donc $15 \times 2 + (-2) \times 14 = 2$.
On montre alors de même que précédemment que les solutions sont les $(-6 + 15k, 6 - 14k)$, $k \in \mathbf{Z}$.

Enfin, pour la dernière, on a $12 \wedge 30 = 6$. Et donc 6 divise toujours $12x + 30y$. Or $6 \nmid 15$, donc l'équation $12x + 30y = 15$ n'a pas de solutions entières.

SOLUTION DE L'EXERCICE 15.11

Si $d \mid a$, alors d est premier avec b.
En effet, si on note $d' = d \wedge b$, alors $d' \mid a$ et $d' \mid b$, donc $d' \mid a \wedge b = 1$. Donc $d \wedge b = 1$.
Et donc si $d \mid bc$, alors[2] $d \mid c$. On en déduit qu'un diviseur commun à a et bc divise a et c, donc en particulier, $a \wedge (bc)$ divise $a \wedge c$.

[2] C'est le lemme de Gauss.

Inversement, $a \wedge c$ divise à la fois a et bc, donc divise $a \wedge (bc)$.
Et donc $a \wedge (bc) = a \wedge c$.

Détails
Les deux PGCD sont positifs, donc s'ils se divisent mutuellement, ils sont égaux.

SOLUTION DE L'EXERCICE 15.12

1. Si $a = bq + r$, alors

$$\begin{aligned} 2^a - 1 = 2^{bq+r} - 1 &= 2^{bq+r} - 2^r + 2^r - 1 = 2^r\left(2^{bq} - 1\right) + 2^r - 1 \\ &= 2^r\left(2^b - 1\right)\left(1 + 2^b + \cdots + 2^{b(q-1)}\right) + 2^r - 1. \end{aligned}$$

Puisque $2^r - 1 < 2^b - 1$, il s'agit bien là de la division euclidienne de $2^a - 1$ par $2^b - 1$.

2. Utilisons l'algorithme d'Euclide pour calculer le PGCD de a et b. Notons r_1 le reste de la division euclidienne de a par b, r_2 le reste de la division euclidienne de b par r_1, etc, jusqu'à r_n, le dernier reste non nul (et donc le PGCD de a et b), et donc $r_n = 0$.
Alors le reste de la division de $2^a - 1$ par $2^b - 1$ est $2^{r_1} - 1$. Puis le reste de la division de $2^b - 1$ par $2^{r_1} - 1$ est $2^{r_2} - 1$, etc. On arrive alors au reste de la division euclidienne de $2^{r_{n-1}} - 1$ par $2^{r_n} - 1$ qui vaut $2^0 - 1 = 0$.
Par le lemme d'Euclide, on a donc

$$(2^a-1)\wedge(2^b-1) = (2^b-1)\wedge(2^{r_1}-1) = (2^{r_1}-1)\wedge(2^{r_2}-1) = \cdots = (2^{r_{n-1}}-1)\wedge(2^0-1) = 2^{r_{n-1}}-1 = 2^{a\wedge b}-1.$$

Donc le PGCD de $2^a - 1$ et $2^b - 1$ est $2^{r_n} - 1$, ce qui est bien le résultat attendu.

Solution de l'exercice 15.13

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 $(a + b) \wedge (ab) = 1$.
Alors $a + b$ 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.

> **Rappel**
> Un entier est premier avec un produit si et seulement si il est premier avec chacun de ses facteurs.

Alternative : supposons qu'il existe un nombre premier p divisant $(a + b) \wedge ab$.
Alors p divise a ou p divise b.
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.

> **⚠ Attention !**
> Ici il est fondamental de supposer p premier, sans cette hypothèse, p peut diviser un produit dans diviser aucun de ses termes. Par exemple $4 \mid 2 \times 6$, mais $4 \nmid 2$ et $4 \nmid 6$.

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

$$(a+b)\wedge(a\vee b) = [d(a'+b')]\wedge[(da')\vee(db')] = d\,[(a'+b')\wedge(a'\vee b')] = d\times 1 = d = a\wedge b.$$

2. Nommons $(\mathcal{S})$ le système de l'énoncé.
Si (a, b) est une solution de $(\mathcal{S})$, 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 $(\mathcal{S})$ si et seulement si il existe deux entiers a', b' premiers entre eux tels que $(a, b) = (12a', 12b')$, avec (a, b') solution de $\begin{cases} a' + b' = 12 \\ a'b' = 35 \end{cases}$ $(\mathcal{S}')$.

> **Méthode**
> Pour calculer ce PGCD on peut, au choix utiliser l'algorithme d'Euclide, ou utiliser les décompositions en produits de facteurs premiers de 420 et 144.

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 $\dfrac{12 + \sqrt{4}}{2} = 7$ et $\dfrac{12 - \sqrt{4}}{2} = 5$.
Ainsi, les couples de réels (a', b') solutions du système $(\mathcal{S}')$ sont $(5, 7)$ et $(7, 5)$.
Et donc les solutions au système $(\mathcal{S})$ 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.

