Arithmétique dans Z

1- Congruences

1.1. Définitions et propriétés.

On fixe dans toute cette partie un entier $n \geq 1$.

Définition (Congruence) : Soient $a,b \in$ Z et $n \in$ N*. On dit que a et b sont *congrus modulo* n si l'entier n divise $a - b$. On note $a \equiv b \mod n$ ou encore $a \equiv b\ [n]$. Cette relation s'appelle *relation de congruence modulo* n.

Exemple : (1) $7 \equiv 1 \mod 6$ car $7 - 1 = 1 \times 6$ est divisible par 6.

(2) $31 \equiv 11 \mod 4$ car $31 - 11 = 20 = 5 \times 4$.

Fait 1 (important) : (1) $a \equiv b \mod n \Longleftrightarrow \exists k \in$ Z : $a = b + kn$.

(2) $a \equiv 0 \mod n \Longleftrightarrow n \mid a$.

Lemme (Propriétés des congruences) : *Soient* $a,b,c,d \in$ Z *et* $n \in$ N*. *Alors,*

(i) *Réflexivité :* $a \equiv a \mod n$,

(ii) *Symétrie :* $a \equiv b \mod n \implies b \equiv a \mod n$,

(iii) *Transitivité :* $a \equiv b \mod n$ *et* $b \equiv c \mod n \implies a \equiv c \mod n$,

(iv) $a \equiv c \mod n$ *et* $b \equiv d \mod n \implies a + b \equiv c + d \mod n$,

(v) $a \equiv c \mod n$ *et* $b \equiv d \mod n \implies ab \equiv cd \mod n$. *En particulier, pour tout* $k \in$ N, *on a* $a^k \equiv c^k \mod n$.

Exemple (récurrence) : $7^n - 1$ est divisible par 6 pour tout $n \in$ N (ou encore $7^n \equiv 1 \mod 6$). En effet, on peut procéder par récurrence sur n.

Si $n = 0$: $7^n - 1 = 1 - 1 = 0$ est bien divisible par 6.

Supposons que pour un certain $n \geq 0$, $7^n - 1$ est divisible par 6 et montrons que c'est encore le cas pour $7^{n+1} - 1$. On a $7^{n+1} = 7 \times 7^n$. Or $7 \equiv 1 \mod 6$

et $7^n \equiv 1 \mod 6$ par hypothèse de récurrence. Alors la propriété (v) du lemme 8 entraîne que $7 \times 7^n \equiv 1 \times 1 \mod 6$, c'est-à-dire $7^{n+1} \equiv 1 \mod 6$. La propriété est donc héréditaire. Etant vraie pour $n = 0$ elle est vraie pour tout $n \geq 0$.

Définition (Classe de congruence) : Soient $a \in$ Z et $n \in$ N*. La *classe* de a mod n est l'ensemble

$$\begin{aligned}
\overline{a} &= \{b \in \mathbb{Z} \mid a \equiv b \mod n\} \\
&= \{b \in \mathbb{Z} \mid b \equiv a \mod n\} \\
&= \{b \in \mathbb{Z} \mid n|b - a\} \\
&= \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z}\ :\ b - a = kn\} \\
&= \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\} \subset \mathbb{Z}
\end{aligned}$$

On note Z/nZ = $\{\overline{a}, a \in$ Z$\}$ (on prononce Z sur nZ)

Exemple : Dans Z/4Z, on a

$\bar{1} = \{1, 1 + 1 \times 4 = 5, 1 + 2 \times 4 = 9, 1 + 3 \times 4 = 13, \dots, 1 - 1 \times 4 = -3, 1 - 2 \times 4 = -7, 1 - 3 \times 4 = -11, \dots\}$.

Lemme : *Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On* $\bar{a} = \bar{b} \iff a \in \bar{b} \iff b \in \bar{a} \iff a \equiv b \mod n$.

Démonstration. Notons (1),(2),(3),(4) les différentes assertions à démontrer.

