Le Grand Théorème de Fermat
Livre 01 - Théorie des Nombres Classique
Version 2.0

Pascal Picard*

18 janvier 2010

*Je suis grand amateur de Mathématiques et de Physique Théorique, convaincu que ces sciences sont accessibles à tous, à condition de les expliquer progressivement et méthodiquement, et de les introduire par les prérequis nécessaires. Depuis quelques années, je m'attèle à écrire des textes théoriques sous forme de pièces de théâtre. Trois personnages y bavardent : Béatrix est la Candide, c'est elle qui pose les questions ; Euristide est un peu philosophe, un peu physicien, il est l'intuitif du groupe ; Mathine est notre mathématicienne, c'est elle qui présente les calculs et les démonstrations. Ces textes sont mis à disposition gratuitement sur Internet, parce que j'aime ça. Le prérequis pour la lecture des documents, quelque complexes qu'ils soient, est le programme de Terminale S en France.

à Pascale, Marine et Morgane

Remerciements... Ce document est en phase de relecture. Les relecteurs motivés recevront mes remerciements chaleureux.

Table des matières

Table des figures

Résumé

`BEATRIX` : J'aime beaucoup la théorie des nombres classiques. C'est une discipline très pure... Des nombres, rien que des nombres...

`EURISTIDE` : C'est vrai. C'est une belle théorie, et ses applications sont très nombreuses. Au quotidien d'abord, puisque nous manipulons les nombres, les opérations, les divisions chaque jour de notre vie, sans y réfléchir. Les nombres premiers, un des piliers de la théorie des nombres, sont d'une grande utilité lorsqu'il s'agit de faire de la cryptographie ; en effet, il est impossible pour un ordinateur même très puissant, de déterminer si un très grand nombre (plusieurs dizaines de chiffres, par exemple) est un nombre premier ou s'il est le facteur de plusieurs nombres premiers. Cette difficulté est un aubaine pour la plupart des systèmes de cryptographie, permettant de coder des mots de passe ou des informations secrètes, en ne laissant aucune chance à un ordinateur même très puissant de trouver le code.

`MATHINE` : Et la théorie des nombres possède une place de choix dans la génèse des mathématiques ; c'est un peu la théorie originelle, à partir de laquelle les mathématiques se sont construites.

1 Acte I - Introduction

EURISTIDE : La théorie des nombres classique constitue un peu les fondements de la théorie des nombres, et donc constitue la matériel de base qu'il faut connaître avant d'aborder des problèmes complexes tels que le théorème de Fermat-Wiles.
Nous aborderons d'abord dans ce livre quelques nombres particuliers appelés nombres figurés, à titre d'illustration initiale du monde passionnant des nombres entiers. Puis nous traiterons des propriétés de la division et de la divisibilité des nombres, ce qui nous conduira aux nombres premiers. Nous étendrons ensuite notre découverte des propriétés de divisibilité en étudiant les congruences. Puis nous étudierons les équations diophantiennes qui sont des équations en nombres entiers, pour aborder ensuite la réciprocité quadratique, théorie de base permettant la résolution d'équations de congruence du second degré. Nous finirons par la présentation d'un certain nombre de fonctions utilisées régulièrement en théorie des nombres classiques.

BEATRIX : Je vois en effet que c'est un beau panorama de la théorie des nombres.

2 Acte II - Nombres particuliers

2.1 Scène II.1 - Nombres figurés

EURISTIDE : Commençons donc par présenter des nombres particuliers qui nous seront utiles à titre d'introduction de la théorie des nombres classique.

MATHINE : Nous allons commencer par les nombres triangulaires :

Définition **2.1.1**
Nombre triangulaire
On appelle nombre triangulaire , la somme des n entiers consécutifs, en commençant à l'unité :

$$T_n = 1 + 2 + \ldots + (n-1) + n. \tag{1}$$

BEATRIX : Pourquoi appelle-t-on ces nombres triangulaires ?

EURISTIDE : Tu vas comprendre tout de suite. Il suffit de les dessiner comme ceci :

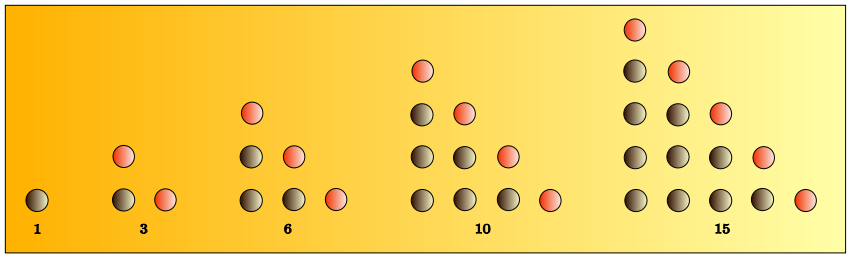

Fig. 1 - Nombres triangulaires

MATHINE : Voici la formule permettant de calculer un nombre triangulaire :

Proposition **2.1.1**
Expression nombre triangulaire
Le n-ième nombre triangulaire (cf. 2.1.1) s'écrit :

$$T_n = \frac{n(n+1)}{2}. \tag{2}$$

Démonstration :

Soit T_n le n-ième nombre triangulaire. Ecrivons T_n sous deux formes différentes :

$$\begin{array}{ccccccccc} 1 & + & 2 & + & \ldots & + & (n-1) & + & n \\ n & + & (n-1) & + & \ldots & + & 2 & & 1. \end{array} \tag{3}$$

En additionnant terme à terme ces deux expressions, on obtient la somme :

$$(n+1) + (2+n-1) + \ldots + (2+n-1) + (n+1), \tag{4}$$

c'est-à-dire :

$$\underbrace{(n+1) + (n+1) + \ldots + (n+1) + (n+1)}_{n \quad \text{fois}} \tag{5}$$

Par construction, cette somme vaut 2 fois le nombre T_n. Donc :

$$2T_n = n(n+1). \tag{6}$$

Donc :

$$T_n = \frac{n(n+1)}{2}. \tag{7}$$

C.Q.F.D.

BEATRIX : Wahoo !

EURISTIDE : Oui, admire la beauté de cette démonstration. Simple. Pure. Efficace. Astucieuse. J'aime ces mathématiques là
On dit que n est la racine triangulaire du nombre T_n. Nous verrons dans quelques instants pourquoi.

BEATRIX : On peut comprendre la démonstration de façon géométrique aussi. Si je reprends la représentation géométrique des nombres triangulaires, pour $n = 3$ par exemple :

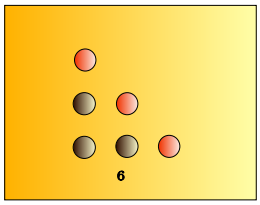

Fig. 2 - Nombre triangulaire de base 3

et que je superpose deux de ces représentations tête-bêche, j'obtiens :

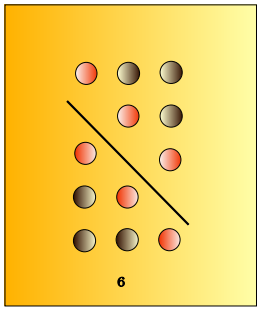

Fig. 3 - Nombres triangulaires tête-bêche

qui comporte $3 \times 4 = n(n+1)$ points. On retrouve le nombre triangulaire en divisant par 2, puisque nous l'avons représenté deux fois dans ce schéma.

EURISTIDE : Bravo, Béatrix !

MATHINE : Nous allons maintenant aborder les nombres carrés.

Définition **2.1.2**
Nombre carré
On appelle nombre carré C_n la somme des n premiers entiers impairs.

BEATRIX : Pourquoi appelle-t-on ces nombres "carrés" ?

EURISTIDE : Nous allons le voir quand nous aurons vu la proposition suivante. Mathine, sais-tu nous donner l'expression de C_n ?

MATHINE : Oui, bien sûr. La voici :

Proposition **2.1.2**
Expression nombre carré
Le n-ième nombre carré (cf. 2.1.2) C_n s'écrit :

$$C_n = n^2. \tag{8}$$

BEATRIX : Ah, d'accord ! Effectivement, je comprends qu'on les appelle des nombre carrés, puisque ce sont justement des carrés parfaits.

EURISTIDE : Le terme carré provient d'ailleurs de ce que n^2 représente la surface d'un carré dont le côté vaut n (centimètres par exemple.)

MATHINE : La démonstration fait appel à la même technique que précédemment.

Démonstration :

Soit C_n le n-ième nombre carré. Nous écrivons C_n sous deux formes différentes :

$$\begin{array}{rcccccccccc} C_n & = & 1 & + & 3 & + & \ldots & + & (2n-3) & + & (2n-1) \\ C_n & = & (2n-1) & + & (2n-3) & + & \ldots & + & 3 & + & 1. \end{array} \tag{9}$$

En ajoutant terme à terme ces deux égalités, nous obtenons :

$$2C_n = (1+2n-1) + (3+2n-3) + \ldots + (2n-3+3) + (2n-1+1), \tag{10}$$

soit :

$$2C_n = \underbrace{2n + 2n + \ldots + 2n + 2n}_{n \quad \text{fois}}. \tag{11}$$

Donc :

$$2C_n = n \times 2n. \tag{12}$$

D'où :

$$C_n = n^2. \tag{13}$$

C.Q.F.D.

EURISTIDE : On peut aussi illustrer leur appellation par le dessin suivant :

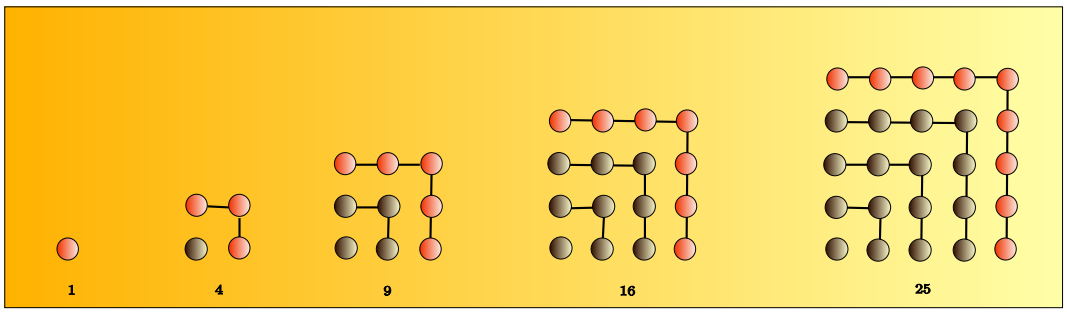

Fig. 4 - Nombres carrés

BEATRIX : Cette représentation nous permet de comprendre immédiatement la formule n^2 pour ces nombres. Peut-on imaginer d'autres nombres ? Des nombres pentagonaux ? Hexagonaux ?

EURISTIDE : Oui, bien sûr. Mathine va nous expliquer cela.

MATHINE : Oui, voici la définition d'un nombre pentagonal :

Définition **2.1.3**
Nombre pentagonal
On appelle nombre pentagonal P_n la somme des n premiers termes d'une suite d'entiers espacés de 3.

$$P_n = 1 + 4 + \ldots + 3(n-1) - 2 + 2n - 2. \tag{14}$$

Proposition **2.1.3**
Expression nombre pentagonal
Le n-ième nombre pentagonal (cf. 2.1.3) P_n s'écrit :

$$P_n = \frac{n(3n-1)}{2}. \tag{15}$$

EURISTIDE : La démonstration, dorénavant classique pour nous, fait toujours appel à la même astuce.

MATHINE : Effectivement, nous allons employer la technique de la sommation des deux formes d'expression du nombre pentagonal :

Démonstration :

Soit P_n le n-ième nombre pentagonal. Nous écrivons P_n sous deux formes différentes :

$$\begin{array}{rcccccccccc} P_n & = & 1 & + & 4 & + & \ldots & + & 3(n-1)-2 & + & 3n-2 \\ P_n & = & 3n-2 & + & 3(n-1)-2 & + & \ldots & + & 4 & + & 1. \end{array} \tag{16}$$

Additionnons terme à terme ces deux égalités :

$$2P_n = (1+3n-2)+(4+3(n-1)-2)+\ldots+(3(n-1)-2+4)+(2n-2+1). \tag{17}$$

Soit :

$$2P_n = \underbrace{(3n-1)+(3n-1)+(3n-1)+\ldots+(3n-1)+(3n-1)}_{n \quad \text{fois}}. \tag{18}$$

Donc :

$$2P_n = n \times (3n-1), \tag{19}$$

d'où :

$$P_n = \frac{n(3n-1)}{2}. \tag{20}$$

C.Q.F.D.

BEATRIX : Et j'imagine qu'on les appelle pentagonaux parce qu'on peut les illustrer par des pentagones...

EURISTIDE : En effet :

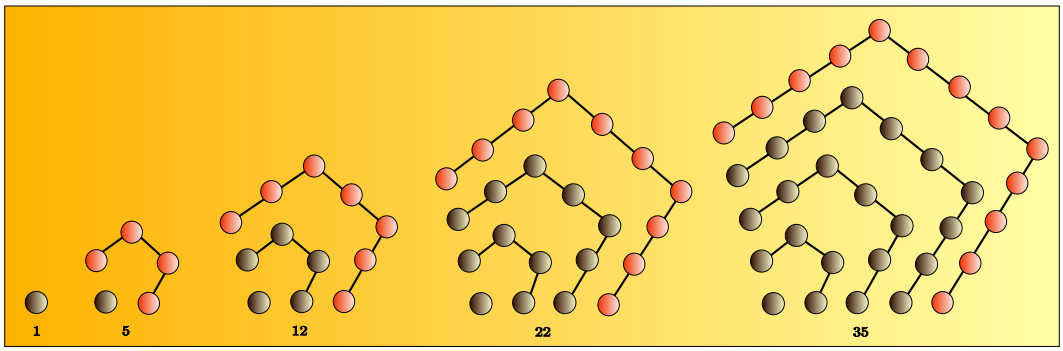

Fig. 5 - Nombres pentagonaux

BEATRIX : Et les nombres hexagonaux ?

MATHINE : En voici la définition :

Définition **2.1.4**
Nombre hexagonal
On appelle nombre hexagonal H_n la somme des n premiers termes d'une suite d'entiers espacés de 4 :

$$H_n = 1 + 5 + 9 + \ldots + (4(n-2) - 3) + (4(n-1) - 3) + (4n - 3). \tag{21}$$

On dit d'une telle suite que c'est une progression arithmétique de premier terme 1 et de raison 4.

BEATRIX : Qu'est-ce qu'une progression arithmétique en général ?

MATHINE : La progression arithmétique est définie comme suit :

Définition **2.1.5**
Progression arithmétique
On appelle progression arithmétique de premier terme a et de raison r, une suite d'entiers A_n de la forme :

$$A_n = a + nr. \tag{22}$$

BEATRIX : D'accord. Et quelle est alors l'expression d'un nombre hexagonal ?

MATHINE : Voici la formule permettant de calculer un nombre hexagonal :

Proposition **2.1.4**
Expression nombre hexagonal
Le n-ième nombre hexagonal H_n s'écrit :

$$H_n = n(2n - 1). \tag{23}$$

Démonstration :

Soit H_n le n-ième nombre hexagonal.

$$\begin{array}{rcccccccccc} H_n & = & 1 & + & 5 & + & \ldots & + & (4(n-1)-3) & + & (4n-3) \\ H_n & = & (4n-3) & + & (4(n-1)-3) & + & \ldots & + & 5 & + & 1. \end{array} \tag{24}$$

D'où :

$$2H_n = (4n-3+1) + (4(n-1)-3+5) + \ldots + 4(n-1)-3+5) + (4n-3+1), \tag{25}$$

soit :

$$2H_n = \underbrace{(4n-2) + (4n-2) + (4n-2) + \ldots + (4n-2) + (4n-2) + (4n-2)}_{n \quad \text{fois}}. \tag{26}$$

D'où :

$$H_n = \frac{n \times (4n-2)}{2} = n(2n-1). \tag{27}$$

C.Q.F.D.

BEATRIX : Alors, laissez-moi deviner comment nous pouvons ilustrer ces nombres hexagonaux. Je fais grandir un hexagone de points autour du point 1 :

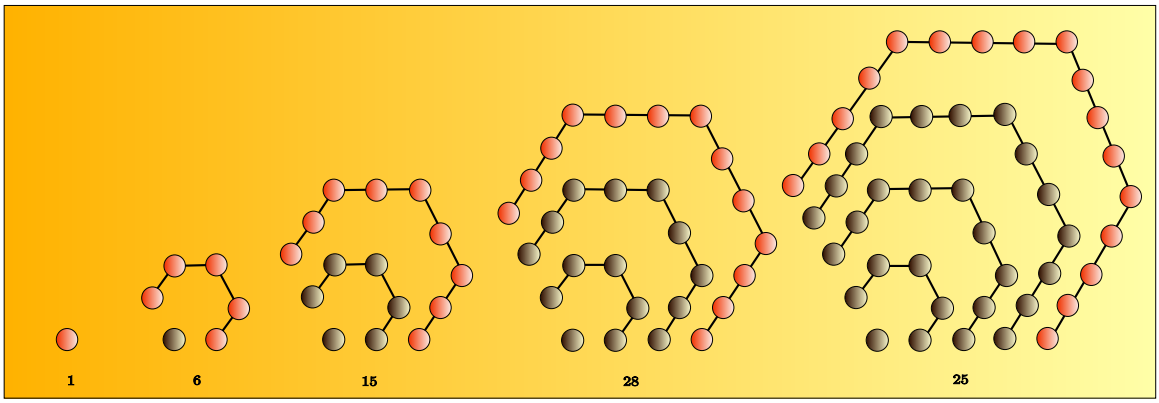

Fig. 6 - Nombres hexagonaux

EURISTIDE : Et voilà ! Tu as compris le principe.

BEATRIX : Nous avons parlé tout à l'heure de progression arithmétique. Je suppose qu'en utilisant la même méthode, nous pourrions généraliser et obtenir l'expression de la somme des n premiers termes d'une progression arithmétique.

EURISTIDE : En effet. Et Mathine va nous le montrer.

MATHINE : Avec plaisir :

Proposition **2.1.5**
Expression somme progression arithmétique
La somme des n premiers termes de la progression arithmétique de premier terme a et de raison r s'écrit :

$$S_n = \frac{n(2a+nr)}{2}. \tag{28}$$

Démonstration :

Soit S_n la somme des n premiers termes de la progression arithmétique (cf. 2.1.5) de premier terme a et de raison (cf. 2.1.5) r. Alors :

$$\begin{array}{rcccccccccc} S_n & = & a & + & a+r & + & \ldots & + & a+(n-1)r & + & a+nr \\ S_n & = & a+nr & + & a+(n-1)r & + & \ldots & + & a+r & + & a. \end{array} \tag{29}$$

Alors :

$$2S_n = \underbrace{(2a+nr)+(2a+nr)+\ldots+(2a+nr)+(2a+nr)}_{n \quad \text{fois}}. \tag{30}$$

D'où :

$$S_n = \frac{n(2a+nr)}{2}. \tag{31}$$

C.Q.F.D.

EURISTIDE : Voilà, nous avons vu quelques nombres polygonaux. Comme nous le savons, les polygones sont des figures dans l'espace à 2 dimensions. Immédiatement, nous avons envie de savoir s'il existe des nombres figurés dans l'espace à 3 dimensions.

BEATRIX : Et je parierais que la réponse est oui.

EURISTIDE : Pari gagné. Mathine va donc nous initier aux nombres pyramidaux.

MATHINE : Voici la définition d'un nombre pyramidal :

Définition **2.1.6**
Nombre pyramidal
On appelle nombre pyramidal de racine n, la somme des n premiers nombres triangulaires (cf. 2.1.1) :

$$\Pi_n = 1+3+6+\ldots+\frac{n(n+1)}{2}. \tag{32}$$

EURISTIDE : Et voici notre objet en dimension 3, la pyramide étant constituée d'un empilage de triangles.

MATHINE : Le nombre pyramidal s'exprime comme suit :

Proposition **2.1.6**
Expression nombre pyramidal
Le nombre pyramidal (cf. 2.1.6) de racine n s'écrit :

$$\Pi_n = \frac{n(n+1)(n+2)}{6} \tag{33}$$

EURISTIDE : Nous allons maintenant étrenner une nouvelle technique de démonstration : il s'agit de l'induction complète ou démonstration par récurrence, consistant à démontrer une propriété, pour tout entier, en prouvant d'abord que la propriété est vraie pour $n = 1$; puis en prouvant que si la propriété est vraie pour un entier n, alors elle est nécessairement vraie pour l'entier $n+1$. On dit que la loi est héréditaire. Nous en déduisons que la loi est vraie pour $n = 1$, donc pour $n = 2$, donc pour $n = 3$, et ainsi de suite pour tout entier n.

BEATRIX : C'est une méthode élégante, et qui doit être très utile en théorie des nombres, où l'on manipule souvent des entiers ou des propriétés dépendant d'un entier.

MATHINE : Voici donc la démonstration par récurrence de l'expression d'un nombre pyramidal :

Démonstration :

Soit Π_n le nombre pyramidal de racine n.
Montrons que :

$$\Pi_n = \frac{n(n+1)(n+2)}{6}. \tag{34}$$

1) Montrons que l'expression est vraie pour $n = 1$.
Le calcul direct, à partir du premier nombre triangulaire, 1, donne :

$$\Pi_1 = 1. \tag{35}$$

Le calcul de l'expression donne :

$$\begin{aligned} \Pi_1 &= \frac{1(1+1)(1+2)}{6} && (36)\\ &= \frac{2\times 3}{6} && (37)\\ &= 1. && (38) \end{aligned}$$

Donc, l'expression est bien vérifiée pour $n = 1$.

2) Supposons maintenant que l'expression est vérifiée pour un entier n donné. On a :

$$\Pi_n = \frac{n(n+1)(n+2)}{6}. \tag{39}$$

Calculons Π_{n+1}. Par définition, le nombre pyramidal de racine $n+1$ est obtenu en ajoutant le nombre triangulaire de racine $n+1$ au nombre pyramidal de racine n :

$$\begin{aligned}
\Pi_{n+1} &= \Pi_n + T_{n+1} && (40)\\
&= \frac{n(n+1)(n+2)}{6} + \frac{(n+1)(n+2)}{2} && (41)\\
&= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{6} && (42)\\
&= \frac{(n+1)(n+2)(n+3)}{6}. && (43)
\end{aligned}$$

Expression que nous pouvons réécrire :

$$\Pi_{n+1} = \frac{(n+1)((n+1)+1)((n+1)+2)}{6}. \tag{44}$$

Donc, l'expression est bien vérifiée pour $n+1$.

3) Nous avons donc vérifié que l'expression est vraie pour $n = 1$, et qu'elle est vraie pour $n+1$ si elle est vraie pour n. Donc, d'après le principe de récurrence, l'expression est vérifiée pour tout entier n.

C.Q.F.D.

2.2 Scène II.2 - Triangle arithmétique

EURISTIDE : Une application intéressante des nombres entiers naturels, des nombres triangulaires et pyramidaux se trouve dans le célèbre triangle de Pascal, étudié au XVIIème siècle par Blaise Pascal.

BEATRIX : Qu'est-ce que le triangle de Pascal ?

EURISTIDE : C'est une sorte de curiosité mathématique. Mathine, peux-tu nous en parler ?

MATHINE : Bien sûr :

Définition **2.2.1**
Triangle de Pascal
Le triangle de Pascal est un triangle de nombres entiers tel que chaque entier y est obtenu en ajoutant le nombre qui le précède dans sa colonne au nombre qui précède celui-ci dans sa propre ligne. On commence

la suite de nombres du triangle par l'entier 1.

$$
\begin{array}{ccccccccc}
1 & & & & & & & & \\
1 & 1 & & & & & & & \\
1 & 2 & 1 & & & & & & \\
1 & 3 & 3 & 1 & & & & & \\
1 & 4 & 6 & 4 & 1 & & & & \\
1 & 5 & 10 & 10 & 5 & 1 & & & \\
1 & 6 & 15 & 20 & 15 & 6 & 1 & & \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 & \\
1 & .. & .. & .. & .. & .. & .. & .. & ...
\end{array}
\tag{45}
$$

EURISTIDE : Nous allons voir que ce triangle permet de calculer le nombre de combinaisons possibles pour ranger n objets dans un paquet de p objets.

MATHINE : Nous allons commencer par définir la factorielle, dont nous aurons besoin régulièrement par la suite.

Définition **2.2.2**
Factorielle
La factorielle d'un entier n, notée $n!$ est le produit des n premiers entiers :

$$n! = 1 \times 2 \times 3 \times \ldots \times n. \tag{46}$$

Par convention :

$$0! = 1. \tag{47}$$

EURISTIDE : Ainsi, par exemple :

$$1! = 1 \tag{48}$$
$$2! = 1 \times 2 = 2 \tag{49}$$
$$3! = 1 \times 2 \times 3 = 6 \tag{50}$$
$$4! = 1 \times 2 \times 3 \times 4 = 24 \tag{51}$$
$$5! = 1 \times 2 \times 3 \times 4 \times 5 = 120 \tag{52}$$
$$6! = \ldots\ldots\ldots\ldots \tag{53}$$

BEATRIX : Dès que n grandit, $n!$ devient faramineux, je pense. Essayons avec 10 :

$$10! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 = 3628800. \tag{54}$$

Ah oui, cela est déjà honorable.
Essayons avec 29 :

$$29! = 1 \times 2 \times \ldots \times 28 \times 29 = 8841761993739701954543616000000. \tag{55}$$

Impressionnant !

MATHINE : Nous allons maintenant utiliser la factorielle pour déterminer les entiers qui se trouvent dans le triangle de Pascal :

Théorème **2.2.1**
Expression triangle de Pascal
Considérons le triangle de Pascal. Numérotons la première ligne avec l'indice 0, et les lignes suivantes 1, 2, 3, etc. Numérotons la première colonne (qui ne comprend que des 1) avec l'exposant 0, et les colonnes suivantes 1, 2, 3, etc. Nous noterons C_i^j l'élément du triangle de Pascal qui se trouve à la ligne i et à la colonne j. Alors :

$$C_i^j = \frac{i!}{j!(i-j)!} \tag{56}$$

EURISTIDE : C'est une jolie formule bien symétrique. Nous allons utiliser de nouveau la démonstration par récurrence.

MATHINE : Voici la démonstration de ce théorème exprimant les coefficients du triangle de Pascal :

Démonstration :

Utilisons donc la démonstration par récurrence. Il s'agira cette fois d'une double récurrence sur les indices i et j. Donc, la démonstration va être un peu plus complexe.

1) Montrons la propriété pour $i = 0$ et $j = 0$.
Nous lisons dans le triangle de Pascal que :

$$C_0^0 = 1. \tag{57}$$

Et le calcul de l'expression donne :

$$C_0^0 = \frac{0!}{0!(0-0)!} = 1. \tag{58}$$

Donc, la propriété est vraie pour $i = j = 0$.
De la même façon, montrons la propriété pour $i = 0, j = 1$:

$$C_0^1 = 1 = \frac{0!}{1!1!} = 1. \tag{59}$$

Montrons la propriété pour $i = 1, j = 0$:

$$C_1^0 = 1 = \frac{1!}{0!1!} = 1, \tag{60}$$

et pour $i = 1, j = 1$:

$$C_1^1 = 1 = \frac{1!}{1!0!} = 1. \tag{61}$$

2) Fixons i tel que la propriété est vérifiée pour i et $i - 1$ et tous les j. Supposons de plus que la propriété

est vraie pour tous les entiers inférieurs ou égaux à un j donné.
Alors :

$$C_i^j = \frac{i!}{j!(i-j)!}; \tag{62}$$

$$C_{i-1}^{j+1} = \frac{(i-1)!}{(j+1)!(i-j-2)!}; \tag{63}$$

$$C_{i-1}^{j} = \frac{(i-1)!}{j!(i-j-1)!}. \tag{64}$$

Par définition du triangle de Pascal (cf. 2.2.1), nous savons que chaque entier y est obtenu en ajoutant le nombre qui le précède dans sa colonne au nombre qui précède celui-ci dans sa propre ligne. Donc :

$$C_i^{j+1} = C_{i-1}^{j+1} + C_{i-1}^{j}. \tag{65}$$

Alors :

$$C_i^{j+1} = \frac{(i-1)!}{(j+1)!(i-j-2)!} + \frac{(i-1)!}{j!(i-j-1)!} \tag{66}$$

$$= \frac{(i-1)!(i-j-1)+(i-1)!(j+1)}{(j+1)!(i-j-1)!} \tag{67}$$

$$= \frac{(i-1)!i}{(j+1)!(i-(j+1))!} \tag{68}$$

$$= \frac{i!}{(j+1)!(i-(j+1))!}. \tag{69}$$

Donc, sous cette forme, nous confirmons que l'expression est bien vérifiée pour $j+1$.