Solution de l'exercice 15.14

Notons $d = a \wedge b$, de sorte qu'il existe a', b' premiers entre eux tels que $a = da'$ et $b = db'$.
On a donc $(a \wedge b)^n = d^n(a' \wedge b')^n = d^n$, et $a^n \wedge b^n = (d^n a'^n) \wedge (d^n b'^n) = d^n\,(a'^n \wedge b'^n)$.
Il s'agit donc de prouver que $a'^n \wedge b'^n = 1$, soit encore que a'^n et b'^n sont premiers entre eux.

Mais puisque a' et b' sont premiers entre eux, a' est premier avec $b' \times b' \times \cdots \times b' = b'^n$.
Et alors b'^n est premier avec a', donc avec $a' \times a' \times \cdots \times a' = a'^n$.
Et donc $a'^n \wedge b'^n = 1$, et donc $(a \wedge b)^n = d^n = d^n(a'^n \wedge b'^n) = a^n \wedge b^n$.

Solution de l'exercice 15.15

1. Supposons que $a \mid c$ et $b \mid c$. Alors c est un multiple commun de a et b, et donc est un multiple de $a \wedge b = ab$. Donc $ab \mid c$.

> **Toujours vrai**
> Notons que cette implication ne nécessite pas que a et b soient premiers entre eux, et est toujours vraie.

Inversement, puisque a et b divisent ab, si $ab \mid c$, alors $a \mid c$ et $b \mid c$.

2.a. Si vous êtes chanceux, vous pouvez peut-être trouver directement une solution particulière, et dans ce cas il ne faut pas se priver de l'utiliser. Par contre, si en deux minutes vous ne voyez pas de solution particulière «évidente», alors il ne faut pas persévérer et essayer de mettre en œuvre une solution un peu plus systématique.

Un entier x_0 est solution de $(\mathscr{S})$ si et seulement si il existe deux entiers relatifs k_1 et k_2 tels que $\begin{cases} x_0 = 6 + 17k_1 \\ x_0 = 4 + 15k_2 \end{cases}$
En particulier, en soustrayant ces deux équations, il vient $2 = 15k_2 - 17k_1$.
Ce système a alors une solution relativement évidente : $2 = 15 \times (-1) - 17 \times (-1)$.
Si $k_1 = k_2 = -1$, on a donc $x_0 = 6 - 17 = 4 - 15 = -11$.
Ainsi, -11 est une solution particulière du système.

2.b. Soit $x \in \mathbf{Z}$. Alors x est solution de $(\mathscr{S})$ si et seulement si

$$\begin{cases} x \equiv x_0 \pmod{17} \\ x \equiv x_0 \pmod{15} \end{cases} \Leftrightarrow \begin{cases} x - x_0 \equiv 0 \pmod{17} \\ x - x_0 \equiv 0 \pmod{15} \end{cases} \Leftrightarrow 15 \mid (x - x_0) \text{ et } 17 \mid (x - x_0).$$

Par la question 1, qui s'applique puisque 15 et 17 sont premiers entre eux[3], cette dernière condition est vérifiée si et seulement si $x - x_0$ est divisible par $15 \times 17 = 255$.
Donc les solutions de $(\mathscr{S})$ sont les $x_0 + 255k = 255k - 11$, $k \in \mathbf{Z}$.

[3] 17 est premier et ne divise pas 15.

SOLUTION DE L'EXERCICE 15.16

Il s'agit de prouver que la suite $(F_{n+1} \wedge F_n)_n$ est constante, et donc autrement dit que pour tout n, $F_{n+2} \wedge F_{n+1} = F_{n+1} \wedge F_n$.

Commençons par noter[4] que (F_n) est strictement croissante.

[4] Il faudrait une récurrence pour le prouver proprement...

Et alors $F_{n+2} = aF_{n+1} + F_n$ est la division euclidienne de F_{n+2} par F_{n+1}.
Le lemme d'Euclide nous affirme qu'alors $F_{n+2} \wedge F_{n+1} = F_{n+1} \wedge F_n$, d'où le résultat cherché.

Rappel
$a \wedge b$ est le plus grand, au sens de la divisibilité, diviseur commun de a et b : tout autre diviseur commun divise le PGCD.

SOLUTION DE L'EXERCICE 15.17

Nous savons que $a \wedge b$ divise $au + bv = d$.
D'autre part, d étant un diviseur commun de a et b, $d \mid a \wedge b$.
Et donc d et $a \wedge b$ étant positifs, on a bien l'égalité $d = a \wedge b$.