(1 ⇒ 2) Si $\bar{a} = \bar{b}$, alors $a \in \bar{a}$ implique que $a \in \bar{b}$.

(2 ⇒ 3) $a \in \bar{b}$, donc a s'écrit sous la forme $b + kn$ pour un certain $k \in \mathbb{Z}$ On en déduit que $b = a - kn = a + (-k)n$. Donc $b \in \bar{a}$.

(3 ⇒ 4) $b \in \bar{a}$, donc $b = a + kn$ pour un certain $k \in \mathbb{Z}$. En particulier, $a - b = (-k)n$, c'est-à-dire $n | a - b$ et donc $a \equiv b \mod n$.

(4 ⇒ 1) On veut montrer que $\bar{a} = \bar{b}$. On procède par double inclusion.

Montrons pour commencer que $a \subset \bar{b}$. Soit $a + kn$ un élément de $\bar{a}$. Par hypothèse, $a \equiv b \mod n$. Donc $n | a - b$ et il existe $l \in \mathbb{Z}$ tel que $a - b = nl$ ou encore $a = b + nl$. Ainsi,

$$a + kn = b + nl + kn = b + (l + k)n \in \bar{b}.$$

On a donc bien montré que tout élément $a+kn$ de $\bar{a}$ appartient aussi à $\bar{b}$. Donc $\bar{a} \subset \bar{b}$. Comme $a \equiv b \mod n \iff b \equiv a \mod n$, on montre de manière symétrique qu'on a aussi $\bar{b} \subset \bar{a}$. D'où l'égalité.

Proposition : *Soit $a \in \mathbb{Z}$. Alors $a \equiv r \mod n$ où r est le reste de la division euclidienne de a par n. De plus, si $r \equiv r_0 \mod n$ avec $0 \le r < n$ et $0 \le r_0 < n$, alors $r = r_0$.*

Démonstration. Par le théorème concernant la division euclidienne, il existe un unique couple (q,r) d'entiers tels que $\begin{cases} a = nq + r \\ 0 \le r < n \end{cases}$. Donc $a - r = nq$, c'est-à-dire $n | a - r$, ou encore $a \equiv r \mod n$. Ceci montre la première partie de la proposition.

Si $0 \le r < n$ et $0 \le r_0 < n$, alors, $-n < r - r_0 < n$. Or

$$r \equiv r_0 \mod n \iff n \mid r - r_0 \iff r - r_0 = nk \text{ pour un certain entier } k.$$

Ainsi, $-n < nk < n$. Il s'ensuit que $nk = 0$ puis $k = 0$ (car $n \neq 0$). Donc $r - r_0 = 0$, c'est-à-dire $r = r_0$.

Exemple (Important : Puissance modulo un entier) : Quel est le reste de la division euclidienne par 13 de 100^{1000}?

Comme $100 = 7 \times 13 + 9$, $100 \equiv 9 \mod 13$. Par propriété (v) des congruences, $100^{1000} \equiv 9^{1000} \mod 13$. Or $9^2 \equiv 81 \equiv 3 \mod 13$ (car $81 = 13 \times 6 + 3$) et donc $9^3 \equiv 9 \times 9^2 \equiv 9 \times 3 \equiv 1 \mod 13$. Finalement,

$$100^{1000} \equiv 9^{1000} \equiv 9^{3*333+1} \equiv (9^3)^{333} \times 9 \equiv 1^{333} \times 9 \equiv 9 \mod 13.$$

Ainsi le reste de la division euclidienne de 100^{1000} par 13 est 9.

On obtient aussi le corollaire suivant :

Corollaire : *Si $a \in \mathbb{Z}$, il existe un unique $0 \le r < n$ tel que : $a \equiv r \mod n$. On en déduit que $\mathbb{Z}/n\mathbb{Z}$*

possède n éléments et $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

Exemple : (Dessin à faire) Pour $n = 4$, $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

De manière générale, on a toujours $\overline{n} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$. En effet, 0 est le reste dans la division euclidienne de n par n. De même, $\overline{n+1} = \overline{1}$, $\overline{n+2} = \overline{2}$, etc.