3) Fixons maintenant j tel que la propriété est vérifiée pour j et pour tout i. Et supposons en outre que la propriété est vraie pour tous les entiers inférieurs ou égaux à un i donné.
Alors :

$$C_i^j = \frac{i!}{j!(i-j)!}; \tag{70}$$

$$C_i^{j-1} = \frac{i!}{(j-1)!(i-j+1)!}. \tag{71}$$

Par définition du triangle de Pascal, nous savons que :

$$C_{i+1}^j = C_i^j + C_i^{j-1}. \tag{72}$$

Alors :

$$C_{i+1}^j = \frac{i!}{j!(i-j)!} + \frac{i!}{(j-1)!(i-j+1)!} \tag{73}$$

$$= \frac{i!(i-j+1)+i!j}{j!(i-j+1)!} \tag{74}$$

$$= \frac{i!(i+1)}{j!(i-j+1)!} \tag{75}$$

$$= \frac{(i+1)!}{j!(i+1-j)!}. \tag{76}$$

Donc l'expression est vérifiée pour $i+1$.

4) Donc la propriété est vérifiée pour $i=0, j=0$, pour $i=1, j=0$, pour $i=0, j=1$, pour $i=1, j=1$, et si elle est vérifiée à i fixé pour j, elle l'est pour $j+1$, et si elle est vérifiée à j fixé pour i, elle l'est pour $i+1$. Donc elle est vérifiée pour tous i, j.

C.Q.F.D.
.

BEATRIX : A quoi servent ces C_i^j que nous venons de calculer ?

EURISTIDE : Ces nombres sont utilisés en Analyse Combinatoire. Les C_n^p permettent le calcul du nombre de combinaisons possibles pour placer n objets dans un sac n'en pouvant contenir que p.
Par exemple, si je possède 3 billes, une rouge notée R, une verte notée V et une bleue notée B, et si je possède une boîte n'en pouvant recevoir que 2 d'entre elles, intuitivement je vais avoir les possibilités suivantes :

$$\{R \quad , \quad V\} \tag{77}$$
$$\{R \quad , \quad B\} \tag{78}$$
$$\{V \quad , \quad R\}. \tag{79}$$

BEATRIX : Alors... cela fait 3 possibilités.
Si je calcule maintenant C_3^2 pour les combinaisons possibles de 3 objets rangés dans un sac de 2 :

$$C_3^2 = \frac{3!}{2!(3-2)!} = \frac{3\times 2\times 1}{2\times 1\times 1} = 3. \tag{80}$$

Miracle !

EURISTIDE : Oui, bravo. Mais il n'y a pas de miracles en mathématiques, il n'y a que des surprises que l'on peut comprendre après réflexion. La relation entre le triangle de Pascal et les combinaisons pour ranger n objets dans un sac de p se comprend assez bien, si on y réfléchit un peu. Nous connaissons déjà la relation fondamentale du triangle de Pascal :

$$C_{i+1}^j = C_i^j + C_i^{j-1}. \tag{81}$$

Si nous analysons la signification de cette relation, nous comprenons ceci : le nombre de combinaisons pour ranger $i+1$ objets j à j est le nombre de combinaisons pour ranger i objets j à j, auquel j'ajoute le nombre de combinaisons pour ranger i objets $j-1$ à $j-1$. Supposons que j'aie à ma disposition i objets et un sac pouvant en contenir j. Je sais que je peux les ranger de C_i^j combinaisons différentes. Que se passe-t-il si j'ajoute un objet, c'est-à-dire un $(i+1)$-ième objet ? Nous pouvons considérer qu'en plus des combinaisons que nous avons déjà comptées, c'est-à-dire C_i^j, l'arrivée du nouvel élément (le $(i+1)$-ième) fait que nous allons occuper une place dans le sac avec cet élément (et pour cela, je n'ai qu'une possibilité), et il restera dans le sac $j-1$ places pour disposer les i éléments d'origine : cette dernière opération pourra se faire suivant C_i^{j-1} combinaisons possibles.

BEATRIX : D'accord ! C'est pourquoi nous faisons la somme du nombre de combinaisons des i éléments placés j à j avec le nombre de combinaisons des i éléments placés $j-1$ à $j-1$. C'est très clair !

EURISTIDE : C'est bien cela. Mais attention, il faut se souvenir que dans l'expression

$$C_n^p, \tag{82}$$

le nombre d'objets est placé à l'indice et la taille des combinaisons à l'exposant. Tandis que dans la formule avec les factorielles, il faut placer au numérateur le nombre d'objets et au dénominateur la taille des combinaisons. Donc, attention aux erreurs !

2.3 Scène II.3 - Nombres de Bernoulli

BEATRIX : Oui, il y a un bon piège, ici !

EURISTIDE : Nous allons maintenant étudier une classe de nombres particuliers, appelés nombres de Bernouilli. Nous avons étudié la somme des n premiers entiers, que nous noterons S_1 :

$$S_1 = \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n. \tag{83}$$

Jacques Bernoulli, au XVIIIème siècle, a étudié les sommes de carrés, de cubes, etc.

BEATRIX : Je pense que nous pourrions calculer la somme des carrés au moyen de la méthode que nous avions vue pour la somme des nombres. Quoiqu'à la réflexion, les calculs avec des carrés ou des puissances de nombres seront beaucoup plus complexes...

EURISTIDE : En réalité, nous allons utiliser une nouvelle méthode plus astucieuse.

MATHINE : Voici l'expression de la somme des n premiers carrés :

Proposition **2.3.1**
Somme n premiers carrés
La somme des n premiers carrés s'écrit :

$$S_2 = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n. \tag{84}$$

Démonstration :

Calculons l'expression suivante :

$$\begin{aligned} (x+1)^3 - x^3 &= x^3 + 3x^2 + 3x + 1 - x^3 & (85)\\ &= 3x^2 + 3x + 1. & (86) \end{aligned}$$

Nous pouvons maintenant remplacer x successivement par 1, 2, 3, etc., et obtenir le tableau d'égalités suivantes :

$$\begin{aligned} 2^3 - 1^3 &= 3 \times 1 + 3 \times 1 + 1 && (87)\\ 3^3 - 2^3 &= 3 \times 4 + 3 \times 2 + 1 && (88)\\ 4^3 - 3^3 &= 3 \times 9 + 3 \times 3 + 1 && (89)\\ \ldots &\quad \ldots\ldots\ldots && (90)\\ (n+1)^3 - n^3 &= 3 \times n^2 + 3 \times n + 1. && (91) \end{aligned}$$

En ajoutant membre à membre ces égalités, on constate que dans le membre de gauche, les termes s'annulent deux à deux à l'exception du terme -1^3 et $(n+1)^3$; et dans le membre de droite, nous pouvons construire, en rassemblant les termes de façon adéquate, les sommes des n premiers carrés et des n premiers entiers :

$$(n+1)^3 - 1^3 = 3S_2 + 3S_1 + n, \tag{92}$$

où S_1 désigne la somme des n premiers entiers, et S_2 la somme des n premiers carrés.
Nous pouvons exprimer S_2 en l'isolant dans le membre de gauche de l'égalité :

$$\begin{aligned} 3S_2 &= n^3 + 3n^2 + 3n - 3S_1 - n && (93)\\ &= n^3 + 3n^2 + 3n - \frac{3}{2}n^2 - \frac{3}{2}n - n. && (94) \end{aligned}$$

D'où :

$$3S_2 = n^3 + \frac{3}{2}n^2 + \frac{1}{2}n. \tag{95}$$

C.Q.F.D.

EURISTIDE : Nous allons maintenant calculer la somme des cubes avec la même méthode.

MATHINE : Voici la proposition exprimant la somme des n premiers cubes :

Proposition 2.3.2
Somme des n premiers cubes
La somme des n premiers cubes s'écrit :

$$S_3 = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2. \tag{96}$$

Démonstration :

Comme précédemment, nous calculons l'expression suivante :

$$\begin{aligned} (x+1)^4 - x^4 &= x^4 + 4x^3 + 6x^2 + 4x + 1 - x^4 && (97)\\ &= 4x^3 + 6x^2 + 4x + 1. && (98) \end{aligned}$$

Nous écrivons maintenant un tableau d'égalités en remplaçant successivement x par 1, 2, 3, etc.

$$\begin{aligned} 2^4 - 1^4 &= 4 \times 1^3 + 6 \times 1^2 + 4 \times 1 + 1 && (99)\\ 3^4 - 2^4 &= 4 \times 2^3 + 6 \times 2^2 + 4 \times 2 + 1 && (100)\\ \dots &\quad \dots\dots\dots && (101)\\ (n+1)^4 - n^4 &= 4 \times n^3 + 6 \times n^2 + 4 \times n + 1. && (102) \end{aligned}$$

En ajoutant terme à terme ces égalités, nous obtenons :

$$(n+1)^4 - 1^4 = 4S_3 + 6S_2 + 4S_1 + n. \quad (103)$$

D'où, en isolant $4S_3$ et en développant :

$$\begin{aligned} 4S_3 &= (n+1)^4 - 1 - 6S_2 - 4S_1 - n && (104)\\ &= n^4 + 4n^3 + 6n^2 + 4n + 1 - 1 - 6S_2 - 4S_1 - n && (105)\\ &= n^4 + 4n^3 + 6n^2 + 4n - 2n^3 - 3n^2 - n - 2n^2 - 2n - n && (106)\\ &= n^4 + 2n^3 + n^2. && (107) \end{aligned}$$

C.Q.F.D.

BEATRIX : Existe-t-il une méthode générale pour trouver la somme des n premières puissances p des entiers consécutifs ?

EURISTIDE : Oui. Et c'est en travaillant sur cette question toute naturelle que tu viens de te poser, que nous allons faire apparaître les nombres de Bernoulli. Commençons par démontrer un théorème, appelé théorème du binôme de Newton, car nous en aurons besoin pour la suite.

MATHINE : Voici le théorème du binôme de Newton :

Théorème 2.3.1 (Binôme de Newton) *Soit n un entier et x et y deux entiers quelconques. Alors :*

$$(x+y)^n = \sum_{p=0}^{n} C_n^p x^{n-p} x^p. \quad (108)$$

BEATRIX : Tiens ! Voilà les nombres de combinaisons C_n^p qui pointent le bout de leur nez.

EURISTIDE : Oui. Et il y a une excellente raison bien intuitive pour cela. Mais laissons d'abord la parole à Mathine pour démontrer ce théorème.

MATHINE : La démonstration se fera par récurrence, bien naturellement.

Démonstration :

1) Vérifions que la propriété est vraie pour $n = 0$.

$$(x+y)^0 = 1, \tag{109}$$

par convention.
En utilisant l'expression du binôme de Newton, nous avons :

$$\begin{aligned}(x+y)^0 &= \sum_{p=0}^{0} C_0^p x^{0-p} y^0 &(110)\\ &= C_0^0 x^0 y^0 &(111)\\ &= 1. &(112)\end{aligned}$$

Donc, la propriété est bien vérifiée pour $n = 0$.

2) Supposons maintenant que la propriété est vraie pour n.
Considérons l'expression $(x+y)^{n+1}$ et calculons-là en fonction de $(x+y)^n$:

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n (x+y) &(113)\\ &= \left(\sum_{p=0}^{n} C_n^p x^{n-p} y^p\right)(x+y) &(114)\\ &= \sum_{p=0}^{n} C_n^p x^{n+1-p} y^p + \sum_{p=0}^{n} C_n^p x^{n-p} y^{p+1}. &(115)\end{aligned}$$

Nous pouvons effectuer une renumérotation des indices de la somme de droite, en remplaçant $p+1$ par p :

$$(x+y)^{p+1} = \sum_{p=0}^{n} C_n^p x^{n+1-p} y^p + \sum_{p=1}^{n+1} C_n^{p-1} x^{n-p+1} y^p. \tag{116}$$

Nous pouvons alors regrouper les deux sommes en une seule, à l'exception du dernier terme en $p = n+1$, qu'il faudra bien veiller à ajouter :

$$(x+y)^{n+1} = \sum_{p=0}^{n} \left(C_n^p + C_n^{p-1}\right) x^{n+1-p} y^p + C_n^n x^0 y^{n+1}. \tag{117}$$

Or, nous savons, d'après la propriété du triangle de Pascal, que :

$$C_n^p + C_n^{p-1} = C_{n+1}^p. \tag{118}$$

Donc :

$$(x+y)^{n+1} = \sum_{p=0}^{n} C_{n+1}^p x^{n+1-p} y^p + C_n^n x^0 y^{n+1}. \tag{119}$$

Par ailleurs, nous savons que $C_n^n = 1$, et $C_{n+1}^{n+1} = 1$ également. Donc, nous pouvons écrire :

$$C_n^n x^0 y^{n+1} = C_{n+1}^{n+1} x^0 y^{n+1}. \tag{120}$$

Nous pouvons donc substituer ce dernier terme dans l'égalité de $(x+y)^{n+1}$.
Et cela va permettre de placer ce terme sous le signe somme $\sum$ du membre de droite et étendre ainsi la somme jusqu'à $n+1$:

$$(x+y)^{n+1} = \sum_{p=0}^{n+1} C_{n+1}^{p} x^{(n+1)-p} y^{p}. \tag{121}$$

2) Donc la propriété est vraie pour $n=0$ et lorsqu'elle est vraie pour n, alors elle l'est pour $n+1$. Donc, d'après le principe de récurrence, la propriété est vraie pour tout n.

C.Q.F.D.

BEATRIX : C'est amusant et surprenant de retrouver les coefficients C_n^p dans le développement de $(x+y)^n$.

EURISTIDE : C'est étonnant, mais compréhensible, en fait. Lorsqu'on effectue le développement de $(x+y)^n$, on peut regarder de plus près ce qui se passe pour les termes en $x^{n-p}y^p$. Nous avons n termes $(x+y)$ multipliés entre eux qui devront être choisis pour constituer des termes en $x^{n-p}y^p$. Ceci revient à ranger ces n objets $(x+y)$ dans une boîte où il n'y a que p compartiments, et cette boîte c'est le terme $x^{n-p}y^p$. Prenons un exemple avec $n=3$:

$$(x+y)^3 = (x+y)(x+y)(x+y). \tag{122}$$

Je dois constituer les termes en x^3y^0. Je n'ai qu'une seule possibilité pour ces termes, celle obtenue en multipliant le premier terme x de chaque expression $(x+y)$.
Je dois maintenant constituer les termes en x^2y^1. J'ai 3 façons de choisir ce terme : en prenant le y de la première expression $(x+y)$, et les x des deux expressions suivantes ; puis en prenant le y de la deuxième expression, et les x des deux autres ; et enfin en prenant le y de la troisième expression et les x des deux autres. Nous sommes bien confrontés à un problème du type : mettre trois objets (le terme y) dans un emplacement (la puissance y^1).
De la même façon, choisissons maintenant la constitution des termes en x^1y^2. J'ai C_3^2 façons de choisir le y^2, en choisissant deux y parmi les trois termes $x+y$.
Et enfin, nous n'aurons qu'une seule façon de choisir le terme x^0y^3.
C'est cette démarche qui nous conduit à l'apparition de l'expression du binôme de Newton dans le calcul de la puissance d'une somme.

BEATRIX : Ah oui ! Je comprends maintenant. C'est finalement une affaire de combinatoire. C'est amusant, ce lien entre deux aspects mathématiques très éloignés l'un de l'autre.

EURISTIDE : C'est de ce type de liens que proviennent la plupart des surprises et des enrichissements des mathématiques. Le pouvoir de celles-ci, c'est de dresser de solides ponts qui raccordent des domaines parfois très distants en mathématiques.
C'est ainsi que la démonstration du célèbre théorème de Fermat-Wiles fait appel à des notions de topologie, d'algèbre et de géométries auxquelles on ne s'attend pas du tout quand on regarde l'énoncé très simple : $x^n + y^n = z^n$ n'a pas de solutions entières pour $n > 2$.
Mais revenons à nos nombres de Bernoulli. La formulation du binôme de Newton va nous aider à calculer

de proche en proche les différentes sommes de puissances d'entiers.
Commençons par S_4, ma chère Mathine.

MATHINE : Voici en effet l'expression des n premières puissances 4 d'entiers :

Proposition **2.3.3**
Somme des n premières puissances 4
La somme des n premières puissances 4 d'entiers s'écrit :

$$S_4 = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 + 0n^2 - \frac{1}{30}n. \tag{123}$$

En voici la démonstration, s'appuyant justement sur le binôme de Newton :

Démonstration :

Calculons l'expression suivante :

$$\begin{aligned}(x+1)^5 - x^5 &= C_5^5x^5 + C_5^4x^4 + C_5^3x^3 + C_5^2x^2 + C_5^1x + C_5^0 - x^5 &(124)\\ &= x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 - x^5. &(125)\end{aligned}$$

En ajoutant terme à terme les expressions pour $x = 1$, 2, 3, etc., nous trouvons :

$$(n+1)^5 - 1 = 5S_4 + 10S_3 + 10S_2 + 5S_1 + n. \tag{126}$$

D'où :

$$\begin{aligned}5S4 &= (n+1)^5 - 1 - 10S_3 - 10S_2 - 5S_1 - n &(127)\\ &= n^5 + 5n^4 + 10n^3 + 10n^2 + 5n - \frac{10}{4}n^4 - \frac{10}{2}n^3 - \frac{10}{4}n^2 &(128)\\ &\quad -\frac{10}{3}n^3 - \frac{10}{2}n^2 - \frac{10}{6}n - \frac{5}{2}n^2 - \frac{5}{2}n - n &(129)\\ &= n^5 + \frac{5}{2}n^4 + \frac{5}{3}n^3 + 0n^2 - \frac{1}{6}n. &(130)\end{aligned}$$

C.Q.F.D.

EURISTIDE : Jusque là, nous avons montré que :

$$\begin{array}{lcccccccc} 2S_1 &=& 1n^2 &+& 1n & & & & \\ 3S_2 &=& 1n^3 &+& \frac{3}{2}n^2 &+& \frac{1}{2}n & & \\ 4S_3 &=& 1n^4 &+& 2n^3 &+& 1n^2 &+& 0n \\ 5S_4 &=& 1n^5 &+& \frac{5}{2}n^4 &+& \frac{5}{3}n^3 &+& 0n \quad - \quad \frac{1}{6}n. \end{array} \tag{131}$$

Nous allons procéder comme le faisaient les mathématiciens des XVIIème et XVIIIème siècles. Tâcher de déterminer une loi en observant et démontrer cette loi ensuite. En regardant ces égalités, nous commençons à trouver une structure ; nous constatons que le premier terme de l'expression $(k+1)S_k$ est n^{k+1} et que le

deuxième terme de cette expression s'écrit toujours $\frac{k+1}{2}n^k$.
Donc, l'expression commence comme suit :

$$(k+1)S_k = n^{k+1} + \frac{k+1}{2}n^k + \dots \tag{132}$$

Les coefficients en n^{k-1} s'écrivent :

$$S_2 \ : \ \frac{1}{2} \tag{133}$$
$$S_3 \ : \ 1 \tag{134}$$
$$S_4 \ : \ \frac{5}{3}. \tag{135}$$

Si nous avons l'idée de multiplier par 6, pour éliminer les fractions de ces trois termes, nous trouvons que les trois premiers termes sont 3, 6 et 10.

BEATRIX : Tiens. Ces nombres me rappellent quelque chose. Ah oui ! Ce sont des nombres du triangle de Pascal, dans la troisième colonne :

$$\begin{array}{cccccc} 1 & & & & & \\ 1 & 1 & & & & \\ 1 & 2 & 1 & & & \\ 1 & 3 & 3 & 1 & & \\ 1 & 4 & 6 & 4 & 1 & \\ 1 & 5 & 10 & 10 & 5 & 1 \end{array} \tag{136}$$

EURISTIDE : C'est exact. Nous pouvons donc conjecturer que les premiers termes de $(k+1)S_k$ s'écrivent :

$$(k+1)S_k = n^{k+1} + \frac{k+1}{2}n^k + \frac{1}{6}C_{k+1}^2 + \dots \tag{137}$$

BEATRIX : Pour en être sûrs, et pour trouver les termes suivants, il nous faudrait avoir l'expression d'autres S_k pour des k plus grands.

EURISTIDE : Tu as tout à fait raison, Béatrix. Nous n'allons pas le faire ici, mais voici, après calculs faits, le tableau des 6 premiers S_k, obtenus comme précédemment par calculs de proche en proche :

$$\begin{array}{lcccccccccccc} 2S_1 & = & 1n^2 & + & 1n & & & & & & & & \\ 3S_2 & = & 1n^3 & + & \frac{3}{2}n^2 & + & \frac{1}{2}n & & & & & & \\ 4S_3 & = & 1n^4 & + & 2n^3 & + & 1n^2 & + & 0n & & & & \\ 5S_4 & = & 1n^5 & + & \frac{5}{2}n^4 & + & \frac{5}{3}n^3 & + & 0n^2 & - & \frac{1}{6}n & & \\ 6S_5 & = & 1n^6 & + & 3n^5 & + & \frac{5}{2}n^4 & + & 0n^3 & - & \frac{1}{2}n^2 & + & 0n \\ 7S_6 & = & 1n^7 & + & \frac{7}{2}n^6 & + & \frac{7}{2}n^5 & + & 0n^4 & - & \frac{7}{6}n^3 & + & 0n & + & \frac{1}{6}n. \end{array} \tag{138}$$

Notre règle :

$$(k+1)S_k = n^{k+1} + \frac{k+1}{2}n^k + \frac{1}{6}C_{k+1}^2 n^{k-1} + \dots \tag{139}$$

se confirme bien.
Nous voyons que les termes suivants sont nuls pour tous les S_k calculés. Nous pouvons conjecturer qu'il en

est de même pour tous les S_k.
Notre expression devient :

$$(k+1)S_k = n^{k+1} + \frac{k+1}{2}n^k + \frac{1}{6}C_{k+1}^2 n^{k-1} + 0n^{k-2} + \dots \tag{140}$$

Pour le terme suivant, on retrouve les coefficients :

$$S_4 \quad : \quad -\frac{1}{6} \tag{141}$$

$$S_5 \quad : \quad -\frac{1}{2} \tag{142}$$

$$S_6 \quad : \quad -\frac{7}{6}. \tag{143}$$

Si on a l'idée de multiplier par -30, on peut alors trouver des nombres du triangle de Pascal :

$$S_4 \quad : \quad 5 \tag{144}$$

$$S_5 \quad : \quad 15 \tag{145}$$

$$S_6 \quad : \quad 35. \tag{146}$$

`BEATRIX` : J'ai vérifié. Ce sont bien de nouveau des entiers du triangle de pascal ; dans la colonne 4 : 1, 5, 15, 35, 70, etc.

`EURISTIDE` : Nous pouvons voir également que le terme suivant a un coefficient nul. Nous pouvons maintenant conjecturer que :

$$(k+1)S_k = n^{k+1} + \frac{k+1}{2}n^k + \frac{1}{6}C_{k+1}^2 n^{k-1} + 0n^{k-2} - \frac{1}{30}C_{k+1}^4 n^{k-3} + 0n^{k-4} + \dots \tag{147}$$

On met donc en évidence une suite de nombres, en réécrivant cette expression sous la forme :

$$(k+1)S_k = 1.C_{k+1}^0 n^{k+1} + \frac{1}{2}C_{k+1}^0 n^{k+1} + \frac{1}{2}C_{k+1}^1 n^k + \frac{1}{6}C_{k+1}^2 n^{k-1} \tag{148}$$

$$+0.C_{k+1}^3 n^{k-2} - \frac{1}{30}C_{k+1}^4 n^{k-3} + 0C_{k+1}^5 n^{n-4} + \dots \tag{149}$$

Notons (f_i) cette suite de nombres. Nous avons :

$$f_0 = 1 \tag{150}$$

$$f_1 = \frac{1}{2} \tag{151}$$

$$f_2 = \frac{1}{6} \tag{152}$$

$$f_3 = 0 \tag{153}$$

$$f_4 = -\frac{1}{30} \tag{154}$$

$$f_5 = 0. \tag{155}$$

Les nombres f_i sont appelés nombres de Faulhaber. Ils permettent d'écrire l'expression :

$$S_k = \frac{1}{k+1}\sum_{p=0}^{k+1} C_{k+1}^p f_p n^{k+1-p}. \tag{156}$$

BEATRIX : C'est bien joli, mais ce n'est pas parce qu'on a donné un joli nom à ces coefficients que nous les connaissons. Le moins qu'on puisse dire, c'est que leurs valeurs ne sont pas très intuitives, à ces coefficients...

$$1; \frac{1}{2}; \frac{1}{6}; 0; -\frac{1}{30}; 0; \dots \tag{157}$$

EURISTIDE : Pour calculer ces coefficients, nous allons devoir ruser. Nous allons définir une fonction $F(x)$ comme suit :

$$F(x) = f_0 + f_1 \frac{x}{1!} + f_2 \frac{x}{2!} + f_3 \frac{x}{3!} + \dots \tag{158}$$

Nous allons avoir besoin maintenant d'une proposition d'Analyse pour continuer. Il s'agit du développement en série de la fonction e^x.

MATHINE : Voici le développement en série de la fonction exponentielle :

Proposition **2.3.4**
Développement en série exponentielle
Pour tout $x \in \mathbb{R}$, nous avons :

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \tag{159}$$

BEATRIX : Encore une fois, la théorie des nombres nous surprend ! Je ne m'attendais pas à devoir utiliser un tel détour par le développement en série de l'exponentielle.

EURISTIDE : C'est là que réside toute la ruse. C'est encore un de ces ponts qui font toute la beauté des mathématiques.

MATHINE : Nous allons démontrer cette proposition, maintenant.