SOLUTION DE L'EXERCICE 15.18

Notons $d = a \wedge b$, de sorte qu'il existe deux entiers a' et b' tels que $a = da'$ et $b = db'$.
Soit alors $z \in \mathbf{U}_{a \wedge b} = \mathbf{U}_d$.
Alors $z^a = z^{a'd} = \left(z^d\right)^{a'} = 1^{a'} = 1$, donc $z \in \mathbf{U}_a$.
De même, on prouve que $z \in \mathbf{U}_b$, et donc $z \in \mathbf{U}_a \cap \mathbf{U}_b$, de sorte que $\mathbf{U}_d \subset \mathbf{U}_a \cap \mathbf{U}_b$.
Inversement, par l'identité de Bézout, il existe u et v tels que $d = au + bv$, et donc pour $z \in \mathbf{U}_a \cap \mathbf{U}_b$, on a

$$z^d = z^{au+bv} = z^{au} z^{bv} = (z^a)^u \left(z^b\right)^v = 1.$$

Et donc $z \in \mathbf{U}_d$, de sorte que $\mathbf{U}_a \cap \mathbf{U}_b \subset \mathbf{U}_d$, et donc par double inclusion, $\mathbf{U}_d = \mathbf{U}_a \cap \mathbf{U}_b$.

Plus généralement
Si $p \mid q$, alors $\mathbf{U}_p \subset \mathbf{U}_q$.

SOLUTION DE L'EXERCICE 15.19

Soit $k \in [\![2, n]\!]$. Alors $k \mid n!$ et donc $k \mid n! + k$.
Et par conséquent, $n! + k$ n'est pas premier.
Pour obtenir 1000 nombres consécutifs, il faut donc $n - 2 + 1 = 1000 \Leftrightarrow n = 1001$.
Et donc les entiers $1001!+2, 1001!+3, \ldots, 1001!+1001$ sont 1000 nombres consécutifs, dont aucun n'est premier par ce qui précède. Aucun de ces entiers n'est premier car $1001! + k$ est divisible par k, pour $2 \leqslant k \leqslant 1000$.

SOLUTION DE L'EXERCICE 15.20

Vous avez probablement reconnu des coefficients du triangle de Pascal : $4, 6, 4, 1$, il ne nous manque qu'un 1 au début de cette séquence pour qu'il s'agisse d'une ligne du triangle de Pascal.
Plus précisément, on a

$$\begin{aligned} 4n^3 + 6n^2 + 4n + 1 &= (n+1)^4 - n^4 \\ &= \left((n+1)^2\right)^2 - \left(n^2\right)^2 \end{aligned}$$

$$= ((n+1)^2 - n^2)((n+1)^2 + n^2) = (2n+1)(2n^2+2n+1).$$

Nous avons donc deux diviseurs de $4n^3 + 6n^2 + 4n + 1$, tous deux strictement supérieurs à 1, donc $4n^3 + 6n^2 + 4n + 1$ n'est pas premier.

Solution de l'exercice 15.21

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 $n = 2^m$.

> **Astuce**
> La troisième identité remarquable, si elle permet de factoriser $a^n - b^n$ quel que soit n permet également de factoriser $a^m + b^m$ lorsque m est impair car $+b^m = -(-b)^m$.

Commentaire historique *: les premiers nombres de Fermat sont $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65\,537$.*
Ces nombres sont tous premiers. On a alors $F_5 = 4\,294\,967\,297$, 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 $64 \mid F_5$, 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.
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[5] 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 ou $68 = 2^2 \times 17$ côtés, mais pas un polygone à $25 = 5^2$ ou à 11 côtés.

[5] Vous savez par exemple comment obtenir un hexagone puisque vous avez déjà tracé une rosace...

2.a. Prouvons le résultat par récurrence sur n.
On a $F_1 = 2^2 + 1 = 5 = 3 + 2 = (2^{2^0} + 1) + 2 = F_0 + 2$. Donc la récurrence est bien initialisée.
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 $n \in \mathbf{N}$, $F_{n+1} = F_0 \cdots F_n + 2$.

2.b. Supposons que $m < n$. Alors $F_n = F_0 \cdots F_m \cdots F_{n-1} + 2$.
Si d est un diviseur 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.

Solution de l'exercice 15.22

Quitte à échanger a et b, on peut supposer que $v_p(a) \leqslant v_p(b)$, et donc que $\min(v_p(a), v_p(b)) = v_p(a)$.
Puisque $p^{v_p(a)}$ divise $p^{v_p(b)}$ et que $p^{v_p(b)}$ divise b, alors $p^{v_p(a)}$ divise b.
Comme $p^{v_p(a)}$ divise évidemment a, il divise $a + b$.
Et donc $v_p(a+b) \geqslant v_p(a)$, ce qui prouve bien l'inégalité demandée.

> **Inégalité**
> Notons que cette inégalité peut être stricte. Par exemple, $v_5(15) = v_5(10) = 1$, mais $v_5(10 + 15) = 2$.