Définition (Somme et produit de classes) : On considère deux éléments $\overline{a}$ et $\overline{b}$ de $\mathbb{Z}/n\mathbb{Z}$. on définit la *somme* et le *produit* de a et b par

$$\overline{a} + \overline{b} := \overline{a+b}$$

$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$$ ou noté plus simplement ab.

Exemple : Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{5} + \overline{3} = \overline{5+3} = \overline{8} = \overline{2}$ et $\overline{5.2} = \overline{10} = \overline{4}$.

Proposition (Eléments neutres) : *Pour tout* $a \in \mathbb{Z}$, *on a* $\overline{a} + \overline{0} = \overline{a}$ *et* $\overline{a}.\overline{1} = \overline{a}$.

Remarque : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif, c'est-à-dire que toutes les propriétés de $\mathbb{Z}$ listées en début de chapitre (Proposition) restent valables pour $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sauf la dernière propriété concernant l'intégrité.

Exemple : Attention : si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas premier. Par exemple dans $\mathbb{Z}/6\mathbb{Z}$, on a

aussi $\overline{2} \times \overline{3} = \overline{6} = \overline{0}$.

Exemple (Table d'addition de Z/6Z) :

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Définition (Classe inversible) : Un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est dit *inversible* s'il existe $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$, appelé *inverse de* $\overline{a}$ tel que $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1}$.

Notation 1 : On note $\mathbb{Z}/n\mathbb{Z}^{\times}$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exemple : Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\overline{3} \times \overline{3} = \overline{3 * 3} = \overline{9} = \overline{1}$ car le reste de la division euclidienne de 9 par 4 est

1. Ainsi $\overline{3}$ est inversible et son inverse est lui-même : $\overline{3} \in \mathbb{Z}/4\mathbb{Z}^{\times}$.

Proposition : *Soit* $a \in \mathbb{Z}/n\mathbb{Z}$. *Si* a *est inversible, son inverse unique. On parle alors de l'inverse de* a *(au lieu de* un *inverse de* a*).*

Démonstration. Soient $\overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$ tels que $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = 1$ et $\overline{a} \cdot \overline{c} = \overline{c} \cdot \overline{a} = \overline{1}$. Alors

$$\bar{c} = \bar{c} \cdot \bar{1} = \bar{c} \cdot (\bar{a} \cdot \bar{b}) = (\bar{c} \cdot \bar{a}) \cdot \bar{b} = \bar{1} \cdot \bar{b} = \bar{b}.$$

Proposition (Caractérisation des éléments inversibles) : *Un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $pgcd(a,n) = 1$ (c'est-à-dire si et seulement si $\exists u \in \mathbb{Z}$, $au \equiv 1 \bmod n$).*

Démonstration. ($\Rightarrow$) On suppose $\bar{a}$ inversible. Donc il existe $\bar{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a} \cdot \bar{u} = \bar{1}$. Or

$$\begin{aligned} \bar{a} \cdot \bar{u} = \bar{1} &\iff \overline{au} = \bar{1} \\ &\iff \bar{1} - \overline{au} = \bar{0} \\ &\iff \overline{1 - au} = \bar{0}. \end{aligned}$$

Donc $1 - au$ est divisible par n :

$$\exists k \in \mathbb{Z} : \qquad 1 - au = nk$$

c'est-à-dire $au+nk = 1$. Dans ce cas, $d = pgcd(a,n) = 1$ d'après un corollaire du théorème de Bezout (dem : $d := pgcd(a,n)$, alors $d|a$ et $d|n$ donc $d|ab + nk = 1$ et finalement $d = 1$ (car $d > 0$)).