Démonstration :

La caractéristique fondamentale de la fonction e^x est qu'elle est sa propre dérivée :

$$(e^x)' = e^x. \tag{160}$$

Supposons qu'il existe une série de la forme :

$$e^x = \sum_{n=0}^{+\infty} a_n x^n, \tag{161}$$

où $a_0 = 1$.
Calculons la dérivée de e^x, pour cette expression :

$$(e^x)' = e^x \tag{162}$$

$$= \sum_{n=1}^{+\infty} n.a_n x^{n-1} \tag{163}$$

En identifiant terme à terme les deux expressions de e^x obtenues, nous trouvons que :

$$a_n = (n+1)a_{n+1}. \tag{164}$$

Démontrons alors par récurrence que $a_n = \frac{1}{n!}$.
1) Pour $n = 0$, nous avons $a_0 = 1$ et $\frac{1}{0!} = 1$. Donc la propriété est vérifiée pour $n = 0$.
2) Supposons la propriété vraie pour n. Alors :

$$a_{n+1} = \frac{a_n}{a_{n+1}} = \frac{1}{n!}\frac{1}{n+1} = \frac{1}{(n+1)!}. \tag{165}$$

3) Donc la propriété est vraie pour $n = 0$, et si elle est vraie pour n, alors elle l'est pour $n + 1$. Donc, par principe de récurrence, la propriété est vraie pour tous n.
Nous avons donc démontré que si e^x possède la forme du développement en série indiqué, alors son expression est :

$$e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}. \tag{166}$$

Il nous reste à prouver que cette forme de développement a bien un sens, c'est-à-dire qu'elle converge (ce qui veut dire qu'elle possède une valeur finie, même si elle comprend un nombre infini de termes), lorsque n tend vers l'infini. La technique que nous allons employer consiste à trouver une série convergente ou une constante qui majore cette série.
Or nous pouvons écrire :

$$\frac{x^{+1}}{(n+1)!} = \frac{x^n}{n!}\frac{x}{n+1} \tag{167}$$

et pour n suffisamment grand, x étant fixé, nous pouvons faire l'hypothèse que $n \geq 2x$.
Par conséquent, nous avons :

$$\frac{x}{n+1} \leq \frac{1}{2}. \tag{168}$$

Donc :

$$\frac{x^{n+1}}{(n+1)!} \leq \frac{1}{2}\frac{x^n}{n!}. \tag{169}$$

Fixons n maintenant suffisamment grand pour que l'inégalité ci-dessus soit vraie et définissons la constante :

$$\frac{x^n}{n!} = C'. \tag{170}$$

C' est bien une constante puisque x et n sont maintenant fixés.
Alors :

$$\frac{x^{n+1}}{(n+1)!} \leq \frac{C'}{2} \tag{171}$$

$$\frac{x^{n+2}}{(n+2)!} \leq \frac{C'}{4} \tag{172}$$

$$\frac{x^{n+3}}{(n+3)!} \leq \frac{C'}{8} \tag{173}$$

$$\ldots \quad \ldots \tag{174}$$

Donc, la série :

$$e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!} \tag{175}$$

est telle que, pour n suffisamment grand :

$$e^x \leq C + \sum_{p=n}^{+\infty} \frac{C'}{2^{(n-p)}}, \tag{176}$$

où C et C' sont des constantes. C représente la valeur de la somme des premiers termes jusqu'à $n-1$. Et C' est la valeur de $\frac{x^n}{n!}$.
En réindexant, nous pouvons écrire :

$$e^x \leq C + D \sum_{p=0}^{+\infty} \frac{1}{2^p}. \tag{177}$$

La démonstration revient donc maintenant à démontrer que la série :

$$\sum_{p=0}^{+\infty} \frac{1}{2^p} \tag{178}$$

est convergente. En effet, si elle est convergente, comme est majore toujours la série e^x pour n suffisamment grand, cela signifie que nécessairement la série e^x converge également.
Mais cette série est ce qu'on appelle une série géométrique.
Nous allons démontrer par récurrence que la valeur du n-ième terme de cette série vaut :

$$\sum_{p=0}^{n} \frac{1}{2^p} = 2 - \frac{1}{2^n}. \tag{179}$$

En effet :
1) Pour $n = 1$, la série vaut :

$$\sum_{p=0}^{1} \frac{1}{2^p} = 1 + \frac{1}{2}. \tag{180}$$

Pour $n = 1$, la formule vaut :

$$2 - \frac{1}{2^1} = 1 + \frac{1}{2}. \tag{181}$$

Donc, la formule est vraie pour $n = 1$.

2) Supposons la formule vraie pour n. Calculons la formule pour $n+1$.
Nous avons :

$$\begin{aligned} \sum_{p=0}^{n+1} \frac{1}{2^p} &= \sum_{p=0}^{n} \frac{1}{2^p} + \frac{1}{2^{n+1}} && (182)\\ &= 2 - \frac{1}{2^n} + \frac{1}{2^{n+1}} && (183)\\ &= 2 - \frac{1}{2^{n+1}}. && (184) \end{aligned}$$

3) Donc, la formule est vraie pour $n = 1$, et lorsqu'elle est vraie pour n, elle l'est pour $n+1$. Donc elle est vraie pour tout n, d'après le principe de récurrence.

Revenons à notre série $\sum_{n=0}^{+\infty} \frac{1}{2^p}$. Nous venons de vérifier que son n-ième terme s'écrit :

$$\sum_{p=0}^{n} \frac{1}{2^p} = 2 - \frac{1}{2^n}. \tag{185}$$

Donc, lorsque n tend vers l'infini, ce terme tend vers 2.
Par conséquent, la série $\sum_{n=0}^{+\infty} \frac{1}{2^n}$ est convergente, de limite 2.
Par conséquent, enfin, puisqu'elle est majorée par cette dernière série, la série e^x est également convergente.
Donc, nous pouvons finalement écrire :

$$e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!} \tag{186}$$

C.Q.F.D.

EURISTIDE : Voilà. Maintenant que Mathine a brillamment démontré l'expression du développement en série de la fonction e^x, nous pouvons poursuivre notre investigation dans le monde des nombres de Bernoulli.
Nous avons introduit tout à l'heure la fonction $F(x)$:

$$F(x) = f_0 + f_1\frac{x}{1!} + f_2\frac{x^2}{2!} + f_3\frac{x^3}{3!} + \dots \tag{187}$$

Par ailleurs, nous avons :

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots, \tag{188}$$

et nous pouvons écrire, en multipliant les deux membres de cette deuxième egalité par x :

$$xe^x = 0 + \frac{x}{1!} + 2\frac{x^2}{2!} + 3\frac{x^3}{3!} + \dots \tag{189}$$

En ajoutant membre à membre l'expression de $F(x)$ avec celle de xe^x, nous obtenons :

$$F(x) + xe^x = f_0 + (1 + f_1)\frac{x}{1!} + (2 + f_2)\frac{x}{2!} + (3 + f_3)\frac{x^3}{3!} + \dots \tag{190}$$

Calculons maintenant $e^x F(x)$:

$$
\begin{aligned}
e^x F(x) &= \left(f_0 + f_1\frac{x}{1!} + f_2\frac{x^2}{2!} + f_3\frac{x^3}{3!} + \dots\right) && (191)\\
&\quad (1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots) && (192)\\
&= f_0 && (193)\\
&+ (f_0 + f_1)\frac{x}{1!} && (194)\\
&+ (f_0 + 2!f_1 + f_2)\frac{x^2}{2!} && (195)\\
&+ (f_0 + \frac{3!}{2!}f_1 + \frac{3!}{2!}f_2 + f_3)\frac{x^3}{3!} && (196)\\
&+ (f_0 + \frac{4!}{3!}f_1 + \frac{4!}{4}f_2 + \frac{4!}{3!}f_3 + f_4)\frac{x^4}{4!} && (197)\\
&+ \dots && (198)\\
&= f_0 && (199)\\
&+ (f_0 + f_1)\frac{x}{1!} && (200)\\
&+ (f_0 + 2f_1 + f_2)\frac{x^2}{2!} && (201)\\
&+ (f_0 + 3f_1 + 3f_2 + f_3)\frac{x^3}{3!} && (202)\\
&+ (f_0 + 4f_1 + 6f_2 + 4f_3 + f_4)\frac{x^4}{4!} && (203)\\
&+ \dots && (204)
\end{aligned}
$$

`BEATRIX` : Tiens ! On retrouve nos fameux coefficients du binôme !

`EURISTIDE` : Oui, et ce n'est pas une surprise. Nous avons effectué un produit de termes comportant des puissances de x, et c'est ce qui a introduit les coefficients du binôme.
Donc :

$$
\begin{aligned}
e^x F(x) &= C_0^0 f_0\frac{x^0}{0!} && (205)\\
&+ (C_1^0 f_0 + C_1^1 f_1)\frac{x^1}{1!} && (206)\\
&+ (C_2^0 f_0 + C_2^1 f_1 + C_2^2 f_2)\frac{x^2}{2!} && (207)\\
&+ (C_3^0 f_0 + C_3^1 f_1 + C_3^2 f_2 + C_3^3 f_3)\frac{x^3}{3!} && (208)\\
&+ (C_4^0 f_0 + C_4^1 f_1 + C_4^2 f_2 + C_4^3 f_3 + C_4^4 f_4)\frac{x^4}{4!} && (209)\\
&+ \dots && (210)
\end{aligned}
$$

Or, nous avons vu que :

$$\begin{aligned} 1 &= f_0 && (211)\\ 2 &= C_2^0 + C_2^1 f_1 = f_0 + 2f_1 && (212)\\ 3 &= C_3^0 f_0 + C_3^1 f_1 + C_3^2 f_2 = f_0 + 3f_1 + 3f_2 = 3 && (213)\\ 4 &= C_4^0 f_0 + C_4^1 f_1 + C_4^2 f_2 + C_4^3 f_3 = f_0 + 4f_1 + 6f_2 + 4f_3 = 4 && (214)\\ 5 &= \ldots\ldots && (215) \end{aligned}$$

Donc, nous pouvons écrire :

$$\begin{aligned} e^x F(x) &= f_0 && (216)\\ &+ (1+f_1)\frac{x}{1!} && (217)\\ &+ (2+f_2)\frac{x^2}{2!} && (218)\\ &+ (3+f_3)\frac{x^3}{3!} && (219)\\ &+ (4+f_4)\frac{x^4}{4!} && (220)\\ &+ \ldots && (221) \end{aligned}$$

Donc, nous avons établi l'égalité :

$$e^x F(x) = F(x) + xe^x. \tag{222}$$

D'où :

$$F(x) = \frac{xe^x}{e^x - 1}. \tag{223}$$

Il se trouve qu'Euler a introduit une autre série, en définissant :

$$B(x) = \frac{x}{e^x - 1} = B_0 + B_1\frac{x}{1!} + B_2\frac{x^2}{2!} + B_3\frac{x^3}{3!} + \ldots \tag{224}$$

Les nombres B_i sont justement appelés nombres de Bernoulli.

`BEATRIX` : Ah, les voici enfin, ces nombres de Bernoulli. Mais comment les calculer ?

`EURISTIDE` : Soit comme nous l'avons fait, de proche en proche, soit à partir des valeurs des nombres de Faulhaber, ou bien en utilisant le développement en série de e^x et un ordinateur pour calculer les itérations successives de la série $B(x) = \frac{x}{e^x-1}$. Nous allons établir une relation entre les nombres de Bernoulli et les nombres de Faulhaber. Ecrivons :

$$\begin{aligned} B(-x) &= \frac{-x}{e^{-x} - 1} && (225)\\ &= \frac{-xe^x}{1 - e^x} && (226)\\ &= \frac{xe^x}{e^x - 1} && (227)\\ &= F(x). && (228) \end{aligned}$$

Or :

$$F(x) = f_0 + f_1\frac{x}{1!} + f_2\frac{x^2}{2!} + f_3\frac{x^3}{3!} + \ldots \tag{229}$$

et :

$$B(-x) = B_0 - B_1\frac{x}{1!} + B_2\frac{x^2}{2!} - B_3\frac{x^3}{3!} + \dots \tag{230}$$

Donc, par identification terme à terme, on obtient :

$$(-1)^n B_n = f_n. \tag{231}$$

Nous en déduisons les nombres de Bernoulli à partir des nombres de Faulhaber :

$$\begin{aligned}
B_0 &= 1 && (232)\\
B_1 &= -\frac{1}{2} && (233)\\
B_2 &= \frac{1}{6} && (234)\\
B_3 &= 0 && (235)\\
B_4 &= -\frac{1}{30} && (236)\\
B_5 &= 0 && (237)\\
B_6 &= \dots && (238)
\end{aligned}$$

Nous allons donc pouvoir exprimer maintenant les sommes S_k en fonction des nombres de Bernoulli :

$$S_k = \frac{1}{k+1}\sum_{p=0}^{k+1} C_{k+1}^p (-1)^p B_p n^{k+1-p}. \tag{239}$$

`BEATRIX` : Et bien ! Nous y sommes arrivés. Il faut avouer que c'était un beau parcours. A-t-on calculé beaucoup de valeurs des nombres de Bernoulli ?

`EURISTIDE` : Avec un ordinateur, on peut en calculer de nombreux. Voici les 30 premiers nombres de Bernoulli :

$$\begin{array}{llllllllll}
B_0 = 1 & B_1 = -\frac{1}{2} & B_2 = \frac{1}{6} & B_3 = 0\\
B_4 = -\frac{1}{30} & B_5 = 0 & B_6 = \frac{1}{42} & B_7 = 0\\
B_8 = -\frac{1}{30} & B_9 = 0 & B_{10} = \frac{5}{66} & B_{11} = 0\\
B_{12} = -\frac{691}{2730} & B_{13} = 0 & B_{14} = \frac{7}{6} & B_{15} = 0\\
B_{16} = -\frac{3617}{510} & B_{17} = 0 & B_{18} = \frac{43867}{798} & B_{19} = 0\\
B_{20} = -\frac{174611}{330} & B_{21} = 0 & B_{22} = \frac{854513}{138} & B_{23} = 0\\
B_{24} = -\frac{236364091}{2730} & B_{25} = 0 & B_{26} = \frac{8553103}{6} & B_{27} = 0\\
B_{28} = -\frac{23749461029}{870} & B_{29} = 0 & B_{30} = \frac{8615841276005}{14322} &
\end{array} \tag{240}$$

3 Acte III - Divisibilité

BEATRIX : Nous connaissons maintenant les nombres de Bernoulli. Quelle est la prochaine étape ?

EURISTIDE : Nous allons maintenant aborder les questions de divisibilité des entiers. Ces questions sont essentielles parce qu'elles constituent les fondations de la plupart des questions passionnantes de la théorie des nombres classiques.

3.1 Scène III.1 - Divisibilité

MATHINE : Commençons par bien définir la divisibilité :

Définition 3.1.1
Divisibilité
Soit a, b deux entiers relatifs, a étant non nul. On dit que a divise b s'il existe un entier q tel que $b = aq$. On note alors $a|b$. Si a ne divise pas b, on écrit $a \nmid b$.

EURISTIDE : Ainsi, par exemple $2|4$, mais $3 \nmid 4$.

BEATRIX : 1 divise tous les entiers.

EURISTIDE : Et il en est de même pour -1.
Nous allons maintenant regarder d'un peu plus près les propriétés de la divisibilité.

MATHINE : Dans ce théorème, j'ai réuni quelques propriétés de base de la divisibilité.

Théorème 3.1.1
Propriétés divisibilité
Soit $a, b, c \in \mathbb{Z}$.

i) Si $a|b$, alors $a|bc$ pour tout $c \in \mathbb{Z}$.
ii) Si $a|b$ et $b|c$, alors $a|c$.
iii) Si $a|b$ et $a|c$, alors $a|(bx + cy)$ pour tous $x, y \in \mathbb{Z}$.
iv) Si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$.
v) Si $a|b$ et $b \neq 0$, alors $|a| \leq |b|$.

Démonstration :

i) Supposons que $a|b$.
Alors, d'après la definition (cf. 3.1.1), il existe un entier q tel que $b = aq$.
Alors $bc = a(cq)$.
Donc a divise bc.

ii) Supposons que $a|b$ et $b|c$.
Alors, il existe un entier q tel que $b = aq$ et un entier r tel que $c = br$.
Alors, en reportant la valeur de b dans l'expression de c, nous obtenons $c = a(qr)$.
Donc, a divise c.

iii) Supposons que $a|b$ et $a|c$.
Considérons $x, y \in \mathbb{Z}$.
Il existe un entier q tel que $b = aq$ et un entier r tel que $c = ar$.
Alors, nous pouvons écrire :

$$bx + cy = a(xq) + a(yr) \quad (241)$$
$$= a(xq + yr). \quad (242)$$

Donc, a divise $bx + cy$.

iv) Supposons que $a|b$ et $b|a$.
Alors, il existe un entier q tel que $b = aq$ et un entier r tel que $a = br$.
Reportons l'expression de a dans celle de b :

$$b = brq. \quad (243)$$

Donc, $rq = 1$.
Par conséquent, $r = q = 1$ ou bien $r = q = -1$.
Ce qui signifie que $a = b$ ou bien $a = -b$.

v) Supposons que $a|b$. Alors il existe un entier $q \neq 0$ tel que $b = aq$.
Alors, puisque $|q| \geq 1$, $|b| = |a||q| \geq |a|$.

C.Q.F.D.

EURISTIDE : Toutes ces propriétés sont immédiates à l'intuition. Il est intéressant de noter que la divisibilité est transitive (propriété ii)), et qu'elle est presque symétrique, puisqu'elle est symétrique au signe près.
Nous allons maintenant aborder la célèbre division euclidienne.

MATHINE : La division euclidienne, c'est effectivement la division que tous les écoliers connaissent :

Théorème 3.1.2 (Division euclidienne) *Soit $a, b \in \mathbb{Z}$, avec $a > 0$. Alors il existe des entiers q et r tels que $b = aq + r$, où $0 \leq r < a$. De plus, si $a \nmid b$, alors $0 < r < a$.*

EURISTIDE : La démonstration de ce théorème va s'appuyer sur un principe appelé principe du bon ordre , qui exprime que tout ensemble ordonné non vide de $\mathbb{N}$ contient un plus petit élément.

BEATRIX : C'est effectivement évident, puisqu'on peut ordonner tous les éléments de $\mathbb{N}$ et que $\mathbb{N}$ possède une borde inférieure 0.

EURISTIDE : Nous n'allons pas chercher à démontrer ce principe, et nous allons le considérer comme un axiome.
Pour démontrer le théorème de la division euclidienne, l'idée est de considérer l'ensemble des différences entre b et aq pour q arbitraire, et d'en trouver le plus petit élément qui sera le reste recherché.

MATHINE : Voici donc comment l'on démontre ce théorème de la division euclidienne :

Démonstration :

Considérons l'ensemble :

$$E = \{b - na; n \in \mathbb{Z}, b - na \geq 0\}. \tag{244}$$

Cet ensemble est non vide et est inclus dans $\mathbb{N}$. Donc d'après le principe du bon ordre, E contient un plus petit élément que nous noterons r.
Désignons q l'entier tel que :

$$r = b - qa. \tag{245}$$

Alors :

$$b = aq + r. \tag{246}$$

Montrons que $r < a$.

EURISTIDE : Pour cela, nous allons effectuer ce qu'on appelle une démonstration par l'absurde. Ce procédé consiste à faire l'hypothèse que ce que l'on cherche à démontrer est faux, puis par déductions successives à partir de cette hypothèse, à mettre en évidence une contradiction. On en déduit alors que l'hypothèse de départ est fausse.

BEATRIX : Et comme l'hypothèse de départ dit que ce qu'on doit démontrer est faux, on en déduit en réalité que ce qu'on veut démontrer est vrai ! C'est génial !

MATHINE : Supposons donc que $r \geq a$.
Alors $b - qa \geq a$.
Ce qui s'écrit $b - (q + 1)a \geq 0$.
Or, par définition : $b - (q + 1)a \in E$.
De plus, évidemment :

$$b - (q + 1)a < b - qa. \tag{247}$$

$b - qa$ étant dans E également, nous avons trouvé par $b - (q + 1)a$ un élément de E plus petit que $b - qa$. Ceci contredit notre hypothèse de départ que $b - qa$ est le plus petit élément de E. Donc l'hypothèse est contradictoire et par conséquent $r < a$.
Enfin, supposons que $r = 0$. Alors $b = qa$, donc $a|b$. On en déduit la négation de cette dernière assertion : si $a \nmid b$, alors $r \neq 0$, donc $0 < r < a$.

C.Q.F.D.

EURISTIDE : Il faut noter que par construction, les entiers q et r de la division euclidienne sont uniques. Pour le démontrer, nous allons de nouveau effectuer une démonstration par l'absurde. En effet, supposons qu'il en existe deux couples (q_1, r_1) et (q_2, r_2).
On a :

$$b = q_1 a + r_1 \quad (248)$$
$$b = q_2 a + r_2, \quad (249)$$

avec $0 \leq r_1 < a$ et $0 \leq r_2 < a$.
On en déduit que :

$$(q_1 - q_2)a = r_2 - r_1. \quad (250)$$

Par conséquent $a|(r_2 - r_1)$.
Donc $|r_2 - r_1| \geq a$.
Mais, nous savons que $0 \leq r_1 < a$ et $0 \leq r_2 < a$, donc :

$$-a < r_2 - r_1 < a, \quad (251)$$

ce qui contredit que a puisse diviser $r_2 - r_1$.
Donc, il ne peut pas exister deux couples différents (q_1, r_1) et (q_2, r_2) vérifiant la division euclidienne. Les entiers q et r sont donc uniques.

MATHINE : Nous allons maintenant poursuivre notre parcours dans la théorie de la divisibilité, et identifier les propriétés des diviseurs communs à plusieurs nombres.

Définition **3.1.2**
Plus grand commun diviseur
Soit $a, b \in \mathbb{Z}$, avec $ab \neq 0$. On appelle plus grand commun diviseur (ou pgcd) de a et b, noté (a, b) ou $pgcd(a, b)$, l'entier positif d qui satisfait à :
- *$d|a$ et $d|b$,*
- *si $c|a$ et $c|b$, alors $c \leq d$.*

EURISTIDE : On peut dire le pgcd, puisque la définition du pgcd lui impose d'être unique.
Prenons quelques exemples. Cherchons le pgcd de 4 et de 6. Pour le déterminer, il suffit de noter les diviseurs de 4 et ceux de 6, et de noter le plus grand d'entre eux :
- Diviseurs de 6 : 1, 2, 3, 6.
- Diviseurs de 4 : 1, 2, 4.

BEATRIX : Le plus grand diviseur commun de 4 et 6 est donc 2.
Je vais traiter un autre exemple moi-même. Je cherche le pgcd de 12 et de 10 :
- Diviseurs de 12 : 1, 2, 3, 4, 6, 12.
- Diviseurs de 10 : 1, 2, 5, 10.

Le pgcd de 12 et 10 est donc 2.
Mais que se passe-t-il s'il n'y a pas de diviseurs communs ?

EURISTIDE : Il y en a toujours au moins un, c'est 1 ! 1 est diviseur de facto de tous les entiers.

Mais, sur le fond, ta remarque est intéressante, parce que le cas où deux entiers n'ont que 1 pour diviseur commun est un peu spécial, donc cela vaut la peine de lui attacher une définition, n'est-ce pas Mathine ?

MATHINE : Oui, nous parlons ici d'entiers dits premiers entre eux :

Définition **3.1.3**
Nombres premiers entre eux
Deux entiers $a, b \in \mathbb{Z}$ sont dits premiers entre eux si et seulement si $(a, b) = 1$ (cf. 3.1.2).

BEATRIX : Alors, laissez-moi réfléchir... Par exemple 4 et 9 :
- Diviseurs de 4 : 1, 2, 4.
- Diviseurs de 9 : 1, 3, 9.

Donc 4 et 9 sont premiers entre eux.

EURISTIDE : Voilà, c'est cela.

BEATRIX : Existe-t-il des nombres qui sont premiers avec tous les autres entiers. 1 semble être un de ces nombres, mais y en a-t-il d'autres ?

EURISTIDE : 1 possède un statut particulier. Mais il existe bien des nombres différents de 1 qui sont premiers avec tous les entiers. On les appelle nombres premiers et nous verrons leur définition plus tard.

MATHINE : En attendant, essayons de caractériser un peu plus précisément ce pgcd :

Proposition **3.1.1**
Expression du pgcd
Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Alors, il existe $x_0, y_0 \in \mathbb{Z}$ tels que :

$$(a, b) = ax_0 + by_0. \tag{252}$$

EURISTIDE : Cette proposition nous dit qu'on sait toujours exprimer le pgcd de a et b comme ce qu'on appelle une combinaison linéaire à coefficients entiers a et b. Pour démontrer cette proposition, nous allons considérer l'ensemble de ces combinaisons linéaires de a et b, et montrer que son plus petit élément est le pgcd recherché.

MATHINE : Oui, et nous allons donc procéder comme tout à l'heure, en créant un ensemble bien adapté pour en déterminer le plus petit élément.

Démonstration :

Considérons l'ensemble :

$$E = \{ax + by; x, y \in \mathbb{Z}, ax + by > 0\}. \tag{253}$$

Cet ensemble E est inclus dans $\mathbb{N}$ et est évidemment non vide.
Il possède donc, d'après le principe de bon ordre, un plus petit élément. Notons d ce plus petit élément.
Nous allons démontrer que d est pgcd (cf. 3.1.2) de a et b.
Nous devons donc démontrer les propriétés de la définition du pgcd.

1) Montrons que d divise a :
   Procédons au moyen d'une démonstration par l'absurde. Supposons que $d \nmid a$. Nous pouvons appliquer la division euclidienne (cf. 3.1.2) à a et d, donc il existe $q, r \in \mathbb{Z}$ tels que :

$$a = qd + r \tag{254}$$
$$0 < r < d. \tag{255}$$

   Ceci peut s'écrire :

$$\begin{aligned} r &= a - qd && (256)\\ &= a - q(ax_0 + by_0) && (257)\\ &= a(1 - qx_0) + b(-qy_0). && (258)\end{aligned}$$

   Nous venons de mettre en évidence que $r \in E$. Par ailleurs, nous savons que $r < d$. Donc ceci contredit le fait que d soit le plus petit élément de E. Donc l'hypothèse que $d \nmid a$ est contradictoire. Et par conséquent, $d|a$.
2) Montrons que d divise b :
   Nous devons procéder de la même façon que pour a, en remplaçant a par b dans la démonstration précédente, mutatis mutandis.
3) Montrons que si $c|a$ et $c|b$, alors $c \leq d$:
   Supposons que $c|a$ et $c|b$.
   Alors, nous savons, d'après le théorème (cf. 3.1.1) que $c|ax + by$, pour tout $x, y \in \mathbb{Z}$.
   Donc, en particulier :

$$c|(ax_0 + by_0). \tag{259}$$

   Donc $c|d$.
   Or $d \geq 0$, donc $c \leq d$.

C.Q.F.D.

BEATRIX : Mon intuition me dit que ces nombres $ax + by$ ont quelque chose d'intéressant à dire... N'auraient-ils pas quelque relation privilégiée avec le *pgcd* ?

EURISTIDE : Oui, en effet, Béatrix. Le pgcd est en effet le plus petit élément de l'ensemble des $ax + by$, mais de plus, il les divise tous. Ton intuition te l'a bien dicté : d'une part les multiples de $d = (a, b)$ sont bien de la forme $ax + by$, puisque que nous avons vu que $d = ax_0 + by_0$. D'autre part, un nombre de la forme $ax + by$ est bien multiple de d puisque d divise à la fois a et b.

MATHINE : Nous allons formaliser cela au moyen du corollaire suivant :

Corollaire **3.1.1**
Multiples du pgcd
Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Alors l'ensemble des éléments $ax + by$ où $x, y \in \mathbb{Z}$ est l'ensemble de tous les multiples de $d = (a, b)$.

Démonstration :

1) Supposons que s est multiple de d.
Alors, il existe un entier $n \in \mathbb{Z}$ tel que $s = nd$.
Or, d'après la proposition (cf. 3.1.1), il existe deux entiers x_0, y_0 tels que $d = ax_0 + by_0$. Donc :

$$\begin{aligned} s &= n(ax_0 + by_0) && (260)\\ &= a(nx_0) + b(ny_0). && (261)\end{aligned}$$

Donc s est bien de la forme $ax + by$ où $x, y \in \mathbb{Z}$.

2) Supposons maintenant que s est de la forme $ax + by$, avec $x, y \in \mathbb{Z}$.
Alors $d|a$ et $d|b$. Donc, par définition de la divisibilité (cf. 3.1.1), il existe deux entiers $q, q' \in \mathbb{Z}$ tels qu'on puisse écrire $a = qd$ et $b = q'd$.
D'où :

$$\begin{aligned} ax + by &= (qd)x + (q'd)y && (262)\\ &= d(qx + q'y). && (263)\end{aligned}$$

Donc, s est bien un multiple de d.

C.Q.F.D.

EURISTIDE : Nous pouvons généraliser la notion de pgcd à plus de deux entiers.

MATHINE : Oui, la généralisation du pgcd est possible :

Définition **3.1.4**
Généralisation pgcd
Soit $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, tels que $a_1 a_2 \ldots a_n \neq 0$. On appelle plus grand commun diviseur de a_1, a_2, …, a_n, et on le note pgcd$(a_1, a_2, \ldots, a_n)$ ou $(a_1, a_2, \ldots, a_n)$, l'entier positif d satisfaisant à :
- *$d|a_1$, $d|a_2$, …, $d|a_n$,*
- *si $c|a_1$, $c|a_2$, …, $c|a_n$, alors $c \leq d$.*

BEATRIX : Et je suppose que nous allons retrouver les mêmes propriétés que celles du pgcd de deux entiers : l'écriture sous forme d'une combinaison linéaire, et la forme de ses multiples.