Si $v_p(b) \neq v_p(a)$, notons alors a' et b' deux entiers tels que $a = p^{v_p(a)}a'$ et $b = p^{v_p(b)}b'$.
Alors $a + b = p^{v_p(a)}\left(a' + p^{v_p(b)-v_p(a)}b'\right)$.
Mais p ne peut pas diviser $a' + p^{v_p(b)-v_p(a)}b'$, car divisant déjà[6] $p^{v_p(b)-v_p(a)}b'$, il diviserait

[6] $v_p(b) - v_p(a) \geqslant 1$.

alors $a' = \left(a' + p^{v_p(b)-v_p(a)}b'\right) - p^{v_p(b)-v_p(a)}b'$.
On en déduit donc que $v_p(a+b) = v_p(a) = \min(v_p(a), v_p(b))$.
En revanche, si $v_p(a) = v_p(b)$, alors on ne peut faire mieux que l'inégalité générale.
Elle peut toujours être une égalité, par exemple, si $p \geqslant 5$ est premier, alors $v_p(p) = 1 = v_p(2p)$ et $v_p(p+2p) = v_p(3p) = 1$.
Mais on peut aussi avoir $v_p(p^n+1) = 0$, $v_p(p^n-1) = 0$ et $v_p(p^n+1+p^n-1) = v_p(2p^n) \geqslant n$.

SOLUTION DE L'EXERCICE 15.23

Commençons par décomposer 2730 en produit de facteurs premiers.
Il est clairement divisible par 10, et 273 est divisible par 3.
Donc $2730 = 2 \times 3 \times 5 \times 91 = 2 \times 3 \times 5 \times 7 \times 13$.
Par le petit théorème de Fermat, on a, pour tout $a \in \mathbf{Z}$, $a^{13} \equiv a \quad [13]$.
De même, $a^7 \equiv a \quad [7]$ et donc $a^{13} = a^7a^6 \equiv aa^6 \equiv a^7 \equiv a \quad [7]$.
Toujours par le petit théorème de Fermat, $a^5 \equiv a \quad [5]$ et donc $a^{13} \equiv a^5a^5a^3 \equiv a^5 \equiv a \quad [5]$.
Enfin, $a^{13} \equiv \left(a^3\right)^4 a \equiv a^4a \equiv a^3a^2 \equiv a^3 \equiv a \quad [5]$.
Et pour 2, évitons le recours au petit théorème de Fermat : a^{13} et a ont la même parité, et donc $a^{13} - a$ est divisible par 2.
Ainsi, 2, 3, 5, 7 et 13 divisent tous $a^{13} - a$. Donc leur PPCM divise $a^{13} - a$.
S'agissant d'entiers premiers entre eux, car tous premiers et distincts, leur PPCM est égal à leur produit : $2730 \mid a^{13} - a$, soit $a^{13} \equiv a \quad [2730]$.

Parité
Notons que pour $p = 2$, le petit théorème de Fermat nous dit que $a^2 \equiv a \quad [2]$, c'est-à-dire que a^2 et a sont de même parité. Ce que vous savez depuis bien longtemps !

SOLUTION DE L'EXERCICE 15.24

Il s'agit donc de prouver que $pq \mid p^{q-1} + q^{p-1} - 1$.
Puisque p et q sont premiers entre eux, il suffit donc de prouver que $p^{q-1} + q^{p-1} - 1$ est divisible à la fois par p et par q.

Par le petit théorème de Fermat, on a donc $p^{q-1} \equiv 1 \quad [q]$ et $q^{p-1} \equiv 1 \quad [p]$.
Puisque $p^{q-1} \equiv 0 \quad [p]$, $p^{q-1} + q^{p-1} \equiv 1 \quad [p]$.
Donc $p \mid p^{q-1} + q^{p-1} - 1$.
De même, $q \mid p^{q-1} + q^{p-1} - 1 \quad [q]$.
Et donc $pq \mid p^{q-1} + q^{p-1} - 1$, de sorte que $p^{q-1} + q^{p-1} \equiv 1 \quad [pq]$.

SOLUTION DE L'EXERCICE 15.25

Par le petit théorème de Fermat, $2^4 \equiv 1 \quad [5]$. Par ailleurs, $2^3 \equiv 3 \quad [5]$ et donc $2^{4k+3} \equiv 3 \quad [5]$, de sorte que $5 \mid 2^{4k+3} - 3$.
De même, $2^{12} \equiv 1 \quad [13]$ et $2^4 \equiv 3 \quad [13]$, donc $2^{12k+4} \equiv 3 \quad [13]$, donc $13 \mid 2^{12k+4} \quad [13]$.