($\Leftarrow$) Si $pgcd(a,n) = 1$, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + nv = 1$; Donc

$$\begin{aligned} \overline{au + nv} = \bar{1} &\iff \overline{au} + \overline{nv} = \bar{1} \\ &\iff \bar{a} \cdot \bar{u} + \bar{n} \cdot \bar{v} = \bar{1} \\ &\iff \bar{a} \cdot \bar{u} + \bar{0} \cdot \bar{v} = \bar{1} \\ &\iff \bar{a} \cdot \bar{u} + \bar{0} = \bar{1} \\ &\iff \bar{a} \cdot \bar{u} = \bar{1} \end{aligned}$$

et $\bar{a}$ est bien inversible dans $\mathbb{Z}/n\mathbb{Z}$, d'inverse $\bar{u}$.

Méthode :

(1) Trouver un inverse de $\bar{a}$ dans $\mathbb{Z}/n\mathbb{Z}$ revient à calculer une relation de Bézout entre a et n.

(2) Si n est petit, il est aussi rapide de faire un tableau de congruence pour trouver (lorsqu'elle existe)

quelle classe $\bar{b}$ vérifie $\bar{a} \cdot \bar{b} = \bar{1}$.

Conséquence 1 : Si p est un nombre premier, tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles. On dit alors que $\mathbb{Z}/p\mathbb{Z}$ est un corps. En particulier, $\mathbb{Z}/p\mathbb{Z}$ est intègre.

2- Equation diophantiennes

Définition : On appelle équation diophantienne toute équation dont on recherche les solutions entières.

Soient a; b $\in \mathbb{Z}^*$ et c $\in \mathbb{Z}$. On considère l'équation suivante :

(1) ax + by = c , dont on recherche les solutions (x; y) $\in \mathbb{Z}$.

Lemme : Soient a; b ∈ $\mathbb{Z}^*$ et c∈ $\mathbb{Z}$. L'équation diophantienne ax+by = c admet au moins une solution si et seulement si pgcd(a; b)|c.

Démonstration. (⇒)) Si (1) a une solution (x_0; y_0) ∈ $\mathbb{Z}^2$, alors a x_0+b y_0= c. Or pgcd(a; b) divise a et b, donc a x_0+b y_0, donc c.

(⇐) Réciproquement, supposons que pgcd(a; b) divise c :

∃k ∈ $\mathbb{Z}$: c = k .pgcd(a; b):

D'après le théorème de Bezout, on a aussi

∃u; v ∈ $\mathbb{Z}$: au + bc = pgcd(a; b):

En multipliant cette dernière égalité par k, il vient

a(ku) + b(kv) = k. pgcd(a; b) = c:

Ainsi (ku; kv) est solution de (1).

Proposition : Soient a; b ∈ $\mathbb{Z}^*$et c ∈ $\mathbb{Z}$ tels que pgcd(a; b)|c. Soient $a' = \frac{a}{\text{pgc d(a;b)}}$ et $b' = \frac{b}{\text{pgc d(a;b)}}$.

Si $(x_0; y_0) \in \mathbb{Z}^2$est une solution de l'équation diophantienne ax + by = c, alors l'ensemble des solutions est

$$S = \{(x_0 + kb'{;}y_0 - ka') \in \mathbb{Z}^2, k \in \mathbb{Z}\}$$

Démonstration. Soient $(x, y) \in \mathbb{Z}^2$ une solution de (1). Alors

ax + by = c = ax_0 + by_0

⇔ ax + by = ax_0 + by_0

⇔ a(x- x_0) = b(y_0 - y)

⇔ a′ (x - x_0) = b′(y_0 - y) en divisant les deux membres par pgcd(a; b) $\neq 0$.

En particulier, a′ divise b′ (y_0 - y). Comme pgcd(a′ ; b′) = 1, le théorème de Gauss assure que a′ | y_0 - y ce qui signifie : ∃ k ∈ $\mathbb{Z}$: y_0 -y = k a′

ce qui équivaut à y = y_0 - k a′ . Il s'ensuit que

a′ (x - x_0) = b′ (k a′)

⇔ x - x_0 = kb′ car $a' \neq 0$

⇔x = x_0 + k b′ .