MATHINE : Oui, tout à fait, et c'est ce que nous résumons dans le théorème suivant :

Théorème **3.1.3**
Propriétés pgcd généralisé
Soit $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tels que $a_1 a_2 \ldots a_n \neq 0$. Posons $d = (a_1, a_2, \ldots, a_n)$.
Alors, il existe des entiers $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ tels que :

$$d = (a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} a_i x_i. \tag{264}$$

De plus, d est le plus petit élément positif de la forme $\sum_{i=1}^{n} a_i y_i$ où $y_i \in \mathbb{Z}$ pour $i = 1$ à n.
Enfin, les éléments de la forme $\sum_{i=1}^{n} a_i y_i$ sont les multiples de d.

BEATRIX : Je pense que la démonstration de ce théorème se fait exactement de la même façon que pour les propriétés que nous avons démontrées pour le pgcd de deux entiers. Je suppose qu'il n'est pas utile de la refaire.

EURISTIDE : Oui, nous nous passerons de la démonstration qui ne présente pas d'intérêt par rapport à celles que nous avons déjà vues. Il suffit de procéder exactement de la même façon.

MATHINE : Nous pouvons caractériser le pgcd de deux nombres légèrement différemment par rapport à la définition (cf. 3.1.2) :

Proposition **3.1.2**
Caractérisation pgcd
Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Soit d un entier positif.
Alors :

$$d = (a, b) \Leftrightarrow \begin{cases} d|a & et \quad d|b \\ c|a & et \quad c|b \Rightarrow c|d. \end{cases} \tag{265}$$

EURISTIDE : Autrement dit, nous caractérisons le pgcd comme le diviseur commun à a et b qui est divisible par tous les autres diviseurs communs. Les propriétés que nous avons vues à propos du pgcd nous suggèrent bien évidemment cette caractérisation du fait de la forme de d comme combinaison linéaire de a et b.

BEATRIX : Ah oui, je comprends. Comme d est combinaison linéaire de a et b, un diviseur de a et b divisera nécessairement d. Et inversement, si tous les diviseurs communs de a et b divisent d, a fortiori, d est le plus grand.

MATHINE : Merci, Béatrix. La démonstration n'est maintenant plus qu'un jeu.

Démonstration :

Nous devons démontrer une équivalence entre deux propositions. Donc, nous allons procéder en deux étapes.

1) Supposons que $d = (a, b)$.
Alors, par définition, $d|a$ et $d|b$.
De plus, d'après la proposition sur l'expression du pgcd (cf. 3.1.1), il existe deux entiers x_0, y_0 tels que :

$$d = ax_0 + by_0. \tag{266}$$

Supposons que $c|a$ et $c|b$. Alors il existe q tel que $a = cq$ et q' tel que $b = cq'$.
Donc :

$$\begin{aligned} d &= cqx_0 + cq'y_0 && (267)\\ &= c(qx_0 + q'y_0). && (268)\end{aligned}$$

Donc, $c|d$.

2) Supposons que d soit tel que :

$$\begin{aligned} d|a \quad &\text{et} \quad d|b && (269)\\ c|a \quad &\text{et} \quad c|b \Rightarrow c|d. && (270)\end{aligned}$$

Alors, a fortiori, si $c|d$, alors $c \leq d$. C'est donc que d est le plus grand commun diviseur.

C.Q.F.D.

EURISTIDE : Nous allons maintenant analyser quelques propriétés du pgcd, et ses relations avec l'addition, la multiplication et la divisibilité.

MATHINE : Oui, voici quatre propriétés importantes du pgcd :

Théorème 3.1.4
Propriétés pgcd
Soit $d = (a, b)$. Soit $n \in \mathbb{Z}$.

i) $(a, b + na) = (a, b) = (a, -b)$.

ii) $(an, bn) = |n|(a, b) \qquad (n \neq 0)$.

iii) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

iv) Si $g \in \mathbb{Z} - \{0\}$, tel que $g|a$ et $g|b$, alors :

$$\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{1}{|g|}(a, b). \tag{271}$$

BEATRIX : La première propriété i) est assez évidente. Un diviseur commun à a et $b + na$ est de facto un diviseur commun à a et b, et vice versa.
La propriété iii) est aussi intuitive. Une fois que l'on s'est débarrassé des diviseurs communs entre deux nombres, ils deviennent premiers entre eux, c'est logique.
La propriété iv) est similaire. Une fois que l'on s'est débarrassé d'un certain nombre de diviseurs communs entre a et b, leur pgcd ne comporte plus ces diviseurs communs.

`MATHINE` : Le principe de la démonstration de i) est d'utiliser les propriétés de divisibilité du pgcd $(a, b + na)$ pour en déduire qu'il divise d et vice versa.
Le principe pour ii) consistera à construire le pgcd de (an, bn) en le considérant comme multiple de dn qui divise évidemment les deux entiers. On montre ensuite que ce multiple est 1.
La mise en facteur de d dans le pgcd permet de démontrer la propriété iii).
La propriété iv) se démontre suivant la même méthode la propriété iii).

Démonstration :

Procédons donc propriété par propriété.

i) Soit $d' = (a, b + na)$.
Alors, puisque $d|a$ et $d|b$, alors $d|a$ et $d|b + na$.
Donc, $d|d'$, puisque d est le pgcd.
Mais, par ailleurs $d'|a$ et $d'|b + na$. Donc $d'|a$ et $d'|b$.
Donc $d'|d$.
Donc $d = d'$ ou $d = -d'$. Mais puisque d et d' sont positifs par définition du pgcd, il s'ensuit que $d = d'$.
Soit maintenant $d' = (a, -b)$.
$d|a$ et $d|b$. Donc $d|a$ et $d| - b$. Donc $d|d'$.
$d'|a$ et $d'| - b$, donc $d'|a$ et $d'|b$. Donc $d'|d$.
Donc $d = d'$.

ii) Nous allons subdiviser notre étude en fonction du signe de n :

a) Supposons que $n > 0$.
On sait que $d|a$ et $d|b$.
Donc $dn|an$ et $dn|bn$.
Donc $dn|(an, bn)$, puisque le pgcd est le plus grand diviseur commun.
Donc (an, bn) est un multiple de dn, donc il existe un facteur $k \in \mathbb{Z}$ tel que :

$$(an, bn) = dnk. \tag{272}$$

Donc, $dnk|an$ et $dnk|bn$.
Ce qui signifie que $dk|a$ et $dk|b$.
Donc dk divise le pgcd de a et b :

$$dk|(a, b). \tag{273}$$

Or $(a, b) = d$, donc $k = 1$.
Par conséquent nous pouvons écrire :

$$(an, bn) = dn = n(a, b). \tag{274}$$

b) Supposons que $n < 0$.
Alors, $-n > 0$.
Nous nous ramenons au cas précédent, en écrivant :

$$(an, bn) = (-an, -bn). \tag{275}$$

Donc, finalement :

$$(an, bn) = |n|(a, b). \tag{276}$$

iii) On peut écrire :

$$d = (a,b) \tag{277}$$
$$= \left(d.\frac{a}{d}, d.\frac{b}{d}\right). \tag{278}$$

D'après ii), on a donc :

$$d = |d| \left(\frac{a}{d}, \frac{b}{d}\right). \tag{279}$$

Et puisque $d > 0$:

$$d = d \left(\frac{a}{d}, \frac{b}{d}\right). \tag{280}$$

Donc :

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1. \tag{281}$$

iv) Ecrivons :

$$a = a'g \tag{282}$$
$$b = b'g. \tag{283}$$

Alors :

$$(a,b) = (a'g, b'g). \tag{284}$$

Donc, d'après ii) :

$$(a,b) = |g|(a', b'). \tag{285}$$

Donc, finalement :

$$(a,b) = |g| \left(\frac{a}{g}, \frac{b}{g}\right). \tag{286}$$

C.Q.F.D.

BEATRIX : Je me demande comment on peut calculer facilement le pgcd de deux entiers. Quand ils sont relativement petits, la détermination des diviseurs et leur comparaison est une bonne méthode. Mais elle peut devenir rapidement fastidieuse.

EURISTIDE : C'est la raison pour laquelle il existe un méthode appelée Algorithme d'Euclide, s'appuyant sur la division euclidienne. Pour cela, nous allons utiliser la propriété i) du théorème (cf. 3.1.4).
En effet, en application de cette propriété et de la division euclidienne, nous pouvons écrire successivement :

$$b = aq_1 + r_1. \tag{287}$$

Donc :

$$(a,b) = (a, aq_1 + r_1) = (a, r_1). \tag{288}$$

Puis :

$$a = r_1 q_2 + r_2. \tag{289}$$

Donc :

$$(a, r_1) = (r_1 q_2 + r_2, r_1) = (r_2, r_1). \tag{290}$$

Puis :

$$r_1 = r_2 q_3 + r_3. \tag{291}$$

Donc :

$$(r_2, r_1) = (r_2, r_2 q_3 + r_3) = (r_2, r_3). \tag{292}$$

Le processus finit par s'arrêter lorsque l'on a, pour un j donné :

$$r_{j-1} = r_j q_{j+1}, \tag{293}$$

c'est-à-dire quand r_j se trouve être un diviseur de r_{j-1}. Cet événement, qui au pire se terminera par $r_j = 1$, arrête l'algorithme.
On obtient alors, par égalités successives :

$$(a, b) = (r_{j-1}, r_j). \tag{294}$$

Or, r_j divise r_{j-1}, donc $(r_{j-1}, r_j) = r_j$.
Et par conséquent, nous avons une méthode pour trouver le pgcd de a et b.

`BEATRIX` : C'est astucieux. Je vais prendre un exemple. Cherchons le pgcd de 1234 et 234.

$$\begin{array}{rcrcrcr} 1234 & = & 234 & \times & 5 & + & 64 \\ 234 & = & 64 & \times & 3 & + & 42 \\ 64 & = & 42 & \times & 1 & + & 22 \\ 42 & = & 22 & \times & 1 & + & 20 \\ 22 & = & 20 & \times & 1 & + & 2 \\ 20 & = & 2 & \times & 10 & & . \end{array} \tag{295}$$

Donc $(1234, 234) = 2$.

`EURISTIDE` : A noter que cette méthode permet également de constituer une combinaison entière de 1234 et 234 égale au pgcd. Pour cela, il faut remonter la chaîne des inégalités ci-dessus :

$$\begin{aligned} 2 &= 22 - 20 \times 1 && (296)\\ &= 22 - 20 && (297)\\ &= 22 - (42 - 22 \times 1) && (298)\\ &= 22 - (42 - 22) && (299)\\ &= 22 \times 2 - 42 && (300)\\ &= (64 - 42 \times 1) \times 2 - 42 && (301)\\ &= 64 \times 2 - 42 \times 3 && (302)\\ &= 64 \times 2 - (234 - 64 \times 3) \times 3 && (303)\\ &= 64 \times 11 - 234 \times 3 && (304)\\ &= (1234 - 234 \times 5) \times 10 - 234 \times 3. && (305) \end{aligned}$$

Donc :

$$2 = 1234 \times 11 - 234 \times 58. \tag{306}$$

Ou encore :

$$2 = 1234 \times 11 + 234 \times (-58) \tag{307}$$

BEATRIX : Effectivement, c'est beaucoup moins laborieux qu'avec la recherche des diviseurs. Et en plus, il y a un bonus, puisque nous obtenons une combinaison linéaire exprimant le pgcd.

EURISTIDE : Nous allons maintenant aborder la relation dite de Bezout. Cette propriété va nous permettre de caractériser deux entiers qui sont premiers entre eux.

BEATRIX : Ah oui, c'est très intéressant.

MATHINE : Voici donc le théorème de Bezout.

Théorème 3.1.5 (de Bezout) *Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Alors a et b sont premiers entre eux si et seulement s'il existe $x, y \in \mathbb{Z}$ tels que :*

$$ax + by = 1. \tag{308}$$

BEATRIX : Cette propriété n'est pas très intuitive, à première vue.

EURISTIDE : A première vue, comme tu dis, je te l'accorde. Mais regardons une seconde fois. L'expression $ax + by$ ne te rappelle-t-elle pas quelque chose ?

BEATRIX : Ah oui, c'est une combinaison linéaire des entiers a et b. Je crois comprendre... Si les entiers a et b sont premiers entre eux, leur pgcd est 1, donc on sait trouver une telle combinaison linéaire égale au pgcd, donc à 1. Inversement, comme le pgcd divise a et b, alors il divise forcément $ax + by$ et si cette expression vaut 1, alors le pgcd sera forcément 1. Magique !

MATHINE : Plus formellement :

Démonstration :

Nous allons procéder en deux étapes pour démontrer cette équivalence.

1) Supposons que a et b sont premiers entre eux.
   Alors par définition, leur pgcd (a, b) vaut 1.
   Donc, d'après la proposition (cf. 3.1.1), il existe $x_0, y_0 \in \mathbb{Z}$ tels que :

$$ax_0 + by_0 = 1. \tag{309}$$

   Nous avons donc démontré le caractère nécessaire de la propriété.

2) Supposons qu'il existe $x_0, y_0 \in \mathbb{Z}$ tels que $ax_0 + by_0 = 1$.
Soit d le pgcd de a et b.
Comme $d|a$ et $d|b$, alors $d|ax_0 + by_0$.
Donc $d|1$, et comme $d > 0$, alors $d = 1$. Nous avons démontré le caractère suffisant de la propriété.

3) En conclusion la propriété est nécessaire et suffisante.

C.Q.F.D.

EURISTIDE : Une propriété intéressante concerne le produit de deux nombres premiers relativement à un troisième. A ton avis, Béatrix, qu'en est-il du produit ?

BEATRIX : Si ces deux nombres n'ont pas de diviseurs $\neq 1$ communs avec le troisième, je ne vois pas comment leur produit pourrait en avoir un. Donc, je dirais que le produit est également premier avec ce troisième entier.

MATHINE : C'est exact. La réciproque est également vraie.

Proposition 3.1.3
Produit d'entiers premiers avec un troisième
Soit $a, b \in \mathbb{Z} - \{0\}$. *Soit* $n \in \mathbb{Z} - \{0\}$.
Alors :

$$(a, n) = (b, n) = 1 \Leftrightarrow (ab, n) = 1. \tag{310}$$

EURISTIDE : Le principe de la démonstration va consister à utiliser la relation de Bezout. Il se trouve qu'en écrivant une relation de Bezout pour ab et n, on écrit une relation de Bezout valide pour a et n d'une part, et b et n d'autre part.

MATHINE : Oui, c'est cette stratégie de démonstration que nous allons suivre.

Démonstration :

Dire que $(ab, n) = 1$ est équivalent à dire qu'il existe des entiers $x_0, y_0 \in \mathbb{Z}$ tels que :

$$ab.x_0 + n.y_0 = 1. \tag{311}$$

On peut écrire, de façon équivalente, cette égalité sous les deux formes suivantes :

$$\left\{ \begin{array}{rcl} a(bx_0) + ny_0 & = & 1 \\ b(ax_0) + ny_0 & = & 1, \end{array} \right. \tag{312}$$

ce qui est équivalent à :

$$\left\{ \begin{array}{rcl} (a, n) & = & 1 \\ (b, n) & = & 1. \end{array} \right. \tag{313}$$

C.Q.F.D.

EURISTIDE : Une autre propriété intuitive. Si un entier divise un produit et si cet entier est premier avec l'un des facteurs du produit, qu'advient-il de l'autre facteur ?

BEATRIX : Voyons... Notre entier est premier avec un des facteurs, donc il n'a aucun diviseur $\neq 1$ commun avec celui-ci. Donc tout diviseur se retrouve nécessairement dans le deuxième facteur. Donc je dis que l'entier divise le second facteur.

MATHINE : Il s'agit d'une propriété appelée Lemme d'Euclide.

Lemme **3.1.1 (d'Euclide)** *Soit $a, b, c \in \mathbb{Z} - \{0\}$.*
Si $a|bc$ et $(a, b) = 1$, alors $a|c$.

Démonstration :

Nous allons utiliser de nouveau la relation de Bezout.
Si $(a, b) = 1$, alors il existe $x_0, y_0 \in \mathbb{Z}$ tels que :

$$ax_0 + by_0 = 1. \tag{314}$$

Alors, en multipliant par c cette égalité, nous obtenons :

$$acx_0 + bcy_0 = c. \tag{315}$$

Or, $a|bc$, donc $a|(acx_0 + bcy_0)$.
Donc, d'après l'égalité ci-dessus, $a|c$.

C.Q.F.D.

BEATRIX : Nous avons beaucoup parlé de pgcd. Il me semble qu'il existe aussi une notion de plus petit commun multiple, non ?

EURISTIDE : Oui, et c'est naturel. A partir du moment où une collection d'entiers possèdent des multiples communs, il est naturel de s'intéresser au plus petit d'entre eux.

MATHINE : Encore une fois, le principe du bon ordre nous le permet.

Définition **3.1.5**
Plus petit commun multiple
Soit $a_1, a_2, \ldots, a_n \in \mathbb{Z} - \{0\}$. On dit que m est un commun multiple de $a_1, a_2, \ldots, a_n$ si $a_i|m$ pour tout i de

1 à n. Le plus petit commun multiple (ppcm) de $a_1, a_2, \ldots, a_n$, noté $ppcm(a_1, a_2, \ldots, a_n)$ ou $[a_1, a_2, \ldots, a_n]$, est le plus petit entier positif parmi tous les communs multiples de $a_1, a_2, \ldots, a_n$.

BEATRIX : D'accord, je comprends.
Par exemple, si je considère les entiers 4, 6 et 8, on voit que 8 est multiple de 4, mais pas de 6. Si on prend 12, il est multiple de 4 et 6, mais pas de 8. Nous sommes obligés de prendre 24 qui est à la fois multiple de 4, 6 et 8, et qui semble être le plus petit commun multiple.
Comment calcule-t-on un ppcm ?

EURISTIDE : Une technique consiste à décomposer 4, 6 et 8 en leurs diviseurs et trouver les diviseurs qu'il faut agglutiner pour obtenir un nombre multiple de tous les entiers qui soit le plus petit possible :

$$4 = 2 \times 2 \tag{316}$$
$$6 = 3 \times 2 \tag{317}$$
$$8 = 2 \times 2 \times 2. \tag{318}$$

Cette présentation nous montre que le ppcm doit être divisible par 8, et qu'il suffit de le multiplier par 3 pour obtenir le ppcm.

BEATRIX : Mais ce n'est ni rigoureux ni fiable.

EURISTIDE : Je te l'accorde. Nous allons d'abord démontrer quelques propriétés du ppcm. Elles nous permettront de trouver une technique de calcul à partir du pgcd.

MATHINE : Voici donc un premier lot de propriétés.

Proposition 3.1.4
Propriétés PPCM
Soit $a_1, a_2, \ldots, a_n \in \mathbb{Z} - \{0\}$.
Soit $m, k \in \mathbb{N} - \{0\}$.

i) Si m est un commun multiple de $a_1, a_2, \ldots, a_n$, alors $[a_1, a_2, \ldots, a_n] | m$.

ii) Si $k > 0$, alors $[ka_1, ka_2, \ldots, ka_n] = k[a_1, a_2, \ldots, a_n]$.

iii) $[a, b].(a, b) = |ab|$.

EURISTIDE : Les deux premières propriétés sont relativement prévisibles. Pour la première propriété, il est assez intuitif, à l'instar de ce que nous avons vu pour le pgcd, que le plus petit commun multiple divise tout autre multiple commun ; sinon, il ne serait pas le plus petit. La seconde propriété est triviale : en multipliant tous les nombres par un même entier, nous sommes obligés de multiplier le ppcm des nombres initiaux par le même coefficient pour trouver le ppcm de ces nouveaux nombres.
La troisième propriété est plus surprenante. Du moins, surprenante tant qu'on y a pas encore réfléchi.

BEATRIX : Oui, je devine ce qui se cache derrière cette troisième propriété. Quand on multiplie les

deux entiers a et b, on obtient de toute évidence un multiple commun. Mais ce multiple commun n'est vraisemblablement pas le plus petit, car nous n'avons pas tenu compte de diviseurs qui seraient en commun dans les entiers a et b. Justement, ces diviseurs communs n'ont pas besoin d'être répétés dans le ppcm, car sinon ce ne serait pas le plus petit. Alors justement, puisqu'on parle de diviseurs communs, il faut les neutraliser. Le meilleur moyen de les neutraliser, c'est d'en enlever le plus grand nombre, donc de diviser le produit par le pgcd. C'est ce qui nous permet d'obtenir le ppcm.

`EURISTIDE` : Félicitations, Béatrix, c'est bien cela qui se passe. Evidemment, ton explication ne constitue pas une démonstration, mais elle est bien utile pour comprendre le sens de cette relation.

`MATHINE` : La démonstration de i) va s'appuyer sur la division euclidienne, où nous viserons à montrer que le reste est nul grâce aux propriétés des multiples communs.
La propriété ii) se démontre en comparant le ppcm multiplié par le coefficient et le ppcm des entiers multipliés. C'est assez facile.
La propriété iii) se démontre en considérant d'abord le cas où a et b sont premiers entre eux. Puis on se ramène du cas général à celui-ci en divisant les deux entiers par le pgcd.

Démonstration :

Procédons par étape pour chaque propriété.

i) Désignons par l le ppcm :
$$l = [a_1, a_2, \ldots, a_n]. \tag{319}$$
Effectuons la division euclidienne de m par l :
$$m = ql + r. \tag{320}$$
Nous cherchons à montrer que $r = 0$.
Procédons au moyen d'une démonstration par l'absurde.
Supposons que $r \neq 0$.
Nous savons que tous les a_i divisent m et tous les a_i divisent q.
Donc, puisque :
$$r = m - ql, \tag{321}$$
nécessairement, tous les a_i divisent r.
Donc r est un multiple commun des a_i.
Mais $r < l$, d'après la division euclidienne. Donc nous avons trouvé un multiple commun plus petit que le ppcm. C'est contradictoire.
Donc l'hypothèse $r \neq 0$ est fausse et par conséquent $r = 0$.
Donc $[a_1, a_2, \ldots, a_n] | m$.

ii) Désignons :
$$l = [a_1, a_2, \ldots, a_n] \tag{322}$$
$$m = [ka_1, ka_2, \ldots, ka_n]. \tag{323}$$
Il s'ensuit que kl est multiple de tous les ka_i, puisque l est le ppcm des a_i.
Donc $m \leq kl$.
Par ailleurs, m est multiple de tous les ka_i.
Donc $\frac{m}{k}$ est multiple de tous les a_i.
Donc $l \leq \frac{m}{k}$, c'est-à-dire $lk \leq m$.
Donc finalement, $m = kl$.

iii) Il suffit de montrer la propriété pour les entiers positifs, parce que :

$$(a, b) = (a, -b), \tag{324}$$

et :

$$[a, b] = [a, -b]. \tag{325}$$

a) Commençons par considérer le cas où $(a, b) = 1$, c'est-à-dire le cas où a et b sont premiers entre eux. Nous savons que $[a, b]$ est multiple de a. Donc on peut écrire :

$$[a, b] = ma. \tag{326}$$

Donc $b|ma$.
Comme $(a, b) = 1$, il s'ensuit que $b|m$, d'après le Lemme d'Euclide (cf. 3.1.1).
Donc $b \leq m$ et par conséquent $ab \leq am$.
Donc, nous avons montré que :

$$ab \leq [a, b]. \tag{327}$$

Or, $[a, b]$ est le plus petit commun multiple de a et b, donc nécessairement :

$$ab = [a, b]. \tag{328}$$

Comme $(a, b) = 1$, nous avons bien vérifié que :

$$ab = (a, b).[a, b]. \tag{329}$$

b) Prenons le cas général $(a, b) = d$.
Nous savons, d'après le théorème (cf. 3.1.4), qu'alors :

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1. \tag{330}$$

Nous pouvons alors appliquer le résultat a) :

$$\left(\frac{a}{d}, \frac{b}{d}\right)\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{a}{d}.\frac{b}{d}. \tag{331}$$

En multipliant cette égalité par d^2, nous obtenons :

$$[a, b](a, b) = ab. \tag{332}$$

C.Q.F.D.

3.2 Scène III.2 - Nombres premiers

EURISTIDE : Nous allons maintenant regarder de près des nombres particuliers, passionnants et un peu mystérieux : les nombres premiers. Ce sont des nombres qui n'ont pas d'autres diviseurs que 1 et eux-mêmes.

BEATRIX : Oui, je connais. Autant considérer qu'ils n'ont pas de diviseurs, puisque 1 et eux-mêmes ne sont pas des diviseurs vraiment significatifs.

EURISTIDE : Ce que ces nombres ont de mystérieux, c'est que leur répartition est imprévisible. Voici pour illustration les 100 premiers nombres premiers :

$$\begin{array}{l} 2, 3, 5, 7 \\ 11, 13, 17, 19 \\ 23, 29 \\ 31, 37 \\ 41, 43, 47 \\ 53, 59 \\ 61, 67 \\ 71, 73, 79 \\ 83, 89 \\ 97. \end{array} \tag{333}$$

Comme on le voit, leur répartition n'est pas régulière. Parfois ils sont quatre par dizaine, parfois trois ou deux, voire un.

BEATRIX : Etrange, non ?

EURISTIDE : Ces nombres sont très importants parce qu'ils vont nous permettre de décomposer un entier de façon unique en facteurs irréductibles. Ce sera donc une façon canonique de représenter les nombres entiers.

MATHINE : Mais commençons par les définir.

Définition **3.2.1**
Nombre premier
On dit qu'un entier $p > 1$ est un nombre premier si ses seuls diviseurs sont 1 et p.
Un entier plus grand que 1 qui n'est pas premier est dit composé .

EURISTIDE : Voilà. Nous avons la définition d'un nombre premier conforme à ce que nous disions tout à l'heure. Le terme composé est tout à fait approprié, puisque nous verrons que les nombres composés se décomposent en facteurs premiers.

MATHINE : Commençons par étudier les propriétés de ces nombres premiers.

Théorème **3.2.1**
Nombre premier divisant un produit
Soit $p \in \mathbb{N}$ et $a, b \in \mathbb{Z}$.
Si p est premier et $p|ab$ alors $p|a$ ou $p|b$

BEATRIX : C'est assez intuitif : comme p est premier, il ne peut être décomposé en 2 ou plusieurs diviseurs. Donc p est entièrement diviseur de a ou entièrement diviseur de b, ou entièrement diviseur des deux, mais il n'y a pas de diviseurs de p qui puissent être répartis entre les deux nombres a et b.

MATHINE : C'est l'idée.

Démonstration :

i) Supposons que $p|a$. Alors le résultat est vérifié.

ii) Supposons maintenant que $p \nmid a$.
Comme les seuls diviseurs de p sont 1 et p, alors $(a, p) = 1$.
Nous pouvons appliquer le Lemme d'Euclide (cf. 3.1.1), puisque $p|ab$ et $(a, p) = 1$.
Donc $p|b$.

C.Q.F.D.

EURISTIDE : Cette propriété est évidemment généralisable à plus de deux nombres.

BEATRIX : Alors, je vais tenter de prendre un exemple pour illustrer cela. 3 divise $6 \times 8 \times 52$. Et il se trouve que $3|6$.

EURISTIDE : Nous pouvons considérer une situation restrictive où les entiers sont tous premiers, c'est-à-dire que si un nombre premier p divise un produit de nombres premiers, alors ce nombre premier p divise nécessairement l'un des nombres premiers. Et comme c'est un nombre premier justement, ceci entraîne que p est égal au nombre premier en question.

MATHINE : En formalisant cette idée, nous obtenons la proposition suivante.

Proposition **3.2.1**
Produit de nombres premiers
Si $p, p_1, p_2, \ldots, p_n$ sont des nombres premiers, et si $p|p_1p_2 \ldots p_n$, alors il existe au moins un k compris entre 1 et n tel que $p = p_k$.