En revanche, $2^6 \equiv -1 \quad [65]$, donc $2^{12} \equiv 1 \quad [65]$.
Donc $2^{n+12} - 3 \equiv 2^n - 3 \quad [65]$. Autrement dit, la suite des restes de la division euclidienne de 2^n par 65 est périodique de période 12.
Il suffit donc de calculer les restes des divisions euclidiennes de $2^k - 3$ par 65 pour $k \in [\![0, 11]\!]$.

Les premières puissances de 2 modulo 65 sont 2, 4, 8, 16, 32, 64.
Or $2^6 = 64 \equiv -1 \quad [65]$.
Donc $2^7 \equiv -2 \quad [65]$, $2^8 \equiv -4, \ldots, 2^{11} \equiv -32 \quad [65]$, $2^{12} \equiv 1 \quad [65]$.
Et alors aucune de ces puissances n'est congrue à 3 modulo 65, si bien que $2^n - 3$ n'est jamais divisible par 65.

SOLUTION DE L'EXERCICE 15.26

Nous savons que tout diviseur de n s'écrit de manière unique $\prod_{i=1}^{k} p_i^{\beta_i}$, avec $0 \leqslant \beta_i \leqslant v_{p_i}(n)$, et qu'inversement, tout nombre de cette forme divise n.
Choisir un diviseur de n, c'est donc choisir les k entiers $\beta_1, \ldots, \beta_k$, avec pour tout i, $0 \leqslant \beta_i \leqslant v_{p_i}(n)$.
Le nombre β_1 peut donc prendre les valeurs $0, 1, \ldots, v_{p_1}(n)$, donc il y a $v_{p_1}(n) + 1$ choix possibles pour la valeur de β_1.
Puis, β_1 étant choisi, il y a $v_{p_2}(n) + 1$ choix possibles pour β_2, etc.
Soit un total de $\left(v_{p_1}(n)+1\right)\left(v_{p_2}(n)+1\right)\cdots\left(v_{p_k}(n)+1\right) = \prod_{i=1}^{k}\left(v_{p_i}(n)+1\right)$ diviseurs de n.

Produit
Le fait qu'on fasse un produit sera vraiment justifié plus tard dans l'année, mais cela doit vous sembler naturel.
Un exemple plus simple serait celui où vous avez le choix entre 3 langues et deux options (SI ou info).
Pour chacun des 3 choix de langue, il y a donc deux options, soit un total de 3×2 couplages langue/option.

SOLUTION DE L'EXERCICE 15.27

Il s'agit de remarquer qu'un entier k est une puissance $n^{\text{ème}}$ si et seulement si pour tout $p \in \mathcal{P}$, $v_p(k)$ est divisible par n.
En effet, si $k = c^n$, on a alors pour tout p premier, $v_p(k) = v_p(c^n) = v_p(c)$.
Et inversement, si pour tout p premier, $v_p(k) = nq_p$, alors

$$k = \prod_{p\in\mathcal{P}} p^{nq_k} = \left(\prod_{p\in\mathcal{P}} p^{q_p}\right)^n.$$

Si ab est une puissance $n^{\text{ème}}$, $ab = c^n$, alors on a $ab = \prod_{p\in\mathcal{P}} p^{nv_p(c)}$.
Soit encore, pour tout $p \in \mathcal{P}$, $v_p(ab) = nv_p(c) \Leftrightarrow v_p(a) + v_p(b) = nv_p(c)$.
Mais a et b étant premiers entre eux[7], pour tout $p \in \mathcal{P}$, $v_p(a) = 0$ ou $v_p(b) = 0$.
Si $v_p(a) = 0$, alors $v_p(a)$ est divisible par n, et $v_p(b) = nv_p(c)$ est divisible par n.
On conclut de même si $v_p(b) = 0$.
Donc pour tout $p \in \mathcal{P}$, $v_p(a)$ et $v_p(b)$ sont des multiples de n, donc a et b sont des puissances $n^{\text{èmes}}$.

[7] Et c'est ici qu'il s'agit d'une hypothèse fondamentale.

Et inversement, si $a = c^n$ et $b = d^n$ sont des puissances $n^{\text{èmes}}$, alors $ab = (cd)^n$ est une puissance $n^{\text{ème}}$.

Solution de l'exercice 15.28

Il s'agit donc de prouver que 100! s'écrit comme un nombre impair fois 2^{97}.
Soit encore que dans la décomposition de 100! en produit de facteurs premiers, 2 apparaît 97 fois. Ce qui signifie que $v_2(100!) = 97$.