Inversement, on vérifie que tout couple$(x_0 + kb'{;}y_0 - ka')$ avec k ∈ $\mathbb{Z}$ est solution de (1). En effet, on a pour tout k ∈ $\mathbb{Z}$, $a(x_0 + kb') + b(y_0 - ka')$ = a x_0 +b y_0= c .

<u>Méthode de résolution de l'équation ax + by = c (1) :</u>

(1) On calcule pgcd(a; b). Si pgcd(a; b) ne divise pas c, l'équation n'admet pas de solution dans $\mathbb{Z}^2$. Sinon, il existe un entier k tel que c = k . pgcd(a; b) et on passe à l'étape 2.

(2) On détermine une relation de Bezout au + bv = pgcd(a; b).

(3) On multiplie cette égalité par k : a(ku) + b(kv) = c ; autrement dit (x_0; y_0)=(k u ;k v) est une solution particulière de (1)

(4) On déduit l'ensemble des solutions générales comme détaillé dans la preuve de la Proposition.

Equation diophantienne ax = b mod n.

Lemme : *Soient $a,b \in \mathbb{Z}$ et un entier $n \geq 2$. L'équation $ax \equiv b \bmod n$ admet une solution dans $\mathbb{Z}$ si et seulement si $pgcd(a,n)|b$.*

Démonstration. ($\Rightarrow$) Si $\exists x_0 \in \mathbb{Z}$ tel que $ax_0 \equiv b \bmod n$, alors

$$n|ax_0 - b$$
$$\Longleftrightarrow \quad \exists k \in \mathbb{Z} : ax_0 - b = kn$$
$$\Longleftrightarrow \quad \exists k \in \mathbb{Z} : ax_0 - kn = b.$$

Alors $pgcd(a,n)$ divise a et n, donc $ax_0 - kn = b$.

($\Leftarrow$) Par le théorème de Bezout, il existe $(u,v) \in \mathbb{Z}^2$: $au + nv = pgcd(a,n)$. D'autre part, $pgcd(a,n)|b$ par hypothèse :

$$\exists k \in \mathbb{Z} : \qquad b = k \cdot pgcd(a,n).$$

Si on multiplie la relation de Bezout ci-dessus par k, il vient

$$a(ku) + n(kv) = k \cdot pgcd(a,b) = b \Longleftrightarrow$$
$$a(ku) = b - n(kv).$$

D'où $a(ku) \equiv b \bmod n$. Alors $x_0 := ku$ est une solution particulière de l'équation $ax \equiv b \bmod n$.

Proposition : *Notons S l'ensemble des solutions de l'équation $ax \equiv b \bmod n$.*

(1) Si $pgcd(a,n)$ ne divise pas b, alors $S = \emptyset$.

(2) Sinon $pgcd(a,n)|b$. Posons $n' = \frac{n}{pgcd(a,n)}$. Soit $x_0 \in \mathbb{Z}$ est une solution particulière de l'équation $ax \equiv b \bmod n$. Alors

$$S = \{x_0 + k \in \mathbb{Z} \mid k \in \mathbb{Z}\}.$$

Démonstration.

$$\begin{aligned}
ax \equiv b \quad \bmod n \quad &\Longleftrightarrow \quad ax \equiv ax_0 \quad \bmod n \\
&\Longleftrightarrow \quad n|ax - ax_0 \\
&\Longleftrightarrow \quad n|a(x - x_0) \\
&\Longleftrightarrow \quad n'|a^0(x - x_0) \qquad \text{en divisant par } pgcd(a,n) \; 6{=}\; 0 \\
&\Longleftrightarrow \quad n'|x - x_0 \qquad \text{par le théorème de Gauss} \\
&\Longleftrightarrow \quad \exists k \in \mathbb{Z}, \qquad x - x_0 = kn'.
\end{aligned}$$

Exemple : Résoudre l'équation $24x \equiv 4 \bmod [10]$. Comme $24 = 2^3 \cdot 3$ et $10 = 2 \cdot 5$, $pgcd(24,10) = 2$ qui divise bien 4. Donc cette équation admet au moins une solution.