Démonstration :

En utilisant le théorème (cf. 3.2.1), nous déduisons qu'il existe $k \in [1, n]$ tel que :

$$p|p_k. \tag{334}$$

Or, p_k est premier, donc $p = 1$ ou $p = p_k$.
Or p est premier également, donc $p_k \neq 1$.

Donc $p = p_k$.

C.Q.F.D.

EURISTIDE : Nous allons maintenant démontrer un théorème très important qui indique que tout entier positif > 1 peut se décomposer de façon unique en un produit de nombres premiers.

BEATRIX : C'est tout à fait naturel. Partant d'un nombre donné, on peut le diviser autant de fois qu'il faut par des nombres premiers, tant qu'on le peut. On finira par épuiser les diviseurs du nombre donné et compléter la décomposition.

EURISTIDE : C'est effectivement l'idée de cette propriété. Mais ta description constitue plus une façon de procéder qu'une réelle démonstration. Mathine nous donnera la démonstration dans quelques instants, et celle-ci repose encore une fois sur le principe de bon ordre. En attendant, nous allons construire une telle décomposition en nous appuyant sur l'algorithme de Béatrix. A toi de jouer, Béatrix ?

BEATRIX : Décomposons par exemple 2772.
Je rappelle que les dix premiers nombres premiers sont :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29. \tag{335}$$

Essayons d'abord la division par 2 :

$$2772/2 = 1386 \tag{336}$$
$$1386/2 = 693. \tag{337}$$

Nous avons épuisé les possibilités de diviser par 2. Passons à 3.

$$693/3 = 231 \tag{338}$$
$$231/3 = 77. \tag{339}$$

Nous avons épuisé les possibilités de diviser par 3. Passons à 5. 77 n'est pas divisible par 5. Passons à 7.

$$77/7 = 11. \tag{340}$$

Ce dernier entier 11 est premier. Donc nous avons fini :

$$2772 = 2^3.3^2.7.11. \tag{341}$$

Et voilà.

MATHINE : Nous allons maintenant énoncer et démontrer le théorème de la décomposition des entiers en facteurs premiers.

Théorème 3.2.2
Décomposition en facteurs premiers
Tout entier naturel > 1 peut s'écrire de façon unique sous la forme :

$$n = q_1^{a_1} q_2^{a_2} \dots q_r^{a_r}, \tag{342}$$

où les q_i sont des nombres premiers distincts tels que $q_1 < q_2 < \dots < q_r$, et où les a_i sont des entiers positifs.

Démonstration :

1) Supposons que n est premier. Alors le théorème est démontré.
2) Supposons maintenant que n est composé.
Nous pouvons considérer l'ensemble E défini par :

$$E = \{d \in \mathbb{N}; d|n \quad \text{et} \quad 1 < d < n\}. \tag{343}$$

Alors E est inclus dans $\mathbb{N}$ et non vide. Donc, d'après le principe du bon ordre, il possède un plus petit élément.
Notons p_1 cet élément.
Si p_1 n'était pas premier, alors il existerait x et y tels que $xy = p_1$, et donc x ou y pourraient être éléments de E plus petits que p_1. Ce serait contradictoire. Donc p_1 est premier.
Donc, nous pouvons écrire :

$$n = p_1 n_1. \tag{344}$$

Si n_1 est premier, alors le théorème est démontré.
Sinon, nous reprenons le même algorithme avec n_1, et nous identifions p_2 premier, tel que :

$$n = p_1 p_2 n_2. \tag{345}$$

Nous procédons ainsi de suite.
Le processus a-t-il une fin ? Oui, nécessairement, car $n_1, n_2, \ldots, n_k$ est une suite décroissante d'entiers diviseurs les uns des autres, et elle possède nécessairement un plus petit élément, différent de 1, qui n'est plus réductible, donc premier.
Par conséquent, nous avons écrit n sous la forme :

$$n = p_1 p_2 \ldots p_k, \tag{346}$$

à la fin du processus.
Il s'agit maintenant de démontrer que la décomposition est unique.
Supposons qu'il y en ait deux :

$$n = p_1 p_2 \ldots p_k \tag{347}$$
$$n = p'_1 p'_2 \ldots p'_l. \tag{348}$$

Alors :

$$p_1 p_2 \ldots p_k = p'_1 p'_2 \ldots p'_l. \tag{349}$$

Si des facteurs premiers sont présents et identiques à la fois à gauche et à droite de l'égalité, nous pouvons simplifier l'égalité en ôtant ces facteurs dans les deux membres de l'égalité.
Nous pouvons donc réécrire l'égalité en considérant que tous les facteurs premiers sont différents de part et d'autre de l'égalité :

$$q_1 q_2 \ldots q_r = q'_1 q'_2 \ldots q'_s. \tag{350}$$

Alors, en particulier, nous aurions pour un i choisi arbitrairement :

$$q_i | q'_1 q'_2 \ldots q'_s. \tag{351}$$

Mais, d'après la proposition (cf. 3.2.1), cela implique qu'il existe $1 \leq j \leq s$ tel que :

$$q_i = q'_j. \tag{352}$$

Ce qui est contradictoire avec notre construction.
Donc, notre hypothèse est fausse. Par conséquent la décomposition est bien unique.

C.Q.F.D.

EURISTIDE : La décomposition d'un entier en facteurs premiers sous cette forme est appelée représentation canonique de l'entier. Cette forme bien utile, va nous permettre de représenter les diviseurs et multiples d'un entier de façon très aisée.

BEATRIX : Oui, je crois bien que les diviseurs d'un entier seront représentés par une portion de la représentation canonique du dividende, c'est-à-dire qu'on trouvera dans la représentation du diviseur les mêmes nombres premiers, avec des puissances inférieures ou nulles, que dans la représentation du dividence.

EURISTIDE : Pour les multiples, la représentation comportera les mêmes nombres premiers, avec des puissances supérieures et éventuellement de nouveaux nombres premiers avec leurs propres puissances.
A ton avis, Béatrix, comment allons nous représenter le pgcd et le ppcm ?

BEATRIX : Voyons... Le pgcd de deux entiers est un diviseur. Mais c'est le plus grand. Il devra nécessairement comporter les facteurs premiers qui ne sont pas présents dans l'un des deux nombres, mais dans l'autre, à la puissance à laquelle il se trouve. Pour les facteurs premiers communs aux deux représentations canoniques, s'ils sont présents à deux puissances différentes, il faudra prendre la plus petite des deux. Cela nous assurera qu'aucun diviseur commun ne sera plus grand. Donc, en résumé, le pgcd sera le produit des facteurs premiers présents dans l'un des deux nombres, à la puissance la plus petite des deux.

EURISTIDE : Bien. Et le ppcm ?

BEATRIX : On a besoin que chacun des facteurs premiers couvre chacun des deux facteurs des deux nombres. Donc il faudra prendre la puissance la plus élevée pour les facteurs premiers des deux nombres.

MATHINE : C'est exact. Voici donc la proposition relative à la décomposition canonique d'un diviseur.

Proposition 3.2.2
Représentation canonique diviseur
Soit $n = \prod_{i=1}^{n} q_i^{a_i}$, $a_i > 0$ *pour tout* $i \in [1, r]$.
Soit $d > 0$. *Alors* d *divise* n *si et seulement si :*

$$d = \prod_{i=1}^{r} q_i^{b_i}, \tag{353}$$

où les b_i *sont des entiers naturels tels que :*

$$\forall i \in [1, n], b_i \leq a_i. \tag{354}$$

La démonstration se fait par un calcul direct sur la représentation canonique.

Démonstration :

Nous allons procéder en deux étapes : d'abord montrer que si d est de la forme indiquée, c'est un diviseur de n, puis montrer que les diviseurs de n sont bien de la forme indiquée.

1) Supposons que $d = \prod_{i=1}^{r} q_i^{b_i}$, alors nous pouvons écrire :

$$\begin{aligned} n &= \prod_{i=1}^{r} q_i^{a_i} && (355)\\ &= \prod_{i=1}^{r} q_i^{a_i - b_i + b_i} && (356)\\ &= \prod_{i=1}^{r} q_i^{a_i - b_i} \prod_{i=1}^{r} q_i^{b_i} && (357)\\ &= \left(\prod_{i=1}^{r} q_i^{a_i - b_i} \right) .d. && (358) \end{aligned}$$

Donc n est bien divisible par d.

2) Supposons que $d|n$.
Alors, il existe un entier q tel que :

$$n = qd. \quad (359)$$

Considérons la représentation canonique de d :

$$d = \prod_{i=1}^{r} q_i^{d_i}, \quad (360)$$

et celle de q :

$$q = \prod_{i=1}^{r} q_i^{s_i}. \quad (361)$$

Ici, il faut bien noter que nous avons adopté pour l'indice maximal r, le plus grand des indices des trois représentations canoniques, ce qui nous permet a priori d'avoir la même indexation pour trois représentations canoniques.
En faisant le produit de la représentation canonique de d et celle de q, nous obtenons :

$$\begin{aligned} n &= qd && (362)\\ &= \prod_{i=1}^{r} q_i^{d_i} \prod_{i=1}^{r} q_i^{s_i} && (363)\\ &= \prod_{i=1}^{r} q_i^{d_i + s_i}. && (364) \end{aligned}$$

Donc, pour tout $i \in [1, r]$, nous avons :

$$a_i = d_i + s_i. \quad (365)$$

Donc, finalement $d_i \leq a_i$.

C.Q.F.D.

EURISTIDE : Voici la première proposition énoncée et démontrée.

MATHINE : Passons maintenant à la proposition concernant la représentation canonique du pgcd et du ppcm.

Proposition 3.2.3
Représentation canonique pgcd et ppcm
Soit $a = \prod_{i=1}^{r} q_i^{a_i}$ *et* $b = \prod_{i=1}^{r} q_i^{b_i}$.
Alors :

$$pgcd(a,b) = \prod_{i=1}^{r} q_i^{min(a_i,b_i)} \tag{366}$$

$$ppcm(a,b) = \prod_{i=1}^{r} q_i^{max(a_i,b_i)}. \tag{367}$$

EURISTIDE : La démonstration se fait simplement en appliquant la définition du pgcd. Puis la relation concernant le ppcm se déduit de l'égalité suivante :

$$ab = (a,b).[a,b], \tag{368}$$

que nous avons vue dans la proposition (cf. 3.1.4).

MATHINE : Voici la démonstration de cette proposition, en deux étapes : d'abord le pgcd, puis le ppcm.

Démonstration :

1) Ecrivons la décomposition canonique de d :

$$d = \prod_{i=1}^{r} q_i^{d_i}, \tag{369}$$

où $d_i = min(a_i, b_i)$.
Puisque $d_i \leq a_i$ et $d_i \leq b_i$, compte tenu de la proposition précédente (cf. 3.2.2), nous savons que :

$$d|a \quad \text{et} \quad d|b. \tag{370}$$

Soit m un diviseur commun de a et b.
Alors $m|a$ et $m|b$.

Alors, en considérant $m > 0$:

$$m = \prod_{i=1}^{r} q_i^{m_i}, \tag{371}$$

avec, pour tout $i \in [1, r]$:

$$m_i \leq a_i \tag{372}$$
$$m_i \leq b_i. \tag{373}$$

Or, $d_i = min(a_i, b_i)$, donc nécessairement :

$$m_i \leq d_i. \tag{374}$$

Donc $m|d$.
Donc d est bien le pgcd de a et b.

2) Nous savons que :

$$ab = (a, b).[a, b]. \tag{375}$$

Soit :

$$[a, b] = \prod_{i=1}^{r} q_i^{m_i} \tag{376}$$

la décomposition canonique du ppcm.
Alors :

$$\prod_{i=1}^{r} q_i^{a_i} \prod_{i=1}^{r} q_i^{b_i} = \prod_{i=1}^{r} q_i^{min(a_i,b_i)} \prod_{i=1}^{r} q_i^{m_i}. \tag{377}$$

D'où, pour tout $i \in [1, r]$:

$$a_i + b_i = min(a_i, b_i) + m_i. \tag{378}$$

Or :

$$a_i + b_i = min(a_i, b_i) + max(a_i, b_i). \tag{379}$$

Donc, par identification des termes de ces deux égalités, nous obtenons :

$$m_i = max(a_i, b_i). \tag{380}$$

C.Q.F.D.

3.3 Scène III.3 - Crible d'Eratosthène

BEATRIX : Nous avons beaucoup parlé des nombres premiers en théorie. Mais j'aimerais bien savoir comment on les détermine. On a vu que leur répartition n'est pas prévisible ; mais il doit bien y avoir un moyen de les calculer.

EURISTIDE : Le moyen encore utilisé aujourd'hui est la méthode employée par Eratosthène durant l'Antiquité. Cette méthode consiste à supprimer progressivement les multiples des entiers identifiés comme non premiers, dans un grand tableau, pour n'y laisser que les nombres premiers. On appelle cette méthode le crible d'Eratosthène.

Illustrons cela pour déterminer les 100 premiers nombres premiers. On commence par écrire dans un tableau les cent premiers entiers naturels :

$$\begin{array}{cccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\
21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\
31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\
41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 \\
51 & 52 & 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 \\
61 & 62 & 63 & 64 & 65 & 66 & 67 & 68 & 69 & 70 \\
71 & 72 & 73 & 74 & 75 & 76 & 77 & 78 & 79 & 80 \\
81 & 82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 \\
91 & 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100
\end{array} \tag{381}$$

Puis, on supprime 1 qui n'est pas un nombre premier.
Le premier nombre non supprimé est 2. C'est donc un nombre premier. On le souligne. On barre alors dans le tableau tous les entiers multiples de 2 :

$$\begin{array}{cccccccccc}
\not{1} & \underline{2} & 3 & \not{4} & 5 & \not{6} & 7 & \not{8} & 9 & \not{10} \\
11 & \not{12} & 13 & \not{14} & 15 & \not{16} & 17 & \not{18} & 19 & \not{20} \\
21 & \not{22} & 23 & \not{24} & 25 & \not{26} & 27 & \not{28} & 29 & \not{30} \\
31 & \not{32} & 33 & \not{34} & 35 & \not{36} & 37 & \not{38} & 39 & \not{40} \\
41 & \not{42} & 43 & \not{44} & 45 & \not{46} & 47 & \not{48} & 49 & \not{50} \\
51 & \not{52} & 53 & \not{54} & 55 & \not{56} & 57 & \not{58} & 59 & \not{60} \\
61 & \not{62} & 63 & \not{64} & 65 & \not{66} & 67 & \not{68} & 69 & \not{70} \\
71 & \not{72} & 73 & \not{74} & 75 & \not{76} & 77 & \not{78} & 79 & \not{80} \\
81 & \not{82} & 83 & \not{84} & 85 & \not{86} & 87 & \not{88} & 89 & \not{90} \\
91 & \not{92} & 93 & \not{94} & 95 & \not{96} & 97 & \not{98} & 99 & \not{100}
\end{array} \tag{382}$$

Le prochain nombre non barré est 3. C'est donc un nombre premier. On le souligne. On barre alors tous les multiples de 3 :

$$\begin{array}{cccccccccc}
\not{1} & \underline{2} & \underline{3} & \not{4} & 5 & \not{6} & 7 & \not{8} & \not{9} & \not{10} \\
11 & \not{12} & 13 & \not{14} & \not{15} & \not{16} & 17 & \not{18} & 19 & \not{20} \\
\not{21} & \not{22} & 23 & \not{24} & 25 & \not{26} & \not{27} & \not{28} & 29 & \not{30} \\
31 & \not{32} & \not{33} & \not{34} & 35 & \not{36} & 37 & \not{38} & \not{39} & \not{40} \\
41 & \not{42} & 43 & \not{44} & \not{45} & \not{46} & 47 & \not{48} & 49 & \not{50} \\
\not{51} & \not{52} & 53 & \not{54} & 55 & \not{56} & \not{57} & \not{58} & 59 & \not{60} \\
61 & \not{62} & \not{63} & \not{64} & 65 & \not{66} & 67 & \not{68} & \not{69} & \not{70} \\
71 & \not{72} & 73 & \not{74} & \not{75} & \not{76} & 77 & \not{78} & 79 & \not{80} \\
\not{81} & \not{82} & 83 & \not{84} & 85 & \not{86} & \not{87} & \not{88} & 89 & \not{90} \\
91 & \not{92} & \not{93} & \not{94} & 95 & \not{96} & 97 & \not{98} & \not{99} & \not{100}
\end{array} \tag{383}$$

On continue, ainsi de suite.

BEATRIX : On continue, oui, mais quand s'arrête-t-on ? Quand nous sommes arrivés à n'avoir aucun nombre ni barré, ni souligné ?

EURISTIDE : On peut s'arrêter avant cela. Nous cherchons tous les entiers premiers inférieurs ou égaux à n (ici, $n = 100$). Supposons que nous ayons rempli le tableau de barrés et de soulignés jusqu'à l'entier premier le plus grand $\leq \sqrt{n}$. Si un entier $m \leq n$ est composé, et s'il comporte un nombre premier supérieur $\sqrt{n}$, alors forcément, puisque $\sqrt{n}.\sqrt{n} = n$, il y aura un autre nombre premier dans sa décomposition qui est

inférieur à $\sqrt{n}$. Cela signifie que nous l'avons déjà barré lors d'un précédent passage. Il est donc inutile de poursuivre l'opération au delà de $\sqrt{n}$.

`BEATRIX` : D'accord, donc je continue. Le prochain nombre non barré est 5. C'est donc un nombre premier. Je le souligne. Je barre alors les multiples de 5 :

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

(384)

Le prochain entier non barré est 7. C'est donc un nombre premier. Je le souligne. Et je barre tous les multiples de 7 :

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

(385)

Le prochain entier non barré est 11. C'est donc...

`EURISTIDE` : Béatrix, je t'interromps. 11 est supérieur à $\sqrt{100}$. C'est donc inutile de vérifier à partir de maintenant. D'ailleurs, tu vois facilement que tous les multiples de 11 : 22, 33, etc. sont déjà barrés.
Il nous reste à souligner les nombres non barrés qui restent, et qui sont nécessairement premiers :

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

(386)

BEATRIX : D'où les nombres premiers inférieurs à 100 :

$$\begin{array}{llllllll} 2; & 3; & 5; & 7; & 11; & 13; & 17; & 19; \\ 23; & 29; & 31; & 37; & & & & \\ 41; & 43; & 47; & 53; & 59; & & & \\ 61; & 67; & 71; & 73; & 79; & & & \\ 83; & 89; & 97 & & & & & \end{array} \tag{387}$$

3.4 Scène III.4 - Infinité des nombres premiers

EURISTIDE : A ton avis, Béatrix, combien y-a-t-il de nombres premiers ?

BEATRIX : Je crois bien qu'il y en a une infinité.

MATHINE : Tu as raison. La démonstration de cette affirmation est due à Euclide. C'est une démonstration par l'absurde, et elle consiste à faire l'hypothèse qu'il existe un nombre fini de nombres premiers, et à construire un nombre premier nouveau à partir de la collection finie des nombres premiers.

Théorème **3.4.1 (d'Euclide)** *Il existe une infinité de nombres premiers.*

Démonstration :

La démonstration se fait effectivement par l'absurde.
Supposons que le nombre de nombres premiers soit fini et égal à m.
Notons les nombres premiers $p_1, p_2, \ldots, p_n$.
Considérons le nombre :

$$p = p_1 p_2 \ldots p_n + 1. \tag{388}$$

Considérons deux cas :

1) Ou bien p est premier, alors nous avons trouvé un nombre premier supplémentaire, ce qui contredit l'hypothèse.
2) Ou bien p est composé.
   Alors, il existe nécessairement un nombre premier qui le divise, donc un $j \in [1, n]$ tel que :

$$p = mp_j. \tag{389}$$

Donc :

$$mp_j = \left(\prod_{i=1 i \neq j}^{n} p_i \right) .p_j + 1, \tag{390}$$

donc :

$$1 = \left(m - \prod_{i=1 i \neq j}^{n} \right) p_j. \tag{391}$$

Par conséquent, p_j divise 1. Ce qui est contradictoire.

Par conséquent, dans tous les cas, l'hypothèse d'un nombre fini de nombres premiers aboutit à la création d'un nouveau nombre premier strictement supérieur à tous les autres, c'est-à-dire aboutit à une contradiction.
Donc il existe une infinité de nombres premiers.

C.Q.F.D.

BEATRIX : Cette démonstration est vraiment belle ! C'est bien le genre de démonstration qui vous fait aimer les mathématiques : simple, astucieuse...

EURISTIDE : Je suis tout à fait d'accord.

BEATRIX : Si je comprends bien la démonstration précédente, le produit de tous les nombres premiers jusqu'à un certain rang, auquel on ajoute 1 est toujours un nombre premier ? Autrement dit :

$$p = p_1 p_2 \dots p_n + 1, \tag{392}$$

pour tout n, serait un nombre premier ?

EURISTIDE : Attention ! Tu es tombée dans un joli piège. Dans la démonstration d'Euclide, nous faisions l'hypothèse que les seuls nombres premiers sont les $p_1, p_2, \dots, p_n$. C'est ce qui nous a permis de dire que lorsque p est composé, il s'écrit nécessairement $p = mp_j$, où $j \in [1, n]$.
Mais, en réalité, nous sommes dans une situation toute différente, et si p est composé, il peut être facteur d'un nombre premier compris entre p_n et $p = p_1 p_2 \dots p_n + 1$. Et dans ce cas le raisonnement d'Euclide ne peut pas se faire, et la contradiction ne peut plus se présenter.
Vérifions le sur quelques valeurs de n, en calculant la somme des n premiers nombres premiers à laquelle nous ajoutons 1.

$$p = 2 + 1 = 3. \tag{393}$$

BEATRIX : 3 est premier. Donc la propriété est vérifiée.

EURISTIDE : $p = 2 \times 3 + 1 = 7$.

BEATRIX : 7 est aussi un nombre premier. La propriété est toujours vraie.

EURISTIDE : $p = 2 \times 3 \times 5 + 1 = 31$.

BEATRIX : 31 est aussi un nombre premier. La propriété reste vraie.

EURISTIDE : $p = 2 \times 3 \times 5 \times 7 + 1 = 211$.

Je te donne la réponse. 211 est bien un nombre premier.

$$p = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311. \tag{394}$$

2311 est aussi un nombre premier.

BEATRIX : Tiens, tiens. Aurions-nous créé ainsi une suite de nombres premiers ?

EURISTIDE : $p = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$.
Il se trouve, enfin, que $30031 = 59 \times 509$.
Nous avons vérifié que cette propriété n'est pas vraie en général.

BEATRIX : D'accord.

4 Acte IV - Congruences

EURISTIDE : Nous allons maintenant un domaine nous permettant d'approfondir le comportement des restes des divisions euclidiennes.

4.1 Scène IV.1 - Définition

MATHINE : C'est l'objet de la théorie des congruences. Qu'est-ce qu'une congruence ? En voici la définition :

Définition 4.1.1
Congruence
Soit $a, b \in \mathbb{Z}$. Soit $m \in \mathbb{Z} - \{0\}$.
On dit que a est congru à b modulo m, ce qu'on note $a \equiv b \pmod{m}$, si $m|(a-b)$.
Si a n'est pas congru à b modulo m, on écrit $a \not\equiv b \pmod{m}$.

EURISTIDE : Béatrix, sais-tu me donner la signification de cette définition, à l'aide de la division euclidienne ?

BEATRIX : Si m divise $(a-b)$, cela signifie qu'en écrivant :

$$a = mq + r \tag{395}$$
$$b = mq' + r', \tag{396}$$

on obtient :

$$a - b = m(q - q') + (r - r'). \tag{397}$$

Pour que m divise $(a-b)$, il faut et il suffit que $r - r' = 0$, donc que $r = r'$.
Donc, je dis que a est congru à b modulo m si a et b ont le même reste dans la division euclidienne par m.

EURISTIDE : C'est exactement cela.
Par exemple :

$$3 \equiv 1 \pmod 2 \tag{398}$$
$$4 \equiv 1 \pmod 3 \tag{399}$$
$$12 \equiv 3 \pmod 9 \tag{400}$$
$$12 \equiv 0 \pmod 3. \tag{401}$$

MATHINE : Voyons maintenant quelques propriétés de cette relation de congruence.

Proposition 4.1.1
Propriétés congruence
Soit $a, b, c \in \mathbb{Z}$ et $m \in \mathbb{N}$, $d \in \mathbb{N} - \{0\}$.

i) $a \equiv a \pmod m$. On dit que la relation de congruence est réflexive.

ii) Si $a \equiv b \pmod m$, alors $b \equiv a \pmod m$. La relation de congruence est symétrique.

iii) Si $a \equiv b \pmod m$ et si $b \equiv c \pmod m$, alors $a \equiv c \pmod m$. La relation de congruence est transitive.

iv) Si $a \equiv b \pmod m$ et $c \equiv d \pmod m$, alors :

$$ac \equiv bd \pmod m \tag{402}$$

v) Si $a \equiv b \pmod m$ et $c \equiv d \pmod m$, alors :

$$\forall x, y \in \mathbb{Z}, ax + cy \equiv bx + dy \pmod m. \tag{403}$$

Autrement dit, la relation de congruence est stable par combinaison linéaire.

vi) Si $a \equiv b \pmod m$ et $d|m$, alors $a \equiv b \pmod d$.

vii) Si $a \equiv b \pmod m$, toutes expressions de a et b identiques faisant intervenir des sommes de puissances de a et de b entières et des coefficients multiplicateurs entiers sont congrues modulo m :

$$\sum_{k=0}^{n} q_k a^k \equiv \sum_{k=0}^{n} q_k b^k \pmod m. \tag{404}$$

EURISTIDE : La propriété i) est évidente, puisque a possède le même reste que lui-même. La propriété ii) est aussi évidente, puisque la relation "avoir le même reste que" est bien sûr symétrique. Il en va de même de la transitivité.
Les propriétés iv), v), vi) et vii) découlent rapidement de l'expression de la division euclidienne.

MATHINE : Voici donc la démonstration de ces propriétés.

Démonstration :

i) Réflexivité : c'est évident, puisque $a - a = 0$ est divisible par m.

ii) Symétrique : c'est évident, puisque si $a-b$ est divisible par m, alors $b-a$ est également divisible par m.

iii) Transitivité : c'est encore évident, puisque si $a-b$ est divisible par m et $b-c$ est divisible par m, alors $a-c=(a-b)+(b-c)$ est également divisible par m.

iv) Par hypothèse, nous avons :

$$a-b=km, \tag{405}$$

et :

$$c-d=k'm. \tag{406}$$

Donc :

$$a=km+b, \tag{407}$$

et :

$$c=k'm+d. \tag{408}$$

Donc :

$$ac=kk'm^2+kdm+bk'm+bd. \tag{409}$$

Donc :

$$ac-bd=m(kk'm+kd+bk'), \tag{410}$$

c'est-à-dire :

$$ac-bd|m. \tag{411}$$

Et, par conséquent :

$$ac\equiv bd \pmod{m}. \tag{412}$$

v) Par hypothèse, nous avons :

$$m|a-b, \tag{413}$$

et :

$$m|c-d. \tag{414}$$

Donc :

$$m|((a-b)x+(c-d)y), \tag{415}$$

ce qui s'écrit :

$$m|((ax+cy)-(bx+dy)). \tag{416}$$

Donc :

$$ax+cy\equiv bx+dy \pmod{m}. \tag{417}$$

vi) C'est évident, puisque si $a-b|m$, alors il existe $k\in\mathbb{Z}$ tel que :

$$a-b=km, \tag{418}$$

et puisque $d|m$, il existe k' tel que $m=k'd$.
Donc :

$$a-b=kk'd. \tag{419}$$

D'où :

$$a\equiv b \pmod{m}. \tag{420}$$

vii) Nous allons procéder par récurrence pour démontrer que si :

$$a\equiv b \pmod{m}, \tag{421}$$

alors, pour tout $k\in\mathbb{N}$:

$$a^k\equiv b^k \pmod{m}. \tag{422}$$

1) La propriété est vraie pour $k = 1$, évidemment.
2) Supposons la propriété vraie pour k.
   Alors, nous avons :
$$a^k \equiv b^k \pmod{m}. \tag{423}$$
   En appliquant la propriété iv), on trouve que :
$$a^k.a \equiv b^k.b \pmod{m}. \tag{424}$$
   Donc :
$$a^{k+1} \equiv b^{k+1} \pmod{m}. \tag{425}$$
   Donc, la propriété est vraie pour tout k.
   On en déduit, d'après la propriété iv), que pour tout k :
$$q_k a^k \equiv q_k b^k \pmod{m}, \tag{426}$$
   et, par conséquent, leurs sommes le sont aussi, d'après la propriété v) :
$$\sum_{k=1}^{n} q_k a^k \equiv \sum_{k=1}^{n} q_k b^k \pmod{m}. \tag{427}$$

C.Q.F.D.