Par définition, $100! = 1 \times 2 \times \cdots \times 98 \times 99 \times 100$.
Les facteurs 2 ne proviennent que des nombres pairs $2, 4, 6, \ldots, 98, 100$.
Autrement dit, puisque $1 \times 3 \times 5 \times \cdots \times 97 \times 99$ est impair,

$$v_2(100!) = v_2(2\times4\times\cdots\times98\times100) = v_2(2^{50}\times1\times2\times\cdots\times49\times50) = v_2(2^{50})+v_2(50!) = 50+v_2(50!).$$

De la même manière, $v_2(50!) = 25 + v_2(25!)$.
On a alors $v_2(25!) = v_2(2 \times 4 \times \cdots \times 22 \times 24) = 12 + v_2(12!)$.
Puis $v_2(12)! = 6 + v_2(6!)$.
Et un calcul direct[8] nous donne $v_2(6!) = v_2(2) + v_2(4) + v_2(6) = 4$.
Et donc enfin, $v_2(100!) = 50 + 25 + 12 + 6 + 4 = 97$, d'où le résultat annoncé.
Notons que nous n'avons pas déterminé la valeur de l'entier n, mais l'énoncé demandait juste de prouver son existence, pas de le calculer.

Si vraiment vous en voulez la valeur, $n = \frac{1}{2}\left(\frac{100!}{2^{97}} - 1\right)$...

[8] Ou une étape supplémentaire si le cœur vous en dit.

Plus généralement, il existe une formule pour la valuation p-adique d'une factorielle, due à Legendre, qui affirme que pour tout premier p,

$$v_p(n!) = \sum_{k=0}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Remarque
Cette somme ne comporte qu'un nombre fini de termes non nuls.

Solution de l'exercice 15.29

Notons $\alpha_n = \left(1+\sqrt{3}\right)^{2n+1}$.

1. En utilisant la formule du binôme, il vient

$$\begin{aligned}
\left(1+\sqrt{3}\right)^{2n+1} + \left(1-\sqrt{3}\right)^{2n+1} &= \sum_{k=0}^{2n+1}\binom{2n+1}{k}\sqrt{3}^k + \sum_{k=0}^{2n+1}\binom{2n+1}{k}\left(-\sqrt{3}\right)^k \\
&= \sum_{k=0}^{2n+1}\binom{2n+1}{k}\left(1+(-1)^k\right)\sqrt{3}^k \\
&= \sum_{\substack{k=0\\k\text{ pair}}}^{2n+1}\binom{2n+1}{k}2\sqrt{3}^k \\
&= \sum_{i=0}^{n}\binom{2n+1}{2i}2\cdot 3^i \in \mathbf{N}.
\end{aligned}$$

Si k est impair, $1 + (-1)^k = 0$.
Et si k pair, $1 + (-1)^k = 2$.

Donc déjà $(1+\sqrt{3})^{2n+1}+(1-\sqrt{3})^{2n+1}$ est un entier.
D'autre part, puisque $\sqrt{3}\in]1,2[$, $1-\sqrt{3}\in]-1,0[$, de sorte que $-1<(1-\sqrt{3})^{2n+1}<0$.
Et donc $(1+\sqrt{3})^{2n+1}+(1-\sqrt{3})^{2n+1}$ est un entier, avec

$$\alpha_n - 1 < \left(1+\sqrt{3}\right)^{2n+1} + \left(1-\sqrt{3}\right)^{2n+1} < \alpha_n.$$

Donc nécessairement, $\left(1+\sqrt{3}\right)^{2n+1}+\left(1-\sqrt{3}\right)^{2n+1} = \lfloor \alpha_n \rfloor = u_n$.

2. La formule prouvée ci-dessus nous donne

$$\begin{aligned} u_n &= (1+\sqrt{3})\left(\left(1+\sqrt{3}\right)^2\right)^n + (1-\sqrt{3})\left(\left(1-\sqrt{3}\right)^2\right)^n \\ &= \left(1+\sqrt{3}\right)\left(4+2\sqrt{3}\right)^n + \left(1-\sqrt{3}\right)\left(4-2\sqrt{3}\right)^n \\ &= 2^n\left[\left(1+\sqrt{3}\right)\left(2+\sqrt{3}\right)^n + \left(1-\sqrt{3}\right)\left(2-\sqrt{3}\right)^n\right] \end{aligned}$$

On a donc $v_2(u_n) = n + v_2\left(\left[\left(1+\sqrt{3}\right)\left(2+\sqrt{3}\right)^n + \left(1-\sqrt{3}\right)\left(2-\sqrt{3}\right)^n\right]\right)$.
On a alors

$$\left(1+\sqrt{3}\right)\left(2+\sqrt{3}\right)^n + \left(1-\sqrt{3}\right)\left(2-\sqrt{3}\right)^n = \underbrace{\left(2+\sqrt{3}\right)^n + \left(2-\sqrt{3}\right)^n}_{=v_n} + \underbrace{\sqrt{3}\left[\left(2+\sqrt{3}\right)^n - \left(2-\sqrt{3}\right)^n\right]}_{=w_n}.$$

De nouveau avec le binôme, on a

$$v_n = 2\sum_{\substack{k=0\\ k \text{ pair}}}^{n} \binom{n}{k}\sqrt{3}^k 2^{n-k} = 2\sum_{i=0}^{\lfloor n/2\rfloor}\binom{n}{2i}3^i 2^{n-2i}.$$