Commençons par chercher une solution particulière. On peut deviner que 1 est une solution évidente. Sinon, on cherche une relation de Bezout entre 24 et 10. On a par l'algorithme d'Euclide :

$$24 = 2 \times 10 + 4$$
$$10 = 2 \times 4 + 2$$
$$4 = 2 \times 2 + 0$$

Ainsi,

$$2 = 10 - 2 \times 4$$
$$= 10 - 2 \times (24 - 2 \times 10) =$$
$$24 \times (-2) + 10 \times 5.$$

Il s'ensuit que $24\times(-4)+10\times(10) = 4$ et donc que $24\times(-4) \equiv 4 \mod 10$. Donc $x_0 = -4$ est une solution particulière.

Cherchons la solution générale en reprenant la démarche de la proposition ci-dessus. Soit $x \in \mathbb{Z}$ solution. Ceci équivaut à

$$\begin{aligned} 24x \equiv 4 \mod 10 &\iff 24x \equiv 24x_0 \mod 10 \\ &\iff 10|24(x+4) \\ &\iff 5|12(x+4) \\ &\iff 5|x+4 \text{ par le théorème de Gauss} \\ &\iff \exists k \in \mathbb{Z} : x = -4 + 5k. \end{aligned}$$

L'ensemble des solutions de l'équation est donc

$$S = \{-4 + 5k \in \mathbb{Z} \mid k \in \mathbb{Z}\}.$$

3- Le petit théorème de Fermat

Définition (Coefficients binomiaux) : Soient $0 \leq k \leq n$ deux entiers. On définit le *coefficient binomial* comme étant l'entier

$$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!} \in \mathbb{N}.$$

où par définition pour un entier $p \in \mathbb{N}^*$, $p! = p(p-1)(p-2)\cdots 1$ et $0! = 1$.

Remarque 11 : On lit « k parmi n ». Il s'agit du nombre de manière de choisir k éléments parmi une liste de n éléments (sans tenir compte de l'ordre). On parle de k-combinaison.

Proposition :

$$\binom{n}{k} = \binom{n}{n-k} \qquad \binom{n}{0} = 1 \qquad \binom{n}{1} = n.$$

:

Proposition (Formule de Pascal) : $$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Démonstration. Première méthode (calcul direct) :

$$\begin{aligned} \binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} = \frac{n!(k+1)}{(k+1)k!(n-k)!} + \frac{n!(n-k)}{(k+1)!(n-k-1)!(n-k)} \\ &= \frac{n!(k+1+n-k)}{(k+1)!(n-k)} = \frac{n!(n+1)}{(k+1)!(n+1-k-1)!} = \frac{(n+1)!}{(k+1)!(n+1-(k+1))!} = \binom{n+1}{k+1}. \end{aligned}$$

Remarque (Triangle de Pascal) :

	$k = 0$	$k = 1$	$k = 2$...
$n = 0$	1		
$n = 1$	1	1	
$n = 2$	1	2	1

$n = 3$ 1 3 3 1

$n = 4$ 1 4 6 4 1...

Proposition (Formule du binôme de Newton) : *Soient x,y ∈ C. Alors pour tout n ∈ N*,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

Démonstration. Par récurrence sur n.

(1) Pour $n = 0$, $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0$.