EURISTIDE : Il faut noter qu'une relation, comme cette relation de congruence, qui est à la fois réflexive, symétrique et transitivie, est appelée relation d'équivalence . Elle permet de constituer justement une équivalence entre tous les entiers ayant même reste dans la division euclidienne par m.
Cette équivalence permet de regrouper les entiers en classes : la classe des entiers ayant 0 pour reste dans la division par m, ceux de reste 1, etc.
Ces classes, au nombre de m, sont appelées classes résiduelles modulo m.

BEATRIX : Dans une égalité de type :
$$ax = ay, \tag{428}$$
on peut simplifier par a si $a \neq 0$ et déduire que $x = y$. Comment cela se passe-t-il pour une congruence modulo m ?

MATHINE : C'est un peu plus sophistiqué pour une congruence. C'est ce que nous allons voir dans la proposition suivante :

Proposition 4.1.2
Simplification congruences
Soit $x, y \in \mathbb{Z}$. Soit $m \in \mathbb{N}$.

i) $ax \equiv ay \pmod{m}$ si et seulement si $x \equiv y \pmod{\frac{m}{(a,m)}}$

ii) Si $ax \equiv ay \pmod{m}$ et $(a, m) = 1$, alors $x \equiv y \pmod{m}$.

iii) Pour tout $i \in [1, r]$, $x \equiv y \pmod{m_i}$ si et seulement si :
$$x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}. \tag{429}$$

EURISTIDE : On voit bien que la simplication d'une congruence n'est pas immédiate. Il faut retenir que la simplification est possible chaque fois que le coefficient à simplifier est premier avec l'entier m du modulo de la congruence ; si ce n'est pas le cas, on retrouve la congruence simplifiée en divisant l'entier m par le pgcd du coefficient et de m.
Dans un même esprit, on voit que si deux entiers sont congrus pour différents modulo, il l'est pour leur ppcm.

BEATRIX : La première et la deuxième propriété sont très intuitives. $ax \equiv ay \pmod{m}$ signifie que $ax - ay$ divise m. Ce n'est simplifiable qu'à la condition d'être certain que a ne possède pas de diviseur en commun avec m, donc que $(a, m) = 1$. Si ce n'est pas le cas, on peut diviser les deux entiers $(ax - ay)$ et m par (a, m) pour identifier la congruence modulo $\frac{m}{(a,m)}$.
La troisième propriété se comprend également aisément. Puisque les m_i divisent $x - y$, $x - y$ est multiple commun aux m_i, donc leur ppcm divise $x - y$.

MATHINE : Voici la démonstration formelle :

Démonstration :

i) Procédons en deux étapes, puisqu'il s'agit de démontrer une équivalence :
   a) Supposons que $ax \equiv ay \pmod{m}$.
   Alors :
   $$m|a(x - y). \tag{430}$$
   Donc, il existe un entier q tel que :
   $$a(x - y) = mq. \tag{431}$$
   En divisant par (a, m), on obtient :
   $$\frac{a}{(a, m)}(x - y) = \frac{m}{(a, m)}q. \tag{432}$$
   Donc :
   $$\frac{m}{(a, m)} \left| \frac{a}{(a, m)}(x - y) \right. \tag{433}$$
   Or, nous savons que $\frac{m}{(a,m)}$ est premier avec $\frac{a}{(a,m)}$, donc :
   $$\frac{m}{(a, m)} |(x - y) \tag{434}$$
   Donc :
   $$x \equiv y \pmod{\frac{m}{(a, m)}}. \tag{435}$$
   b) Supposons que :
   $$x \equiv y \pmod{\frac{m}{(a, m)}}. \tag{436}$$
   Alors :
   $$\frac{m}{(a, m)} |(x - y) \tag{437}$$

Donc :

$$m|(a,m)(x-y), \tag{438}$$

et, a fortiori :

$$m|a(x-y). \tag{439}$$

D'où :

$$ax \equiv ay \pmod{m}. \tag{440}$$

ii) Si a et m sont premiers entre eux, alors le résultat de la propriété i) nous indique que :

$$x \equiv y \pmod{\frac{m}{1}}, \tag{441}$$

soit :

$$x \equiv y \pmod{m}. \tag{442}$$

iii) Pour tout $i \in [1,r]$, nous avons :

$$m_i|(x-y). \tag{443}$$

Donc, $x-y$ est un multiple commun des m_i pour $i \in [1,r]$.
Il s'ensuit que $x-y$ est un multiple du ppcm des m_i.
Donc :

$$[m_1,m_2,\ldots,m_r]|(x-y). \tag{444}$$

D'où :

$$x \equiv y \mod [m_1,m_2,\ldots,m_r]. \tag{445}$$

C.Q.F.D.

EURISTIDE : Nous allons maintenant introduire un peu de vocabulaire et quelques propriété supplémentaires sur les congruences.

MATHINE : Commençons par définir ce qu'est un résidu.

Définition 4.1.2
Résidu
Soit x un entier. Soit $m \in \mathbb{N}$. On appelle résidu de x modulo m un entier y tel que :

$$x \equiv y \pmod{m}. \tag{446}$$

BEATRIX : Donc un résidu est un entier congru à un autre, modulo un entier donné. Jusque là, c'est simple.
Par exemple, 1 est un résidu modulo 2 de 3. C'est le cas également de 3 et de 5. Le résidu, c'est donc un peu équivalent au reste de la division euclidienne par m, auquel on peut ajouter ou retrancher un multiple arbitraire de m.

MATHINE : Poursuivons en définissant la notion de système de résidus.

Définition **4.1.3**
Système complet de résidus
Soit $m \in \mathbb{N}$. On appelle système complet de résidus modulo m, un ensemble d'entiers $\{x_1, x_2, \ldots, x_m\}$ tels que pour tout entier $y \in \mathbb{Z}$, il existe un et un seul x_i tel que :

$$y \equiv x_i \pmod{m}. \tag{447}$$

EURISTIDE : Nous savons que la relation de congruence comporte m classes résiduelles modulo m, correspondant aux m restes possibles de la division d'entiers par m. Donc, un système complet de résidus est en fait un système de nombres contenant un et un seul représentant de chaque classe de congruence.

BEATRIX : D'accord, j'ai compris. Si l'on regarde la congruence modulo 6, nous avons évidemment un système complet de résidus modulo 6 en écrivant :

$$\{0, 1, 2, 3, 4, 5\}. \tag{448}$$

EURISTIDE : C'est exact. Mais l'ensemble suivant est aussi un système complet de résidus modulo 6 :

$$\{6, 13, 2, -3, 22, 11\}. \tag{449}$$

On peut le vérifier en constatant que :

$$\begin{aligned}
6 &\equiv 0 \pmod{6} && (450)\\
13 &\equiv 1 \pmod{6} && (451)\\
2 &\equiv 2 \pmod{6} && (452)\\
-3 &\equiv 3 \pmod{6} && (453)\\
22 &\equiv 4 \pmod{6} && (454)\\
11 &\equiv 5 \pmod{6}. && (455)
\end{aligned}$$

MATHINE : C'est bien cela. Voyons maintenant ce qu'est un système réduit de résidus.

Définition **4.1.4**
Système réduit de résidus
Soit $m \in \mathbb{N}$.
On appelle système réduit de résidus modulo m un ensemble d'entiers $\{r_1, r_2, \ldots, r_l\}$ tels que pour tout $i \in [1, l]$, r_i est premier avec m, tels que $r_i \not\equiv r_j \pmod{m}$ pour $i \neq j$, et tels que pour tout y entier premier avec m, il existe un et un seul r_i tel que :

$$y \equiv r_i \pmod{m}. \tag{456}$$

EURISTIDE : Cette définition consiste à sélectionner dans les systèmes complets de résidus modulo

m, ceux qui sont premiers avec m et n'appartenant pas à la même classe de congruence.
Ainsi, si nous reprenons la congruence modulo 6, un exemple en partant du deuxième système complet de résidus vu précédemment, de système réduit de résidus modulo 6 serait :

$$\{13, 11\}, \tag{457}$$

car 6, 2, -3, 22 ne sont pas premiers avec 6.

BEATRIX : Oui. Et si on reprend mon exemple, je trouve le système réduit de résidus modulo 6 suivant :

$$\{1, 5\}. \tag{458}$$

Si l'on prenait la congruence modulo 11, on aurait le système réduit suivant :

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}. \tag{459}$$

EURISTIDE : D'ailleurs, si m est premier, on peut dire que le système réduit de résidus modulo m comporte $(m-1)$ entiers.

BEATRIX : Donc, pour connaître le cardinal d'un système réduit de résidus modulo m, il nous faut connaître le nombre d'entiers qui sont premiers avec m.

MATHINE : Oui, et Euler a défini une fonction pour donner cette quantité. C'est la fonction d'Euler.

Définition **4.1.5**
Fonction d'Euler
On appelle fonction d'Euler , la fonction définie de $\mathbb{N}$ dans $\mathbb{N}$:

$$m \longmapsto \phi(m) = Card(\{n \leq m; (n, m) = 1\}). \tag{460}$$

BEATRIX : Donc, on a vu que :

$$\phi(6) = 2 \tag{461}$$
$$\phi(11) = 10. \tag{462}$$

EURISTIDE : Pour un nombre premier p, on a plus généralement :

$$\phi(p) = p - 1. \tag{463}$$

4.2 Scène IV.2 - Petit théorème de Fermat

MATHINE : Nous allons maintenant voir une propriété assez surprenante mise en évidence par Euler.

Théorème **4.2.1 (d'Euler)** *Soit $a \in \mathbb{Z}$; soit $m \in \mathbb{N}$.*
Si $(a, m) = 1$, alors :

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{464}$$

BEATRIX : Oui, en effet, c'est surprenant ! On se demande d'où tombe cette relation. Je vais prendre un exemple pour voir :
2 et 7 sont premiers entre eux.
$\phi(7) = 6$.

$$2^6 = 64, \tag{465}$$

et $64 = 9 \times 7 + 1$.
Donc :

$$2^6 \equiv 1 \pmod{7}. \tag{466}$$

Mais comment donc cela s'explique-t-il ?

EURISTIDE : C'est assez subtil, mais cela s'explique plutôt bien. Si l'on considère les classes de congruence modulo m des puissances a^k, il est bien évident qu'il y aura au plus m valeurs de classes.
Mais comme a est premier avec m, la classe nulle est exclue. Il reste donc $m - 1$ classes possibles.
Mais de plus, toujours parce que a est premier avec m, les classes qui ne sont pas premières avec m sont également exclues ; en effet, si on les gardait, le reste aurait un diviseur commun avec le quotient m, donc le dividence aussi, ce qui contredirait que a est premier avec m.
Donc, il ne reste que les classes de restes qui sont premières avec m, ce qui fait un nombre de $\phi(m)$ classes.
Ceci étant dit, il s'ensuit par une symétrie assez intuitive, que les a^k successifs lorsqu'on augmente k auront des restes déterminés suivant une loi cyclique, en l'occurrence dont le cycle sera $\phi(m)$, c'est-à-dire que a^k et $a^{k+\phi(m)}$ auront même reste dans la division par m, une fois que l'on aura épuisé toutes les valeurs possibles de restes distincts dans la division par m.
Or $a^0 = 1$ possède 1 pour reste dans la division par m, donc $a^{\phi(m)}$ aura également pour reste la valeur 1, à cause de ce caractère cyclique expliqué précédemment. C'est ce qui conduit à la propriété d'Euler.

MATHINE : Bien évidemment, cette explication ne constitue pas une démonstration, mais fournit plutôt la raison d'être de cette relation peu intuitive au premier abord.

Démonstration :

Nous allons utiliser les systèmes réduits de résidus modulo m pour cette démonstration.
Soit un système réduit de résidus modulo m :

$$\{r_1, r_2, \ldots, r_{\phi(m)}\}. \tag{467}$$

On a, pour tout $i \in [1, \phi(m)]$:

$$(r_i, m) = 1, \tag{468}$$

et par ailleurs :

$$(a, m) = 1. \tag{469}$$

Donc :

$$(ar_i, m) = 1. \tag{470}$$

Supposons qu'il existe $i, j \in [1, \phi(m)]$ tels que :

$$ar_i \equiv ar_j \pmod{m}. \tag{471}$$

Alors, d'après la proposition sur la simplification des congruences (cf. 4.1.2), nous en déduisons que :

$$r_i \equiv r_j \pmod{m}, \tag{472}$$

ce qui contredit le fait que $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ est un système réduit de résidus modulo m.
Donc, $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ est un système réduit de résidus modulo m.
Donc, on peut donc écrire, pour tout $i \in [1, \phi(m)]$, après un rangement adéquat des résidus des deux systèmes :

$$ar_i \equiv r_i \pmod{m}. \tag{473}$$

Par conséquent, d'après la proposition (cf. 4.1.1) :

$$\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}. \tag{474}$$

Ce qui s'écrit encore :

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}. \tag{475}$$

Or, tous les r_i sont premiers avec m, donc leur produit également. Donc on peut appliquer la proposition de simplification de congruence (cf. 4.1.2), et simplifier la congruence ci-dessus par ce produit pour obtenir :

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{476}$$

C.Q.F.D.

BEATRIX : La démonstration est moins intuitve que l'explication. Mais elle est effectivement plus rigoureuse.

MATHINE : Nous allons pouvoir énoncer maintenant le Petit Théorème de Fermat qui est un cas particulier du Théorème d'Euler que nous venons de voir, lorsque m est premier.

Théorème **4.2.2 (Petit Théorème de Fermat)** *Soit p un nombre premier.*
Soit a un entier positif tel que $p \nmid a$.
Alors :

$$a^{p-1} \equiv 1 \pmod{p}. \tag{477}$$

De plus :

$$a^p \equiv a \pmod{p}. \tag{478}$$

Démonstration :

Tout élément a tel que $p \nmid a$ et p premier est premier avec p.
Donc, nous pouvons appliquer le Théorème d'Euler (cf. 4.2.1), et puisque $\phi(p) = p - 1$, nous obtenons :

$$a^{p-1} \equiv 1 \pmod{p}. \tag{479}$$

De plus, en appliquant la proposition (cf. 4.1.1), nous obtenons directement :

$$a^{p} \equiv a \pmod{p}. \tag{480}$$

C.Q.F.D.

4.3 Scène IV.3 - Equation de congruence

EURISTIDE : Nous connaissons les équations du premier degré :

$$ax + b = 0. \tag{481}$$

La question que nous allons nous poser maintenant est de savoir quelles sont les solutions d'une équation de congruence du premier degré.

MATHINE : Oui, nous allons pouvoir étudier les équations du type :

$$ax \equiv b \pmod{m}, \tag{482}$$

grâce au théorème d'Euler (cf. 4.2.1) que nous avons vu précédemment.

Théorème 4.3.1
Equation de congruence
Soit $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}$.
Si $(a, m) = 1$, alors l'équation :

$$ax \equiv b \pmod{m}, \tag{483}$$

possède au moins une solution x_0, et toutes les autres solutions x sont données par :

$$x = x_0 + km, k \in \mathbb{Z}. \tag{484}$$

BEATRIX : Et comment trouve-t-on une solution à une telle équation. Je connais la méthode pour une équation du premier degré classique, mais ici, c'est différent.

EURISTIDE : Pour trouver une solution, il suffit de se ramener au théorème d'Euler, ou presque.
Le théorème d'Euler nous dit que :

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{485}$$

Donc :

$$a^{\phi(m)}b \equiv b \pmod{m}, \tag{486}$$

ce qui s'écrit également :

$$a\left(a^{\phi(m)-1}b\right) \equiv b \pmod{m}. \tag{487}$$

Et nous tenons une solution. Les autres solutions proviennent des propriétés de la congruence.

MATHINE : Voici la démonstration complète.

Démonstration :

Effectivement, en choisissant :

$$x_0 = a^{\phi(m)-1}b, \tag{488}$$

on trouve :

$$ax_0 = a^{\phi(m)}b, \tag{489}$$

donc x_0 est bien une solution de l'équation.
Si x est une autre solution, on a :

$$ax \equiv b \pmod{m}, \tag{490}$$

et :

$$ax_0 \equiv b \pmod{m}. \tag{491}$$

Donc, en appliquant la proposition (cf. 4.1.1), on en déduit que :

$$a(x - x_0) \equiv 0 \pmod{m}. \tag{492}$$

Or, a est premier avec m, donc nécessairement :

$$x - x_0 \equiv 0 \pmod{m}. \tag{493}$$

Donc $x = x_0 + km, k \in \mathbb{Z}$.

C.Q.F.D.

4.4 Scène IV.4 - Théorème de Wilson

EURISTIDE : Ce théorème va nous permettre de démontrer le Théorème de Wilson.

MATHINE : Le théorème de Wilson constitue un moyen de caractériser un nombre premier.

Théorème 4.4.1 (de Wilson) *Soit $m \in \mathbb{N}$, $m > 1$. Alors m est premier si et seulement si :*

$$(m-1)! \equiv -1 \pmod{m}. \tag{494}$$

BEATRIX : Encore une propriété assez surprenante !

EURISTIDE : Pour démontrer ce théorème, nous allons démontrer que l'on peut constituer un regroupement des nombres 2, 3, ...,$p-2$ par couples de la forme :

$$(p-i)(p-j), \tag{495}$$

tels que :

$$(p-i)(p-j) \equiv 1 \pmod{m}. \tag{496}$$

Et cela s'avère vrai, parce que si m est premier, il est évident que $p-i$ est toujours premier avec m, donc l'équation de congruence admet toujours une solution, d'après le théorème sur l'équation de congruence (cf. 4.3.1).

MATHINE : Voici donc la démonstration du théorème de Wilson.

Démonstration :

Comme il s'agit de démontrer que la condition est nécessaire et suffisante, nous allons procéder en deux étapes.

1) Supposons que m est un nombre premier.
Considérons les entiers n tels que :

$$1 \leq n \leq m-1. \tag{497}$$

Puisque m est premier, $(n, m) = 1$, pour tout n.
Donc, on peut appliquer le théorème sur l'équation de congruence, et nous savons donc que pour tout n, il existe un entier q tel que :

$$nq \equiv 1 \pmod{m}. \tag{498}$$

Pour $n = 1$, $q = 1$ convient.
Pour $n = m-1$, $q = m-1$ convient.
Pour $2 \leq n \leq m-2$, qui constitue un nombre pair d'entiers possibles lorsque $m > 2$, nous allons montrer que les nombres n et q sont associés deux à deux dans cette collection de nombres et ne sont pas associés à eux-mêmes.
Supposons le contraire :

$$(m-i)(m-i) \equiv 1 \pmod{m}, \tag{499}$$

aurait pour conséquence :

$$(m-i)^2 - 1 \equiv 0 \pmod{m}, \tag{500}$$

c'est-à-dire :

$$(m-i-1)(m-i+1) \equiv 0 \pmod{m}, \tag{501}$$

Or, $m-i-1$ et $m-i+1$ sont tous deux premiers avec m, donc ceci est contradictoire.
Donc, nous venons de démontrer que tous les $(m-i)$ pour $2 \leq i \leq m-2$ peuvent être rangés deux par deux et chaque couple $(m-i)$ et $(m-j)$ vérifie :

$$(m-i)(m-j) \equiv 1 \pmod{m}. \tag{502}$$

Par conséquent, nous pouvons écrire, en multipliant entre elles ces relations de congruence :

$$2 \times 3 \times \ldots \times (m-3) \times (m-2) \equiv 1 \pmod{m}. \tag{503}$$

Par conséquent :

$$2 \times 3 \times \ldots \times (m-3) \times (m-2) \times (m-1) \equiv m-1 \pmod{m}. \tag{504}$$

Or :

$$m-1 \equiv -1 \pmod{m}. \tag{505}$$

Donc, finalement :

$$(m-1)! \equiv -1 \pmod{m}. \tag{506}$$

Nous avons dû écarter le cas $m = 2$ dans notre démonstration.
Mais nous voyons que :

$$1! \equiv -1 \pmod{2}. \tag{507}$$

Donc, la propriété est également vérifiée pour $m = 2$.
Par conséquent, elle l'est pour tout nombre premier.

2) En logique formelle, les deux propositions suivantes sont équivalentes :

$$P \Rightarrow Q \Leftrightarrow \neg Q \Rightarrow \neg P. \tag{508}$$

Cela signifie qu'au lieu de démontrer qu'une propriété P entraîne une propriété Q, nous pouvons tout aussi bien démontrer que le contraire de la propriété Q (on l'appelle contraposée) entraîne le contraire de la propriété P.

`BEATRIX` : Je comprends. Donc au lieu de démontrer que si $(m-1)! \equiv -1 \pmod{m}$ alors m est premier, nous allons supposer que m n'est pas premier, et démontrer que cette congruence n'est pas vérifiée.

`MATHINE` : Exactement.

Supposons donc que m n'est pas premier.
Alors, il existe des entiers q et r tels que :

$$m = qr, \tag{509}$$

où l'on peut faire l'hypothèse, sans nuire à la généralité, que $1 < q < m$.
Par conséquent, q est forcément l'un des entiers de 2 à $m-1$.
Donc :

$$q | (m-1)! \tag{510}$$

Donc :

$$q \nmid ((m-1)! + 1). \tag{511}$$

Et par conséquent, un même raisonnement s'applique à r et :

$$qr \nmid ((m-1)! + 1). \tag{512}$$

Donc :

$$(m-1)! \not\equiv -1 \pmod{m}. \tag{513}$$

C.Q.F.D.

4.5 Scène IV.5 - Théorème chinois

EURISTIDE : Concernant les congruences, il nous reste à voir un théorème, appelé le Théorème Chinois.

BEATRIX : Joli nom, ma foi. En quoi consiste-t-il ?

EURISTIDE : Ce théorème est dans la continuité du théorème concernant l'équation de congruence. Nous avons vu une équation de congruence. Le Théorème Chinois permet de constituer un système d'équations de congruences déterminant un ensemble de solutions congrues entre elles, étant le reste commun à un ensemble de nombres modulo des entiers premiers entre eux deux à deux.

MATHINE : Voici ce théorème.

Théorème 4.5.1 (Théorème Chinois) *Soit $m_1, m_2, \dots, m_r$ des entiers naturels relativement premiers deux à deux. Soit $a_1, a_2, \dots, a_r$ des entiers quelconques de $\mathbb{Z}$.*
Alors, le système de congruences :

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} && (514)\\ x &\equiv a_2 \pmod{m_2} && (515)\\ &\dots && (516)\\ x &\equiv a_r \pmod{m_r}, && (517)\end{aligned}$$

possède une solution telle qu'il existe des entiers $b_j \in \mathbb{Z}$ tels que :

$$\prod_{i=1 i\neq j}^{r} m_i.b_j \equiv 1 \pmod{m_j}, \tag{518}$$

et :

$$x_0 = \sum_{j=1}^{r} \prod_{i=1 i\neq j}^{r} m_i.b_j a_j. \tag{519}$$

Les autres solutions sont congrues à x_0 modulo $\prod_{i=1}^{r} m_i$.

Démonstration :

Notons $m = m_1 m_2 \dots m_r$.
Puisque les m_i sont premiers entre eux deux à deux, nous avons :

$$\left(m_i, \frac{m}{m_i}\right) = 1, \tag{520}$$

pour tout i.
Donc nous pouvons appliquer le théorème de l'équation de congruence (cf. 4.3.1) et il existe donc, pour tout $j \in [1, r]$, un entier b_j tel que :

$$\frac{m}{m_j}.b_j \equiv 1 \pmod{m_j}. \tag{521}$$

Montrons que l'entier :

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \tag{522}$$

est bien une solution.
Fixons i.
Pour $j \neq i$, nous savons que :

$$\frac{m}{m_j}.b_j \equiv 0 \pmod{m_i}. \tag{523}$$

puisque $m_i | \frac{m}{m_j}$ lorsque $j \neq i$.
Donc, pour $j \neq i$:

$$\frac{m}{m_j} b_j a_j \equiv 0 \pmod{m_i}. \tag{524}$$

Par conséquent :

$$\sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \equiv \frac{m}{m_i} b_i a_i \pmod{m_i}. \tag{525}$$

Or, par définition des b_i,

$$\frac{m}{m_i} b_i \equiv 1 \pmod{m_i}. \tag{526}$$

Donc :

$$\sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \equiv a_i \pmod{m_i}. \tag{527}$$

Donc :

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \tag{528}$$

est une solution.

Montrons maintenant que toutes les autres solutions sont congrues modulo $\prod_{i=1}^{r} m_i$.
Soit x une autre solution. Alors, pour tout j :

$$x_0 \equiv a_j \pmod{m_j} \tag{529}$$
$$x \equiv a_j \pmod{m_j}. \tag{530}$$

Donc :

$$x_0 \equiv x \pmod{m_j}, \tag{531}$$

d'après la transitivité de la congruence (cf. 4.1.1).
Et d'après les propriétés de simplification des congruences (cf. 4.1.2), on en déduit que :

$$x_0 \equiv x \pmod{\prod_{j=1}^{r} m_j}. \tag{532}$$

C.Q.F.D.

EURISTIDE : Prenons un exemple, et cherchons les solutions de :

$$x \equiv 2 \pmod 4 \tag{533}$$
$$x \equiv 5 \pmod 7 \tag{534}$$
$$x \equiv 3 \pmod 9. \tag{535}$$

Nous sommes bien dans le cas du Théorème Chinois, puisque 4, 7 et 9 sont deux à deux premiers entre eux.
Notons $m = 4 \times 7 \times 9 = 252$.
Considérons les congruences :

$$\frac{252}{4} \times b_1 \equiv 1 \pmod 4 \tag{536}$$
$$\frac{252}{7} \times b_2 \equiv 1 \pmod 7 \tag{537}$$
$$\frac{252}{9} \times b_3 \equiv 1 \pmod 9, \tag{538}$$

c'est-à-dire :

$$63 \times b_1 \equiv 1 \pmod 4 \tag{539}$$
$$36 \times b_2 \equiv 1 \pmod 7 \tag{540}$$
$$28 \times b_3 \equiv 1 \pmod 9. \tag{541}$$

Pour l'équation :

$$63 \times b_1 \equiv 1 \pmod 4, \tag{542}$$

on sait d'après le théorème sur les équations de congruences (cf. 4.3.1), qu'une solution est donnée par :

$$b_1 = 63^{\phi(4)-1} \times 1. \tag{543}$$

Or $\phi(4) = 2$, donc $b_1 = 63$.
Or $63 \equiv 3 \pmod 4$, donc on peut choisir $b_1 = 3$.
Pour l'équation :

$$36 \times b_2 \equiv 1 \pmod 7, \tag{544}$$

puisque $7 \times 5 = 35$, on voit que $36 \equiv 1 \pmod 7$, donc $b_2 = 1$ convient.
Pour l'équation :

$$28 \times b_3 \equiv 1 \pmod 9, \tag{545}$$

on voit que $28 \times 1 \equiv 1 \pmod 9$, donc $b_3 = 1$ convient.
Par conséquent, la solution du système est :

$$x_0 = \frac{252}{4} \times 3 \times 2 + \frac{252}{7} \times 1 \times 5 + \frac{252}{9} \times 1 \times 3 \tag{546}$$
$$= 378 + 180 + 84, \tag{547}$$

soit :

$$x_0 = 642. \tag{548}$$

BEATRIX : Et ça marche :

$$642 = 160 \times 4 + 2 \tag{549}$$
$$642 = 91 \times 7 + 5 \tag{550}$$
$$642 = 71 \times 9 + 3. \tag{551}$$

Donc, nous avons bien :

$$642 \equiv 2 \pmod 4 \quad (552)$$
$$642 \equiv 5 \pmod 7 \quad (553)$$
$$642 \equiv 3 \pmod 9. \quad (554)$$

Les autres solutions sont les :

$$642 + 252.k. \quad (555)$$

Donc, en prenant $k = -2$, on peut trouver la plus petite solution positive :

$$x_0 = 138. \quad (556)$$

$$138 = 34 \times 4 + 2 \quad (557)$$
$$138 = 19 \times 7 + 5 \quad (558)$$
$$138 = 15 \times 9 + 3. \quad (559)$$

Donc, nous avons bien :

$$138 \equiv 2 \pmod 4 \quad (560)$$
$$138 \equiv 5 \pmod 7 \quad (561)$$
$$138 \equiv 3 \pmod 9. \quad (562)$$

5 Acte V - Analyse diophantienne

EURISTIDE : C'est vrai, la méthode de la démonstration ne donne pas nécessairement la valeur de la solution qui soit la plus petite. Mais cette dernière reste facile à déduire.
Nous allons maintenant aborder un nouveau chapitre palpitant de la théorie des nombres. Il s'agit des équations diophantiennes.