Il est clair qu'il s'agit là d'un entier pair.
► Si n est pair, alors tous les termes de la somme sont divisibles par 2, sauf le dernier qui est $\binom{n}{n}3^{n/2}2^{n-n}$.
Donc v_n est divisible par 2, mais pas par 4, donc $v_2(v_n)=1$.
► En revanche, si n est impair, alors tous les termes de la somme sont divisibles par 2, y compris le dernier qui est cette fois $\binom{n}{n-1}3^{(n-1)/2}2^{n-(n-1)} = n3^{(n-1)/2}2$.
Non seulement ce terme est pair, mais en plus il n'est pas divisible par 4 car n est impair.
Tous les autres termes de la somme étant divisibles par 4, on en déduit que $v_2(v_n)=2$.
Pour le dire autrement, on a $v_n \equiv 2 \pmod 4$ si n est pair et $v_n \equiv 0 \pmod 4$ si n est impair.

Sur le même principe, on a

$$w_n = 2\sqrt{3}\sum_{\substack{k=0\\ k \text{ impair}}}^{n}\binom{n}{k}\sqrt{3}^k 2^{n-k} = 2\sqrt{3}\sum_{i=0}^{\lfloor (n-1)/2\rfloor}\binom{n}{2i+1}\sqrt{3}^{2i+1}2^{n-2i-1} = 2\cdot 3\sum_{i=0}^{\lfloor (n-1)/2\rfloor}\binom{n}{2i+1}3^i 2^{n-2i-1}.$$

Comme pour v_n, on prouve que $v_2(w_n)=2$ si n est pair et $v_2(w_n)=1$ si n est impair.
Autrement dit, que $w_n \equiv 0 \pmod 4$ si n est pair et $w_n \equiv 2 \pmod 4$ si n est impair.

Donc dans tous les cas, $v_n + w_n \equiv 2 \pmod 4$, ce qui signifie que $v_2(v_n+w_n)=1$: il s'agit d'un nombre divisible par 2 et pas par 4.
Et donc au final, on a $v_2(u_n) = n + v_2(v_n+w_n) = n+1$.

Alternative
On peut utiliser le résultat de l'exercice 22, en notant que $v_2(v_n)\neq v_2(w_n)$ et donc
$v_2(v_n+w_n) = \min(v_2(v_n), v_2(w_n)) = 1$.

SOLUTION DE L'EXERCICE 15.30

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 $(u,v)\in\mathbf{Z}^2$ 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 $1\leqslant b\leqslant p-1$. Il vient donc $xu+pv = xb+p(ax+v)=1$ et par conséquent $xu\equiv 1 \quad [p]$.
Ceci prouve donc l'existence demandée.

$b\neq 0$
Nous venons de dire que u n'est pas divisible par p, donc $b\neq 0$.

Passons à l'unicité, et supposons qu'il existe deux entiers y_1 et y_2 dans $[\![1, p-1]\!]$ tels que $xy_1 \equiv xy_2 \quad [p]$.
Alors $x(y_1 - y_2) \equiv 0 \quad [p]$ 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, $-(p-2) \leqslant y_1 - y_2 \leqslant p-2$, 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 $xy \equiv 1 \quad [p]$.

1.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 $ky \equiv 1 \quad [p]$.
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 $k^2 \equiv 1 \quad [p]$.
Mais $k^2 \equiv 1 \quad [p] \Leftrightarrow k^2 - 1 \equiv 0 \quad [p] \Leftrightarrow p \mid k^2 - 1$.
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

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

2. Supposons donc que $(n-1)! \equiv -1 \quad [n]$.
Alors il existe $k \in \mathbf{Z}$ 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.

Commentaires *: si on sait que $\mathbf{Z}/p\mathbf{Z}$ est un corps, la première partie est évidente : tout élément non nul possède un unique inverse.*
Et alors le regroupement des termes deux par deux dans la question 1.b. revient à regrouper chaque élément avec son inverse, ce qui n'est possible que pour ceux qui ne sont pas égaux à leur propre inverse modulo p.

Solution de l'exercice 15.31

Notons tout de suite qu'il y a un cas trivial : celui où $m = n = 1$, où alors $H_{m,n} = 1 \in \mathbf{N}$.
Nous allons prouver qu'il s'agit de la seule solution.
Dans la suite, on suppose donc $n \geqslant 2$. Puisque $\frac{1}{n}$ n'est pas un entier, on peut également supposer $m < n$.
Comme indiqué, nous allons donc nous intéresser aux valuations 2-adiques des $k \in [\![m, n]\!]$.
Plus précisément, notons α la plus grande de ces valuations, c'est-à-dire $\alpha = \max\{v_2(k),\ m \leqslant k \neq n\}$.
Notons que $\alpha \geqslant 1$, puisque m étant différent de n, il existe au moins un entier pair entre m et n.
Alors cette valuation n'est atteinte qu'une seule fois : il existe un unique $k \in [\![m, n]\!]$ tel que $v_2(k) = \alpha$.
En effet, supposons par l'absurde qu'il existe deux tels entiers $k < k'$.
Alors $k + 2^\alpha$, qui est le multiple de 2^α immédiatement supérieur à k est également entre m et n (il est inférieur ou égal à k').