BEATRIX : Pourquoi portent-elles ce nom ?

EURISTIDE : Leur nom vient de Diophante qui était un mathématicien du IIIème siècle, et qui a étudié le premier les équations en nombres entiers à coefficients entiers. Puis ces équations ont été étudiées intensivement par de nombreux mathématiciens au long de plusieurs siècles : Fermat, Euler, Lagrange, Waring, Hilbert, etc.

5.1 Scène V.1 - Equation du premier degré

MATHINE : Nous allons commencer par l'équation diophantienne $ax + by = c$ dite du premier degré.

Théorème **5.1.1**
Equation diophantienne du premier degré

Soit $a, b, c \in \mathbb{Z}$. Soit $d = (a, b)$.
Alors, l'équation diophantienne :

$$ax + by = c, \tag{563}$$

possède des solutions entières, si et seulement si $d|c$, auquel cas les solutions sont données par :

$$x = x_0 + \frac{bt}{d} \tag{564}$$

$$y = y_0 - \frac{at}{d}, \tag{565}$$

où t est un entier arbitraire, et x_0 et y_0 sont des solutions particulières de l'équation diophantienne.

EURISTIDE : Autrement dit, dès lors que nous avons trouvé une solution, les autres solutions sont déduites par congruence modulo $\frac{b}{d}$ pour x et par congruence modulo $-\frac{a}{d}$ pour y.

MATHINE : La démonstration se fait en se ramenant à une équation de congruence, que nous savons déjà résoudre.

Démonstration :

L'équation étant triviale pour $ab = 0$, c'est-à-dire pour $a = 0$ ou $b = 0$, nous allons supposer que $ab \neq 0$.
Soit $d = (a, b)$.

1) Nous allons d'abord supposer que $d = 1$, c'est-à-dire que a et b sont premiers entre eux.
Puisque l'équation $ax + by = c$ signifie que ax est congru à c modulo b, considérons l'équation de congruence :

$$ax \equiv c \pmod{|b|}. \tag{566}$$

Comme $(a, |b|) = 1$, nous savons, d'après le théorème sur les équations de congruence (cf. 4.3.1), qu'une telle équation a toujours une solution x_0 au moins, et que toutes ses solutions s'écrivent :

$$x = x_0 + |b|t, \tag{567}$$

que nous pouvons écrire plus simplement, parce que t parcourt $\mathbb{Z}$:

$$x = x_0 + bt. \tag{568}$$

Transcrivons ce résultat dans l'équation diophantienne :

$$ax_0 + abt + by = c, \tag{569}$$

ce qui s'écrit, en isolant y :

$$y = \frac{c - ax_0}{b} - at. \tag{570}$$

Choisissons simplement pour y_0 la valeur en $t = 0$:

$$y_0 = \frac{c - ax_0}{b}. \tag{571}$$

Donc, les solutions de l'équation diophantienne sont :

$$x = x_0 + bt \tag{572}$$
$$y = y_0 - at, \tag{573}$$

où $t \in \mathbb{Z}$ et x_0, y_0 sont des solutions particulières.

2) Etudions maintenant le cas général où $d = (a, b)$ est différent de 1.
Il est nécessaire que $d|c$, car sinon l'équation ne peut pas avoir de solution. En effet, puisque $d = (a, b)$, il existe k tel que $a = kd$ et k' tel que $b = k'd$. Donc :

$$ax + by = d(kx + k'y). \tag{574}$$

Donc :

$$d(kx + k'y) = c. \tag{575}$$

Ce qui impose que $d|c$.
Nous pouvons alors écrire l'équation sous la forme :

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}. \tag{576}$$

Or :

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1, \tag{577}$$

donc nous sommes ramenés au cas 1).
Donc, en appliquant le résultat du 1), nous en déduisons les solutions de l'équation diophantienne dans le cas général :

$$x = x_0 + \frac{bt}{d} \tag{578}$$
$$y = y_0 - \frac{at}{d}. \tag{579}$$

C.Q.F.D.

EURISTIDE : Alors Béatrix, à toi de travailler maintenant. Peux-tu me donner toutes les solutions de l'équation :

$$2x + 3y = 31. \tag{580}$$

BEATRIX : Je commence par écrire l'équation de congruence correspondante, comme dans la démonstration :

$$2x \equiv 31 \pmod 3. \tag{581}$$

Or, $31 \equiv 1 \pmod 3$, donc l'équation de congruence s'écrit :

$$2x \equiv 1 \pmod 3. \tag{582}$$

Donc, on peut prendre :

$$x_0 = 2. \tag{583}$$

Alors, nous avons vu pendant la démonstration que nous pouvions choisir :

$$y_0 = \frac{31 - 2x_0}{3}, \tag{584}$$

soit :

$$y_0 = \frac{27}{3} = 9. \tag{585}$$

Ainsi les solutions sont :

$$2 + \frac{3t}{1} = 2 + 3t \tag{586}$$

$$9 - \frac{2t}{1} = 9 - 2t. \tag{587}$$

EURISTIDE : C'est bien, Béatrix. C'est la bonne méthode. Cependant, tu as oublié une chose : vérifier que le pgcd de 2 et 3 (a et b en l'occurrence) divise bien 31 (c en l'occurrence).
Prenons un autre exemple :

$$9x + 6y = 8. \tag{588}$$

BEATRIX : Je sens qu'il y a un piège... Je vais donc commencer par vérifier que $(a, b)|c$. Le pgcd de 9 et 6 est :

$$(9, 6) = 3. \tag{589}$$

Or 3 ne divise par 8. Donc, il n'y a aucune solution à cette équation.

EURISTIDE : C'est bien, Béatrix, tu as déjoué le piège.
Nous allons pouvoir passer à plus difficile. Nous allons étudier maintenant l'équation pythagoricienne $x^2 + y^2 = z^2$.

5.2 Scène V.2 - Equation pythagoricienne

BEATRIX : Pourquoi ce nom ?

EURISTIDE : Cette équation représente la propriété décrite par Pythagore concernant tous les triangles rectangles, pour lequels le carré de l'hypothénuse est égal à la somme des carrés des deux autres côtés. Il s'agit donc de trouver les triangles rectangles dont la mesure des côtés est exprimée en nombres entiers.

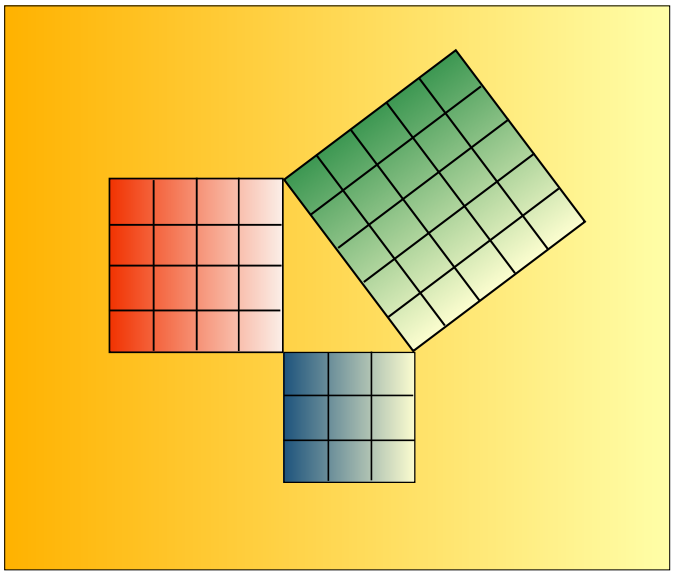

Fig. 7 - Equation pythagoricienne

BEATRIX : Donc, 3, 4, 5 est une solution.

MATHINE : Il faut maintenant une méthode pour trouver les autres solutions.

Théorème **5.2.1**
Equation pythagoricienne
Les solutions primitives (c'est-à-dire telles que $(x, y, z) = 1$*), de* $x^2 + y^2 = z^2$*, avec* y *pair, sont :*

$$x = r^2 - s^2 \tag{590}$$
$$y = 2rs \tag{591}$$
$$z = r^2 + s^2, \tag{592}$$

où r *et* s *sont des entiers arbitraires de parités opposées et satisfaisant à* $r > s > 0$ *et* $(r, s) = 1$.

EURISTIDE : La démonstration va comporter un assez grand nombre d'étapes. D'abord, nous montrerons que x, y et z sont premiers entre eux deux à deux.
Puis, nous démontrerons que z est impair et x et y sont de parité opposée.
Puis, sur hypothèse que y est impair, nous montrerons que $(z - x, z + x) = 2$.
Ensuite, nous démontrerons que l'on peut écrire :

$$\left(\frac{y}{2}\right)^2 = uv, \tag{593}$$

où u et v sont premiers entre eux.
Et nous en déduirons qu'on peut écrire :

$$u = r^2 \tag{594}$$
$$v = s^2. \tag{595}$$

D'où le résultat.
Puis nous montrerons la réciproque, c'est-à-dire que les x, y, z de la forme indiquée sont bien solutions de l'équation.

`MATHINE` : Voici donc cette longue démonstration :

Démonstration :

1) Montrons que x, y, z sont premiers entre eux deux à deux.
   Ecrivons :
   $$(x, y) = d. \tag{596}$$
   Or $z^2 = x^2 + y^2$.
   Donc $d^2|z^2$.
   Donc $d|z$.
   Donc $d|(x, y, z)$.
   Or x, y, z est une solution primitive de l'équation pythagoricienne, donc $(x, y, z) = 1$, d'où $d = 1$.
   On procède de même pour (x, z) et (y, z).
2) Montrons que z est impair.
   Supposons que z est pair, alors son carré est divisible par 4, donc :
   $$z^2 \equiv 0 \pmod 4. \tag{597}$$
   Comme :
   $$x^2 + y^2 = z^2, \tag{598}$$
   il s'ensuit que x et y doivent être impairs tous deux. Mais ceci entraîne :
   $$x^2 + y^2 \equiv 2 \pmod 4, \tag{599}$$
   ce qui est contradictoire.
   Donc z est impair.
   Par conséquent, x est pair et y impair, ou y est pair et x est impair.
   Sans nuire à la généralité, on fait ici l'hypothèse pour la suite que y est pair et x impair.
3) Montrons que $(z - x, z + x) = 2$.
   Soit $d = (z - x, z + x)$.
   Alors $d|2x$ par combinaison linéaire.
   Et $d|2z$ par combinaison linéaire.
   Donc $d|2(x, z)$.
   Or :
   $$(x, z) = 1, \tag{600}$$
   donc, nécessairement $d|2$.
   Or x et z sont tous deux impairs, donc :
   $$2 \mid z + x \tag{601}$$
   $$2 \mid z - x. \tag{602}$$

Donc $2|d$, et finalement $d = 2$.

4) Par conséquent, il existe deux entiers u et v tels que :

$$z + x = 2u \tag{603}$$
$$z - x = 2v. \tag{604}$$

Et comme $(z + x, z - x) = 2$, il s'ensuit que u et v sont premiers entre eux, donc :

$$(u, v) = 1. \tag{605}$$

Or :

$$x^2 + y^2 = z^2, \tag{606}$$

donc :

$$z^2 - x^2 = y^2, \tag{607}$$

et donc :

$$(z + x)(z - x) = y^2. \tag{608}$$

Donc, on peut écrire finalement, en introduisant u et v dans cette dernière égalité :

$$\left(\frac{y}{2}\right)^2 = uv. \tag{609}$$

Comme u et v sont premiers entre eux, on peut écrire leurs décompositions en facteurs premiers comme suit, en adoptant une indexation adéquate :

$$u = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_r^{\alpha_r} \tag{610}$$
$$v = q_{r+1}^{\alpha_{r+1}} q_{r+2}^{\alpha_{r+1}} \dots q_{r+s}^{\alpha_{r+s}}. \tag{611}$$

Par conséquent :

$$uv = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_r^{\alpha_r} q_{r+1}^{\alpha_{r+1}} q_{r+2}^{\alpha_{r+2}} \dots q_{r+s}^{\alpha_{r+s}}. \tag{612}$$

Par ailleurs, si on écrit la décomposition de $\frac{y}{2}$:

$$\frac{y}{2} = p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}, \tag{613}$$

on a :

$$p_1^{2\beta_1} p_2^{2\beta_2} \dots p_t^{2\beta_t} = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_{r+s}^{\alpha_{r+s}}. \tag{614}$$

Donc, on peut identifier chaque nombre premier et chaque puissance, d'où :

$$u = \left(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}\right)^2 \tag{615}$$
$$v = \left(p_{r+1}^{\alpha_{r+1}} p_{r+2}^{\alpha_{r+2}} \dots p_{r+s}^{\alpha_{r+s}}\right)^2. \tag{616}$$

Donc, u et v sont tous deux des carrés.

5) Donc, il existe deux entiers positifs r et s tels que :

$$u = r^2 \tag{617}$$
$$v = s^2. \tag{618}$$

D'où :

$$\frac{z + x}{2} = r^2 \tag{619}$$
$$\frac{z - x}{2} = s^2. \tag{620}$$

6) On a :

$$(r,s) = (r^2, s^2) = \frac{(2r^2, 2s^2)}{2} = \frac{(z+x, z-x)}{2} = 1. \tag{621}$$

Puis, nous avons $r^2 > s^2$, donc $r > s$, et :

$$\frac{z+x}{2} + \frac{z-x}{2} = r^2 + s^2. \tag{622}$$

Donc :

$$z = r^2 + s^2. \tag{623}$$

Et :

$$\frac{z+x}{2} - \frac{z-x}{2} = r^2 - s^2. \tag{624}$$

Donc :

$$x = r^2 - s^2. \tag{625}$$

Et par conséquent :

$$\begin{aligned} y^2 &= z^2 - x^2 && (626)\\ &= (r^2+s^2)^2 - (r^2-s^2)^2 && (627)\\ &= r^4 + 2r^2s^2 + s^4 - r^4 + 2r^2s^2 - s^4 && (628)\\ &= 4r^2s^2. && (629) \end{aligned}$$

D'où $y = 2rs$.
Par ailleurs, comme z est impair, et $z = r^2 + s^2$, r et s sont de parités opposées.

7) Inversement, considérons une solution candidate sous la forme :

$$\begin{aligned} x &= r^2 - s^2 && (630)\\ y &= 2rs && (631)\\ z &= r^2 + s^2. && (632) \end{aligned}$$

Alors, une telle solution répond au besoin :

$$\begin{aligned} x^2 + y^2 &= r^4 - 2r^2s^2 + s^4 + 4r^2s^2 && (633)\\ &= r^4 + 2r^2s^2 + s^4 && (634)\\ &= (r^2+s^2)^2 && (635)\\ &= z^2. && (636) \end{aligned}$$

C.Q.F.D.

BEATRIX : Je vais faire quelques essais :

1) $r = 2$.
$s = 1$.
$x = 2^2 - 1^2 = 3$.
$y = 2 \times 2 \times 1 = 4$.
$z = 2^2 + 1^2 = 5$.
Solution : $(3, 4, 5)$; $3^2 + 4^2 = 5^2$.

2) $r = 3$.
$s = 2$.
$x = 3^2 - 2^2 = 9 - 4 = 5$.
$y = 2 \times 3 \times 2 = 12$.
$z = 3^2 + 2^2 = 9 + 4 = 13$.
Solution : $(5, 12, 13)$; $5^2 + 12^2 = 13^2$.

3) $r = 4$.
$s = 3$.
$x = 4^2 - 3^2 = 16 - 9 = 7$.
$y = 2 \times 4 \times 3 = 24$.
$z = 4^2 + 3^2 = 16 + 9 = 25$.
Solution : $(7, 24, 25)$; $7^2 + 24^2 = 25^2$.

5.3 Scène V.3 - Equation en puissance 4

EURISTIDE : Nous allons maintenant aborder l'équation $x^4 + y^4 = z^2$. Cette fois, il s'agira de démontrer que cette équation n'a pas de solutions entières. Pour le démontrer, nous allons utiliser une méthode chère à Fermat : la descente infinie. Cette méthode, basée sur le principe de la démonstration par l'absurde, consiste à déduire une propriété étape par étape, de façon à ce que cette propriété fasse appel à des entiers de plus en plus petits au fur et à mesure des déductions. Cela conduit à une contradiction, parce que la propriété ne peut se propager ainsi vers des nombres de plus en plus petits indéfiniment, puisqu'on finit par atteindre l'entier 0.
C'est pourquoi la méthode s'appelle la descente infinie.

BEATRIX : C'est effectivement très astucieux. Quel génie, ce Fermat !

MATHINE : Voici donc un théorème concernant une équation en puissance 4.

Théorème 5.3.1
Equation en puissance 4
L'équation diophantienne :

$$x^4 + y^4 = z^2 \tag{637}$$

n'a aucune solution en entiers x, y, z pour $x, y, z \neq 0$.

Démonstration :

Nous allons faire une démonstration par l'absurde, et utiliser la méthode de la descente infinie de Fermat.
Supposons donc que x, y, z soit une solution.
Supposons que $(x, y, z) = d$.
Alors, il existe $u, v, w \in \mathbb{Z}$ tels que :

$$x = ud \tag{638}$$
$$y = vd \tag{639}$$
$$z = wd. \tag{640}$$

Alors, puisque :

$$x^4 + y^4 = z^2, \tag{641}$$

on a :

$$d^4u^4 + d^4v^4 = d^2w^2. \tag{642}$$

Donc, en divisant par d^2 :

$$d^2u^2 + d^2v^2 = w^2. \tag{643}$$

Alors, $(u, v, w) = 1$ par définition du pgcd d, et par conséquent :

$$(du, dv, w) = 1. \tag{644}$$

Donc, nous sommes ramenés à une équation :

$$x'^2 + y'^2 = z'^2, \tag{645}$$

où $(x', y', z') = 1$.
Nous allons donc supposer dans la suite que $(x, y, z) = 1$.
Nous pouvons écrire :

$$(x^2)^2 + (y^2)^2 = z^2. \tag{646}$$

Donc, x^2, y^2 et z sont racines de l'équation pythagoricienne, et ils sont premiers entre eux, puisque si $(x, y, z) = 1$, alors $(x^2, y^2, z) = 1$.
Donc, d'après le théorème sur l'équation pythagoricienne (cf. 5.2.1), nous savons qu'il existe deux entiers r et s, de parités opposées, premiers entre eux, et tels que $r > s$, tels que :

$$x^2 = r^2 - s^2 \tag{647}$$
$$y^2 = 2rs \tag{648}$$
$$z = r^2 + s^2. \tag{649}$$

Démontrons que r est impair.
Supposons que r est pair. Alors s est impair. Puisque r est pair, alors $r^2 \equiv 0 \pmod 4$
Donc :

$$x^2 \equiv -s^2 \pmod 4, \tag{650}$$

et par conséquent, on aurait :

$$x^2 \equiv -1 \pmod 4. \tag{651}$$

Mais un carré ne peut pas être congru à -1 modulo 4. En effet, si un entier a est pair, son carré est congru à 0 modulo 4. S'il est impair, alors il est congru à 1 modulo 2, donc son carré est congru à 1 modulo 4. Donc, nous aboutissons à une contradiction.
Donc r est impair.
On a :

$$(x^2)^2 + s^2 = r^2. \tag{652}$$

Donc x^2, s et r sont solution d'une nouvelle équation pythagoricienne, telle que $(x^2, s, r) = 1$.
Nous pouvons donc de nouveau appliquer le théorème sur l'équation pythagoricienne, et écrire qu'il existe des entiers a et b tels que $(a, b) = 1$ et $a > b$ et :

$$s = 2ab \tag{653}$$
$$x^2 = a^2 - b^2 \tag{654}$$
$$r = a^2 + b^2. \tag{655}$$

Or, nous savons que :

$$y^2 = 2rs. \tag{656}$$

Donc :

$$y^2 = 4ab(a^2 + b^2). \tag{657}$$

Or, a et b sont premiers entre eux, donc $(a, b) = 1$.
Par conséquent :

$$(a, b^2) = 1. \tag{658}$$

Et donc :

$$(a, a^2 + b^2) = 1. \tag{659}$$

En effet, si :

$$(a, a^2 + b^2) = d, \tag{660}$$

alors :

$$\begin{aligned} a &= kd & (661)\\ a^2 + b^2 &= k'd. & (662) \end{aligned}$$

D'où :

$$k'^2 d^2 + b^2 = k'd. \tag{663}$$

Donc d diviserait b.
Donc a et b diviseraient d, donc $d = 1$, puisque $(a, b) = 1$.
Par conséquent :

$$(a, a^2 + b^2) = 1. \tag{664}$$

De la même façon :

$$(b, a^2 + b^2) = 1. \tag{665}$$

Donc, nous avons :

$$y^2 = 4ab(a^2 + b^2), \tag{666}$$

avec a, b et $a^2 + b^2$ premiers entre eux deux à deux. Donc, nous avons vu que chacun des termes doit alors être un carré. Donc a, b, $a^2 + b^2$ sont des carrés :

$$\begin{aligned} a &= u^2 & (667)\\ b &= v^2 & (668)\\ a^2 + b^2 &= w^2, & (669) \end{aligned}$$

ce que nous pouvons écrire, en reportant les expressions de a et b dans la dernière égalité :

$$u^4 + v^4 = w^4. \tag{670}$$

Par construction, u, v, et w sont plus petits que x, y et z. Nous avons donc construit une nouvelle égalité dont les termes sont strictement inférieurs aux précédents.
En poursuivant ainsi indéfiniment, on aboutit à une contradiction, puisque l'ensemble des entiers $\mathbb{N}$ possède une borne inférieure 0.

C.Q.F.D.

BEATRIX : C'est une bien jolie démonstration !

EURISTIDE : Nous allons maintenant parler un peu du Grand Théorème de Fermat. C'est le but de

notre discussion aujourd'hui, donc il vaut bien un détour. Ce théorème était une conjecture à l'origine, puisque nous n'avions pas de démonstration disponible.
Fermat avait fait un commentaire sur ce théorème dans la marge d'un manuscrit des Arithmétiques de Diophante :

> Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestarum in duos ejusdem nominis fas est dividere : cujes rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caparet.
> Pierre de Fermat - 1637.
>
> Il n'est pas possible de diviser un cube en deux cubes, ni une puissance quatre en deux puissances quatre, ni plus généralement toute puissance plus grande que le carré en deux telles puissances : j'ai découvert une merveilleuse démonstration de cette proposition. Mais la marge est trop étroite pour la contenir.

BEATRIX : C'est donc ce problème qui a été résolu en 1993 par Wiles.

EURISTIDE : Oui. Et c'est l'objet de notre discussion aujourd'hui. Nous allons faire un voyage extrêmement long dans les mondes de l'algèbre, de la topologie, et de la théorème des nombres moderne pour parvenir à démontrer ce fameux théorème dont Fermat disait simplement qu'il manquait de place dans la marge des Arithmétiques de Diophante pour écrire la démonstration.

BEATRIX : Amusant. On peut penser que Fermat avait une démonstration erronée, n'est-ce pas ?

EURISTIDE : Soit sa démonstration était réellement géniale, avec les connaissances de son époque, pour que personne ne la trouve pendant plus de trois siècles. Soit sa démonstration comportait une erreur. Mais nous ne le saurons sans doute jamais, à moins qu'une personne ne découvre finalement une démonstration faisant appel aux mathématiques connues à l'époque de Fermat.
Nous allons voir maintenant des équations de congruences du second degré. Cela nous permettra d'étudier la notion de réciprocité quadratique, vue par Gauss, notion que nous retrouverons plus tard dans nos développements sur l'algèbre.

6 Acte VI - Réciprocité quadratique

6.1 Scène VI.1 - Résidus quadratiques

BEATRIX : Qu'est-ce que la réciprocité quadratique ?

MATHINE : Avant de parler de réciprocité quadratique, nous allons parler des résidus quadratiques.

Définition **6.1.1**
Résidu quadratique
Soit a un entier et p un nombre premier.
On suppose que p est impair (donc $p > 2$).

On suppose également que $(a, p) = 1$.
Si la congruence :

$$x^2 \equiv a \pmod{p}, \tag{671}$$

possède une solution, on dit que a *est un résidu quadratique modulo* p.
Si la congruence ci-dessus n'a pas de solution, on dit que a *est un non-résidu quadratique modulo* p.

EURISTIDE : Autrement dit, les résidus quadratiques sont les entiers qui ont même reste dans la division euclidienne par p qu'un carré.

BEATRIX : Donc un carré est toujours un résidu quadratique, n'est-ce pas ?

MATHINE : En effet. Nous aurons également besoin de la définition suivante.

Définition **6.1.2**
Symbole de Legendre
Soit a *un entier et* p *un nombre premier impair tels que* a *et* p *soient premiers entre eux.*
On définit le symbole de Legendre $\left(\frac{a}{p}\right)$ *par :*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } a \text{ est un non-résidu quadratique modulo } p. \end{cases} \tag{672}$$

EURISTIDE : Le symbole de Legendre est en quelque sorte un moyen de repérer les résidus quadratiques, et il permet de transformer une notion logique "être résidu quadratique" en une expression arithmétique qui peut être intégrée dans un calcul.

BEATRIX : Donc cela veut dire qu'on va pouvoir calculer ce symbole de Legendre ?

EURISTIDE : Oui, exactement.

MATHINE : C'est l'objet du prochain théorème, qui donne un critère pour déterminer si un entier est un résidu quadratique ou non. Et c'est naturellement le symbole de Legendre qui est calculé pour ce critère. c'est ce qu'on appelle le critère d'Euler.

Théorème **6.1.1 (Critère d'Euler)** *Soit* p *un nombre premier impair. Alors, pour tout entier* a *tel que* a *est premier avec* p, *on a :*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{673}$$

EURISTIDE : Intuitivement, cette relation peut se comprendre de la façon suivante. En passant cette relation au carré, on voit que :

$$\left(\frac{a}{p}\right)^2 \equiv a^{p-1} \pmod{p}. \tag{674}$$

Mais, le petit théorème de Fermat (cf. 4.2.2) nous a appris que :

$$a^{p-1} \equiv 1 \pmod{p}. \tag{675}$$

Donc :

$$\left(\frac{a}{p}\right)^2 \equiv \left(a^{(p-1)/2}\right)^2 \equiv 1 \pmod{p}, \tag{676}$$

c'est-à-dire que les deux seules valeurs de congruence de $a^{(p-1)/2}$ sont 1 ou -1.
Et en particulier, si a est un résidu quadratique, il est congru à un carré x_0^2, donc s'écrit :

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} \pmod{p}, \tag{677}$$

qui, encore une fois, par le petit théorème de Fermat, est congru à 1 modulo p.

MATHINE : Voici la démonstration plus formelle de ce théorème.

Démonstration :

Nous allons distinguer deux cas.

1) En effet, si a est un résidu quadratique, alors il existe $x_0 \in \mathbb{Z}$ tel que :

$$x_0^2 \equiv a \pmod{p}. \tag{678}$$

En substituant cette expression dans $a^{(p-1)/2}$, nous obtenons :

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} \pmod{p} \tag{679}$$
$$\equiv x_0^{p-1} \pmod{p}. \tag{680}$$

D'après le petit théorème de Fermat, si $p \nmid b$, on a :

$$b^{p-1} \equiv 1 \pmod{p}. \tag{681}$$

Ici, a et p sont premiers entre eux, donc a fortiori, x_0 et p sont premiers entre eux et donc x_0 ne divise pas p. Donc :

$$x_0^{p-1} \equiv 1 \pmod{p}. \tag{682}$$

Et par conséquent :

$$a^{(p-1)/2} \equiv 1 \pmod{p}. \tag{683}$$

Ceci est conforme à la valeur suivante, lorsque a est résidu quadratique :

$$\left(\frac{a}{p}\right) = 1, \tag{684}$$

donc, nous avons bien dans ce cas :

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{685}$$

2) Supposons maintenant que a est non-résidu quadratique.
Alors, l'équation de congruence :

$$x^2 \equiv a \pmod{p}, \tag{686}$$

n'a pas de solution.
Cela signifie que si nous considérons un entier u quelconque dans $[1, p[$, il n'est pas possible d'avoir :

$$u^2 \equiv a \pmod{p}. \tag{687}$$

En revanche, il est toujours possible de trouver un entier v dans $[1, p[$, unique d'ailleurs, tel que :

$$uv \equiv a \pmod{p}. \tag{688}$$

En effet, pour u donné, $uv \equiv a \pmod{p}$ est une équation de congruence, où $(v, p) = 1$. Donc elle possède une solution $v = v_0$, et toutes les autres solutions sont :

$$v = v_0 + kp. \tag{689}$$

Donc, nécessairement une solution se trouve dans l'intervalle $[1, p[$. Donc nous pouvons ainsi constituer $\frac{p-1}{2}$ congruences, de la forme :

$$u_i v_i \equiv a \pmod{p}, \tag{690}$$

pour $i \in [1, \frac{p-1}{2}]$.
Notons $x_i = u_i v_i$, en faisant parcourir u_i dans $[1, p[$. Est-il possible que l'un des v_j soit égal à l'un des u_i ? Alors, nous aurions $u_j u_i \equiv a \pmod{p}$ et $v_i u_i \equiv a \pmod{p}$. Or, il n'y a qu'une solution à l'équation de congruence $u_i x \equiv a \pmod{p}$ dans l'intervalle $[1, p[$, donc cela signifie que $u_j = u_i$.
Alors, en multipliant membre à membre ces congruences, nous obtenons :

$$\prod_{i=1}^{p-1} x_i \equiv a^{(p-1)/2} \pmod{p}. \tag{691}$$

Comme nous l'avons vu, les u_i et les v_i sont tous distincts et ils parcourent $[1, p[$, c'est-à-dire qu'ils parcourent les $p-1$ entiers de 1 à $p-1$. Par conséquent, nous avons :

$$\prod_{i=1}^{p-1} x_i = (p-1)! \tag{692}$$

Or, d'après le théorème de Wilson (cf. 4.4.1) :

$$(p-1)! \equiv -1 \pmod{p}. \tag{693}$$

Donc, nous avons bien :

$$a^{(p-1)/2} \equiv -1 \pmod{p}. \tag{694}$$

Donc la relation :

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \tag{695}$$

est également vérifiée lorsque a est non-résidu quadratique.

C.Q.F.D.

BEATRIX : Ouf ! Pas simple, cette démonstration.

EURISTIDE : En fait, cette démonstration se résume à deux aspects. Le cas du résidu quadratique nous ramène au petit théorème de Fermat, comme je l'ai expliqué tout à l'heure. Le cas du non-résidu quadratique se ramène au théorème de Wilson avec $(p-1)!$ en construisant des couples d'entiers inférieurs à $p-1$, donc le produit est congru à p.

MATHINE : Etudions maintenant quelques propriétés du symbole de Legendre.

Proposition 6.1.1
Propriétés symbole de Legendre
Soit p un nombre premier impair.
Soit $a, b \in \mathbb{Z}$, a et b premiers avec p.
Alors :

i) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

ii) $\left(\frac{a^2}{p}\right) = 1$.

iii) $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

iv) $\left(\frac{1}{p}\right) = 1$.

v) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

EURISTIDE : Intuitivement, la première propriété découle des constats suivants : si un entier est non résidu quadratique, la multiplication par un entier résidu quadratique en fera un non résidu quadratique également. De même, le produit de deux entiers résidus quadratiques fera un résidu quadratique évidemment. Le cas délicat est le produit de deux entiers non résidus quadratiques. La proposition nous indique un fait qui n'est pas forcément très intuitif : le produit de deux entiers qui sont non résidus quadratiques est un résidu quadratique.

BEATRIX : Oui, en effet, c'est un peu inattendu. Y-a-t-il une explication intuitive ?

EURISTIDE : C'est l'explication basée sur le théorème de Wilson qui nous aide à comprendre. En faisant, comme dans la démonstration du théorème du critère d'Euler (cf. 6.1.1), les produits de tous les $u_i v_i$ et $u'_i v'_i$, où d'une part $u_i \neq v_i$, $u_i, v_i \in [1, p[$ et $u_i v_i \equiv a \pmod p$, et d'autre part $u'_i \neq v'_i$, $u'_i, v'_i \in [1, p[$ et $u'_i v'_i \equiv b \pmod p$, on duplique, en quelque sorte tous les entiers de 1 à $p-1$, et on obtient à gauche de la congruence un carré élevé à la puissance $(p-1)/2$ et à droite de la congruence, le produit ab élevé à la puissance $(p-1)/2$. En prenant la racine $(p-1)/2$-ième de cette congruence, on trouve bien un carré congru au produit ab.

BEATRIX : En d'autres termes, le produit nous conduit à créer des redondances sur les paires d'entier possibles dont le produit peut être congru à a. Et ces redondances nous conduisent nécessairement à trouver parmi elles un carré congru au produit ab. J'ai compris !

EURISTIDE : La propriété ii) de notre proposition est tout à fait naturelle. Il suffit de choisir a comme solution de l'équation de congruence.
La propriété iii) découle de la seconde sur les carrés et de la première sur les produits.
La propriété iv) provient du fait que 1 peut être considéré comme un carré, le carré de 1.
La dernière propriété est une réécriture quasiment directe du critère d'Euler. Elle signifie en particulier qu'un carré ne peut être congru à -1 modulo un nombre premier p que si $p \equiv 1 \pmod 4$.

MATHINE : Voici la démonstration exacte.

Démonstration :

i) D'après le critère d'Euler :

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2}b^{(p-1)/2} \pmod p \tag{696}$$

$$\equiv (ab)^{(p-1)/2} \pmod p \tag{697}$$

$$\equiv \left(\frac{ab}{p}\right) \pmod p. \tag{698}$$

Or, les symboles de Legendre ne prennent pour valeurs que -1 ou 1.
Donc la différence :

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \tag{699}$$

ne prend pour valeurs possibles que 0, 2 ou -2.
La congruence :

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod p \tag{700}$$

signifie que $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)$ a pour reste 0 dans la division euclidienne par p.
Donc, puisque $p > 2$:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right). \tag{701}$$

ii) Nous pouvons écrire :

$$a^2 \equiv a^2 \pmod p. \tag{702}$$

Donc :

$$\left(\frac{a^2}{p}\right) = 1. \tag{703}$$

iii) Nous savons d'après ii) que :

$$\left(\frac{a^2}{p}\right) = 1. \tag{704}$$

Et par ailleurs, d'après i), nous avons :

$$\left(\frac{a^2}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{a^2 b}{p}\right). \tag{705}$$

Donc :

$$\left(\frac{a^2 b}{p}\right) = 1. \tag{706}$$

iv) Nous pouvons écrire :

$$1^2 \equiv 1 \pmod{p}. \tag{707}$$

Donc :

$$\left(\frac{1}{p}\right) = 1. \tag{708}$$

v) Nous avons, d'après le critère d'Euler (cf. 6.1.1) :

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}. \tag{709}$$

Or, ou bien :

$$\left(\frac{-1}{p}\right) = -1, \tag{710}$$

ou bien :

$$\left(\frac{-1}{p}\right) = 1. \tag{711}$$

Donc, finalement :

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{712}$$

C.Q.F.D.

6.2 Scène VI.2 - Lemme de Gauss

BEATRIX : En résumé, le symbole de Legendre ressemble à un artifice de calcul, puisque ses valeurs sont conventionnelles. Mais le choix est très judicieux, parce que les lois calculatoires sont cohérentes et naturelles.

EURISTIDE : Oui, c'est une représentation bien utile, parce qu'on peut développer des calculs avec ce symbole, en oubliant un peu son caractère artificiel.

MATHINE : Nous allons maintenant découvrir un théorème appelé lemme de Gauss, qui nous sera indispensable pour la suite, et qui apporte une nouvelle expression du symbole de Legendre.

Théorème **6.2.1 (Lemme de Gauss)** *Soit p un nombre premier impair. Soit a un entier premier avec p. Considérons les entiers a, $2a$, ..., $\frac{p-1}{2}a$ et leurs plus petits résidus positifs modulo p.*
Soit n le nombre de ces résidus qui excèdent $\frac{p}{2}$. Alors :

$$\left(\frac{a}{p}\right) = (-1)^n. \tag{713}$$

BEATRIX : Encore une propriété ésotérique ! Mais d'où vient ce mystérieux n ?

EURISTIDE : Ce n'est effectivement pas une propriété immédiate.
Cette propriété repose de nouveau sur la propriété :

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{714}$$

Il nous faut donc comprendre pourquoi $a^{(p-1)/2} \equiv (-1)^n \pmod{p}$.
Pour le comprendre, nous considérons les multiples de a et leurs résidus. Si on considère les résidus inférieurs à $p/2$ (tous distincts) d'une part, et les résidus supérieurs à $p/2$ d'autre part (tous distincts également), ces derniers, lorsqu'on les retranche à p constituent alors avec les premiers la liste complète des entiers de 1 à $\frac{p-1}{2}$. Si ce n'était pas le cas, on trouverait deux résidus dont la somme est p, donc congrue à 0 modulo p, ce qui conduirait à construire un multiple de a congru à 0 modulo p, ce qui serait contradictoire avec le fait que a et p sont premiers entre eux.
Une fois qu'on a constitué cette collection d'entiers de 1 à $\frac{p-1}{2}$, on applique le théorème de Wilson (cf. 4.4.1) à leur produit qui est la factorielle $\left(\frac{p-1}{2}\right)!$, congru à -1 modulo p. Par ailleurs, le produit des résidus donne également cette factorielle $\left(\frac{p-1}{2}\right)!$, mais ceux supérieurs à $p/2$ qui ont été préalablement retranchés à p vont donner un signe négatif. Comme il y en a n de cette espèce, on obtient le facteur recherché $(-1)^n$.

MATHINE : Voici la démonstration précise.

Démonstration :

Considérons les entiers a, $2a$, $3a$,..., $\frac{p-1}{2}a$. Ces entiers sont tous non congrus entre eux modulo p, par hypothèse de primalité de p.
En effet, si on avait :

$$ia \equiv ja \pmod{p}, \tag{715}$$

alors, on aurait :

$$i \equiv j \pmod{p}, \tag{716}$$

avec i et $j < \frac{p-1}{2}$, donc $i - j$ diviserait p, ce qui serait contradictoire avec p premier.
Classons leurs plus petits résidus positifs en deux ensembles disjoints.
Soit $u_1, u_2, \ldots, u_r$ les résidus inférieurs à $p/2$.
Soit $v_1, v_2, \ldots, v_n$ les résidus supérieurs à $p/2$.
Bien sûr, ces $\frac{p-1}{2}$ résidus sont tous distincts dans l'ensemble des entiers de 1 à p.
Pour les v_i, considérons les entiers :

$$v'_i = p - v_i, \tag{717}$$

pour i de 1 à n.
Supposons qu'il existe un $j \in [1, r]$ tel que :

$$v'_i = u_j. \tag{718}$$

Alors, on aurait :

$$p - v_i = u_j, \tag{719}$$

donc :

$$p = u_j + v_i, \tag{720}$$

d'où :

$$u_j + v_i \equiv 0 \pmod{p}. \tag{721}$$

Or, par définition de u_j, il existe un entier α dans $[1, \frac{p-1}{2}]$ tel que :

$$\alpha a \equiv u_j \pmod{p}, \tag{722}$$

et il existe un entier β dans $[1, \frac{p-1}{2}]$ tel que :

$$\beta a \equiv v_i \pmod{p}. \tag{723}$$

Par conséquent :

$$\alpha a + \beta a \equiv u_j + v_i \pmod{p}, \tag{724}$$

et par suite :

$$\alpha a + \beta a \equiv 0 \pmod{p}, \tag{725}$$

soit :

$$\alpha a \equiv \beta a \pmod{p}, \tag{726}$$

ce qui est contradictoire avec nos hypothèses initiales.
Donc, les v'_i et les u_j sont tous distincts deux à deux.
Or ce sont tous des entiers inférieurs à $p/2$, et ils sont au nombre de $\frac{p-1}{2}$.
Par conséquent, l'ensemble réuni des v'_i et des u_j constitue l'ensemble des entiers de 1 à $\frac{p-1}{2}$.
Donc leur produit est :

$$\prod_{i=1}^{n} v'_i \prod_{j=1}^{r} u_j = \left(\frac{p-1}{2}\right)! \tag{727}$$

Or $v'_i = p - v_i$.
Donc :

$$\begin{aligned} \prod_{i=1}^{n} v'_i \prod_{j=1}^{r} u_j &\equiv \prod_{i=1}^{n} (-v_j) \prod_{j=1}^{r} u_j \pmod{p} && (728) \\ &\equiv (-1)^n \prod_{i=1}^{n} v_j \prod_{j=1}^{r} u_j \pmod{p}. && (729) \end{aligned}$$

Or, chaque v_k et chaque u_k est congru à un $\alpha_k a$ différent, α_k parcourt donc tous les entiers de 1 à $\frac{p-1}{2}$.
Donc, le produit obtenu précédemment s'écrit :

$$\prod_{i=1}^{n} v'_i \prod_{j=1}^{r} u_j \equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}. \tag{730}$$

Donc, on a obtenu finalement :

$$(-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{p}, \tag{731}$$

ou encore :

$$(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{732}$$

Or, d'après le critère d'Euler (cf. 6.1.1) :

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}. \tag{733}$$

Donc, finalement :

$$\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}. \tag{734}$$

Mais, comme $\left(\frac{a}{p}\right)$ ne peut prendre que les valeurs -1 ou 1, la congruence se transforme en égalité :

$$\left(\frac{a}{p}\right) = (-1)^n. \tag{735}$$

C.Q.F.D.

6.3 Scène VI.3 - Loi de réciprocité quadratique

EURISTIDE : Nous sommes maintenant bien armés pour aborder la loi de réciprocité quadratique. Nous verrons que cette loi nous permet de déterminer aisément les racines d'une équation de congruence du deuxième degré.

MATHINE : Avant de commencer, il nous faut déterminer plus précisément la valeur de n dans le Lemme de Gauss (cf. 6.2.1). Pour cela, nous allons démontrer le lemme suivant.

Lemme **6.3.1**
Nombre de résidus plus grands que p/2
Soit p un nombre premier, $p > 2$.
Soit $a \in \mathbb{Z}$ tel que a soit premier avec p.
Alors :

$$\left(\frac{a}{p}\right) = (-1)^n, \tag{736}$$

avec :

$$n \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right] + \frac{1}{8}(a-1)(p^2-1) \pmod{2}. \tag{737}$$

EURISTIDE : Le symbole $[x]$ représente la partie entière du nombre réel x. Par exemple $[0,5] = 0$, $\left[\frac{3}{2}\right] = 1$.

MATHINE : Passons maintenant à la démonstration de ce lemme.

Démonstration :

Soit i un entier tel que $1 \leq i \leq \frac{p-1}{2}$.
On peut écrire :

$$\frac{ia}{p} = \left[\frac{ia}{p}\right] + \epsilon, \tag{738}$$

où ϵ est un nombre rationnel de la forme $\frac{x}{p}$ compris entre 0 et 1 :

$$0 < \epsilon < 1. \tag{739}$$

Par conséquent, en multipliant l'égalité précédente par p, nous obtenons :

$$ia = p\left[\frac{ia}{p}\right] + \epsilon p, \tag{740}$$

soit :

$$ia = p\left[\frac{ia}{p}\right] + a_i, \tag{741}$$

où a_i est un entier tel que $0 < a_i < p$.
Donc a_i est le reste de la division euclidienne de ia par p, donc a_i est le plus petit résidu modulo p de ia.
Donc, si l'on reprend les notations de la démonstration du Lemme de Gauss, on peut partager la somme des résidus a_i en la somme de ceux qui sont plus petits que $\frac{p-1}{2}$ et ceux qui sont plus grands que $\frac{p-1}{2}$, on obtient :

$$\sum_{i=1}^{\frac{p-1}{2}} a_i = \sum_{i=1}^{k} u_i + \sum_{i=1}^{n} v_i. \tag{742}$$

Or, pour tout i, nous avons vu que :

$$a_i = ia - p\left[\frac{ia}{p}\right]. \tag{743}$$

Donc :

$$a\sum_{i=1}^{\frac{p-1}{2}} i - p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right] = \sum_{i=1}^{k} u_i + \sum_{i=1}^{n} v_i. \tag{744}$$

Or, durant la démonstration du Lemme de Gauss, nous avions vu que les u_i et les $p - v_i$ parcouraient entièrement la liste des entiers de 1 à $\frac{p-1}{2}$. Donc :

$$\sum_{i=1}^{k} u_i + \sum_{i=1}^{n} p - v_i = \sum_{i=1}^{\frac{p-1}{2}} i, \tag{745}$$

ou encore :

$$\sum_{i=1}^{k} u_i - \sum_{i=1}^{n} v_i = \sum_{i=1}^{\frac{p-1}{2}} i - np. \tag{746}$$

En additionnant membre à membre les deux égalités précédentes (cf. 744) et (cf. 746), nous avons :

$$2\sum_{i=1}^{k} u_i = (a+1)\sum_{i=1}^{\frac{p-1}{2}} i - np - p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right], \tag{747}$$

que nous pouvons réécrire :

$$2\sum_{i=1}^{k} u_i + np = (a+1)\sum_{i=1}^{(p-1)/2} -p\sum_{i=1}^{(p-1)/2}\left[\frac{ia}{p}\right]. \tag{748}$$

Etudions la congruence modulo 2 des constituants de cette expression :

$$2\sum_{i=1}^{k} u_i \equiv 0 \pmod 2, \tag{749}$$

bien évidemment. Et :

$$p \equiv 1 \pmod 2 \tag{750}$$

par hypothèse. Donc :

$$np \equiv n \pmod 2. \tag{751}$$

Et enfin :

$$a+1 \equiv a-1 \pmod 2. \tag{752}$$

Donc :

$$n \equiv (a-1)\sum_{i=1}^{(p-1)/2} i - p\sum_{i=1}^{(p-1)/2}\left[\frac{ia}{p}\right] \pmod 2. \tag{753}$$

De plus :

$$2p\sum_{i=1}^{(p-1)/2}\left[\frac{ia}{p}\right] \equiv 0 \pmod 2. \tag{754}$$

Donc :

$$n \equiv (a-1)\sum_{i=1}^{(p-1)/2} i + p\sum_{i=1}^{(p-1)/2}\left[\frac{ia}{p}\right] \pmod 2. \tag{755}$$

Enfin :

$$\sum_{i=1}^{(p-1)/2} i \tag{756}$$

est un nombre triangulaire, de valeur :

$$\sum_{i=1}^{(p-1)/2} i = \frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2} \tag{757}$$

$$= \frac{(p-1)(p-1+2)}{8} \tag{758}$$

$$= \frac{p^2-1}{8}. \tag{759}$$

Donc, finalement :

$$n \equiv (a-1)\frac{p^2-1}{8} + p\sum_{i=1}^{(p-1)/2}\left[\frac{ia}{p}\right] \pmod 2. \tag{760}$$

C.Q.F.D.

EURISTIDE : Nous voici maintenant équipés pour parler de la fameuse loi de réciprocité quadratique.

BEATRIX : En quoi consiste-t-elle ?

EURISTIDE : C'est une formule qui va nous permettre de calculer le produit des symboles de Legendre de deux nombres premiers impairs distincts. Nous verrons qu'en utilisant la décomposition d'un entier quelconque en facteurs premiers, nous aurons ainsi la possibilité de calculer le symbole de Legendre pour un entier quelconque dans $\mathbb{Z}$.

BEATRIX : A condition de connaître le symbole de Legendre pour -1 et pour 2, parce que d'après ce que vous dites, la loi de réciprocité quadratique s'applique aux nombres premiers impairs uniquement.

EURISTIDE : Oui, c'est bien vu, Béatrix ! Nous verrons cela en traitant un exemple dans quelques instants.

MATHINE : Dans l'immédiat, nous allons énoncer la loi de réciprocité quadratique.

Théorème **6.3.1 (Loi de réciprocité quadratique)** *Soit p et q deux nombres premiers impairs distincts. Alors :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{761}$$

Démonstration :

Pour démontrer ce théorème, nous allons utiliser le lemme que nous avons démontré précédemment, fournissant le nombre de résidus plus grands que $p/2$.

1) Calculons $\left(\frac{p}{q}\right)$.
En appliquant le lemme précédent, nous obtenons :

$$\left(\frac{p}{q}\right) = (-1)^n, \tag{762}$$

où :

$$n \equiv \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right] + \frac{1}{8}(p-1)(q^2-1) \pmod 2. \tag{763}$$

Comme q est impair, soit $q+1$ est divisible par 4, soit $q-1$ est divisible par 4.
Dans tous les cas, $q-1$ et $q+1$ sont tous deux divisibles par 2. Donc $q^2-1=(q-1)(q+1)$ est divisible par 8.
Or p est impair, donc $p-1$ est pair.

Donc $\frac{1}{8}(p-1)(q^2-1)$ est pair.
Donc :

$$\frac{1}{8}(p-1)(q^2-1) \equiv 0 \pmod 2. \tag{764}$$

Donc :

$$n \equiv \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right] \pmod 2. \tag{765}$$

Par ailleurs, pour chaque j, $\left[\frac{jp}{q}\right]$ représente le nombre de fois que l'on peut juxtaposer la longueur q dans la longueur jp, autrement dit, il représente le nombre d'entiers $i \in [1, \frac{p-1}{2}]$ tels que $qi < jp$.

2) Calculons $\left(\frac{q}{p}\right)$.
Un raisonnement équivalent au précédent nous conduit à :

$$n \equiv \sum_{i=1}^{(p-1)/2} \left[\frac{iq}{p}\right] \pmod 2, \tag{766}$$

et donc pour chaque i, $\left[\frac{iq}{p}\right]$ représente le nombre d'entiers $j \in [1, \frac{p-1}{2}]$ tels que $jp < iq$.

3) Par ailleurs, puisque p et q sont premiers, il n'y a pas d'entiers i et j tels que $qi = jp$.
Donc, le nombre d'entiers $i, j \in [1, \frac{p-1}{2}]$ tels que $qi < jp$ et $qi > jp$ représente la totalité des entiers i, j appartenant à $[1, \frac{p-1}{2}]$.
Donc :

$$\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right] + \sum_{i=1}^{(p-1)/2} \left[\frac{iq}{p}\right] = \frac{p-1}{2}.\frac{q-1}{2}. \tag{767}$$

Donc finalement :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}. \tag{768}$$

C.Q.F.D.

EURISTIDE : Nous allons appliquer cette loi pour déterminer s'il existe des solutions à l'équation de congruences :

$$x^2 \equiv -21 \pmod{31}. \tag{769}$$

Je te laisse faire, Béatrix.

BEATRIX : Pour savoir s'il existe des solutions à cette équation, il faut calculer le symbole de Legendre :

$$\left(\frac{-21}{31}\right). \tag{770}$$

Mais, comme $-21 \equiv 10 \pmod{31}$, on peut écrire :

$$\left(\frac{-21}{31}\right) = \frac{10}{31}. \tag{771}$$

Or, $10 = 2 \times 5$, donc en appliquant la propriété de multiplicativité du symbole de Legendre (cf. 6.1.1), on obtient :

$$\left(\frac{-21}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{5}{31}\right). \tag{772}$$

Or, en appliquant la loi de réciprocité quadratique (cf. 6.3.1), on obtient :

$$\begin{aligned}
\left(\frac{5}{31}\right)\left(\frac{31}{5}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{31-1}{2}} && (773)\\
&= (-1)^{\frac{4}{2}\frac{30}{2}} && (774)\\
&= (-1)^3 0 && (775)\\
&= 1. && (776)
\end{aligned}$$

Donc :

$$\left(\frac{5}{31}\right) = \left(\frac{31}{5}\right). \tag{777}$$

Or $31 \equiv 1 \pmod 5$, donc :

$$\left(\frac{31}{5}\right) = \left(\frac{1}{5}\right). \tag{778}$$

Alors, 1 étant un carré, on sait que :

$$\left(\frac{1}{5}\right) = 1. \tag{779}$$

Par ailleurs, nous savons que :

$$\left(\frac{2}{p}\right) = (-1)^n, \tag{780}$$

où :

$$n \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{2j}{p}\right] + \frac{1}{8}(p^2-1) \pmod 2. \tag{781}$$

Le premier terme de la congruence est évidemment un multiple de 2, donc il s'annule dans la congruence et nous obtenons :

$$n \equiv \frac{p^2-1}{8} \pmod 2. \tag{782}$$

Donc, on peut écrire :

$$\begin{aligned}
\left(\frac{2}{31}\right) &= (-1)^{\frac{31^2-1}{8}} && (783)\\
&= (-1)^{120} && (784)\\
&= 1. && (785)
\end{aligned}$$

Donc, finalement :

$$\begin{aligned}
\left(\frac{-21}{31}\right) &= \left(\frac{2}{31}\right)\left(\frac{5}{31}\right) && (786)\\
&= 1 \times 1 && (787)\\
&= 1. && (788)
\end{aligned}$$

Donc, l'équation de congruence $x^2 \equiv -21 \pmod{31}$ a des solutions.

7 Acte VII - Fonctions de la théorie des nombres

EURISTIDE : Voilà. Nous avons fini notre petit tour d'horizon de la théorie des nombres classique.
Avant de passer à l'algèbre, qui constitue les fondements de la théorie des nombres moderne, nous allons lister à l'aide de Mathine, un certain nombre de fonctions de la théorie des nombres classique qui nous seront bien utiles.

BEATRIX : Nous avons déjà vu la fonction d'Euler (cf. 4.1.5), qui donne le nombre d'entiers premiers avec un entier donné et qui sont inférieurs à celui-ci. Et nous avons utilisé également la partie entière d'un nombre réel.

MATHINE : En voici donc une collection complémentaire.

Définition **7.0.1**
Nombre de diviseurs
Soit $n \in \mathbb{N}$. La fonction tau :

$$\tau : n \longmapsto \tau(n) \tag{789}$$

désigne le nombre de diviseurs de n.

Définition **7.0.2**
Somme des diviseurs
Soit $n \in \mathbb{N}$. La fonction sigma :

$$\sigma : n \longmapsto \sigma(n) \tag{790}$$

désigne la somme des diviseurs de n.

Définition **7.0.3**
Nombre de facteurs premiers
Soit $n \in \mathbb{N}$. La fonction omega :

$$\omega : n \longmapsto \omega(n) \tag{791}$$

désigne le nombre de facteurs premiers distincts dans la décomposition canonique de n.

Définition **7.0.4**
Fonction de Moebius
Soit $n \in \mathbb{N}$. La fonction de Moebius est définie par :

$$\mu : n \longmapsto \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par un carré} \\ (-1)^{\omega(n)} & \text{sinon} \end{cases} . \tag{792}$$

Index