Mais puisque $k = 2^\alpha p$, avec p impair, $k + 2^\alpha = 2^\alpha(p+1) = 2^{\alpha+1}\dfrac{p+1}{2}$, qui possède une valuation 2-adique supérieure ou égale à $\alpha + 1$.

> **Explications**
> De deux multiples successifs de 2^α, l'un des deux est un multiple de $2^{\alpha+1}$.
> Cela généralise un résultat bien connu : de deux nombres pairs successifs, l'un est multiple de 4.

Notons alors $p = 2^\alpha q$, avec q impair, le PPCM des entiers de $[\![m, n]\!]$. Notons également ℓ l'unique entier de $[\![m, n]\!]$ tel que $v_2(\ell) = \alpha$.
Et pour tout $k \in [\![m, n]\!]$, notons a_k l'entier tel que $\frac{1}{k} = \frac{a_k}{p} \Leftrightarrow ka_k = p$.
Alors pour $k \neq \ell$, puisque $v_2(k) < \alpha$, $v_2(a_k) \geqslant 1$, donc a_k est pair.
En revanche, $v_2(a_\ell) = 0$, et donc a_ℓ est impair.
Et alors $H_{m,n} = \dfrac{1}{p}\displaystyle\sum_{k=m}^{n} a_k = \dfrac{1}{2^\alpha q}\sum_{k=m}^{n} a_k$.

Puisque $\sum_{k=m}^{n} a_k$ est impair, p ne divise pas $\sum_{k=m}^{n} a_k$, et donc $H_{m,n}$ n'est pas entier.

SOLUTION DE L'EXERCICE 15.32

1. Nous savons que $\langle\overline{1}\rangle = \left\{k\langle\overline{1}\rangle,\ k \in \mathbf{Z}\right\}$, où pour $k \geqslant 1$, $k\overline{1} = \overline{1} + \overline{1} + \cdots + \overline{1} = \overline{k}$.
Et donc en particulier, pour $k \in [\![1, n]\!]$, $\overline{k} \in \langle\overline{1}\rangle$.
Puisque $\mathbf{Z}/n\mathbf{Z} = \{\overline{k}, 1 \leqslant k \leqslant n\}$, on a donc $\mathbf{Z}/n\mathbf{Z} \subset \langle\overline{1}\rangle$, et l'inclusion réciproque étant évidente, on a égalité.

2. Soient a, a' deux représentants de la même classe de congruence modulo n.
Alors il existe $k \in \mathbf{Z}$ tel que $a' = a + nk$. Mais alors, par le lemme d'Euclide, $a \wedge n = a' \wedge n$.

Par Bézout, il existe $u, v \in \mathbf{Z}$ tels que $au + bv = d$, et donc $\overline{d} = \overline{au} = u\overline{a} \in \langle\overline{a}\rangle$.
Donc déjà $\langle\overline{d}\rangle \subset \langle\overline{a}\rangle$.
Inversement, il existe $a' \in \mathbf{Z}$ tel que $a = da'$, et donc $\overline{a} = \overline{da'} = a'\overline{d} \in \overline{d}$, donc $\langle\overline{a}\rangle \subset \langle\overline{d}\rangle$.
Donc $\langle\overline{a}\rangle = \langle\overline{d}\rangle$.

> **Rappel**
> Le groupe engendré par $\overline{d}$ est inclus dans tout sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ contenant $\overline{d}$.

Pour le cardinal de $\langle d\rangle$, notons simplement que $\frac{n}{d}d = n$, et donc $\frac{n}{d}\overline{d} = \overline{n} = \overline{0}$.
Et pour $0 \leqslant k < \frac{n}{d}$, alors $0 \leqslant kd < n$, donc les $k\overline{d}$ sont deux à deux distincts. Donc déjà $\langle\overline{d}\rangle$ est de cardinal supérieur ou égal à $\frac{n}{d}$.
Par ailleurs, pour $k \in \mathbf{Z}$, si $k = \frac{n}{d}q + r$ est la division euclidienne de k par $\frac{n}{d}$, alors $kd = nq + dr$ et donc $k\overline{d} = r\overline{d}$, avec $0 \leqslant r < \frac{n}{d}$.
Et donc $\langle\overline{d}\rangle = \left\{k\overline{d}, 0 \leqslant k < \frac{n}{d}\right\}$ est donc de cardinal $\frac{n}{d}$.