(2) Supposons le résultat vrai au rang n. (3) Alors

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y)\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i \\ &= x^{n+1} + x\sum_{i=1}^{n}\binom{n}{i}x^{n-i}y^i + y\sum_{i=0}^{n-1}\binom{n}{i}x^{n-i}y^i + y^{n+1} \\ &= x^{n+1} + \sum_{i=1}^{n}\binom{n}{i}x^{n-i+1}y^i + \sum_{i=0}^{n-1}\binom{n}{i}x^{n-i}y^{i+1} + y^{n+1} \\ &= x^{n+1} + \sum_{i=1}^{n}\left[\binom{n}{i} + \binom{n}{i-1}\right]x^{n-i+1}y^i + y^{n+1} && \text{en réindexant et factorisant} \\ &= x^{n+1} + \sum_{i=1}^{n}\binom{n+1}{i}x^{n-i+1}y^i + y^{n+1} \\ &= \sum_{i=0}^{n+1}\binom{n+1}{i}x^{(n+1)-i}y^i && \text{par la formule de Pascal}\end{aligned}$$

D'où le résultat par principe de récurrence.

Exemple :

$(x + y)^2 = 1x^2 + 2xy + 1y^2$

$(x + y)^3 = 1x^3 + 3x^2y + 3xy^2 + 1y^3$

$(x + y)^4 = 1x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + 1y^3$...

Lemme : *Soit p un nombre premier. Si k est un entier tel que* $0 < k < p$*, alors p divise* $\binom{p}{k}$.

Démonstration. Soit k un entier entre $0 < k < p$. On a par définition des coefficients binomiaux :

$$p! = k!(p-k)!\binom{p}{k}.$$

Comme p divise $p!$, p divise aussi $k!(p-k)!\binom{p}{k}$ et puisque p est premier, le lemme d'Euclide assure que p divise l'un des entiers

$k!$ $(p - k)!$ $\binom{p}{k}$.

Or $k < p$ donc p ne divise pas $k!$ (toujours d'après Euclide : les facteurs premiers de $k!$ sont $\leq k$). De même puisque $0 < k$, alors $p-k < p$, donc p ne divise pas non plus $(p-k)!$. Ainsi, p divise nécessairement $\binom{p}{k}$. Théorème 7 (Petit théorème de Fermat) : *Soit p un nombre premier. Si x ∈ Z, alors on a* $x^p \equiv x \bmod p$.

Démonstration. Soit $x \in \mathbb{Z}$.

On commence par le cas $p = 2$. Alors, on a $x^2 - x = x(x-1)$. Donc $x^2 - x$ est le produit de deux entiers consécutifs, donc est pair. Il s'ensuit que $x^2 - x \equiv 0 \bmod 2$ et le résultat est vrai.

Dans le cas où p est premier > 2, p est impair et on montre par récurrence sur $x \in \mathbb{N}$ que $x^p \equiv x \bmod p$.

(1) Si $x = 0$, le résultat est vrai.

(2) Supposons que l'on a $x^p \equiv x \bmod p$.

(3) Alors par la formule du binôme de Newton,

$$(x+1)^p = x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + \binom{p}{k}x^{p-k} + \ldots + \binom{p}{p-1}x + 1.$$

Le lemme précédent montre que p divise $\binom{p}{k}$ pour $0 < k < p$. Autrement dit, $\binom{p}{k} \equiv 0 \mod p$ pour $0 < k < p$. Ainsi,

$$(x+1)^p \equiv x^p + 0 + \ldots + 0 + 1 \equiv x + 1 \qquad \bmod p.$$

Ainsi le théorème est montré pour tout $x \in \mathbb{N}$ par principe de récurrence.

Maintenant, si $x < 0$, alors $(-x)^p \equiv -x \bmod p$ (car $-x \geq 0$). Mais p étant impair, $(-x)^p = -x^p$ et en multipliant cette congruence par -1, on obtient également le résultat pour x négatif. Corollaire 7 : *Soit p un nombre premier. Si p ne divise pas x, alors* $x^{p-1} \equiv 1 \bmod p$.

Démonstration. Soit $x \in \mathbb{Z}$ tel que p ne divise pas x. Alors d'après le petit théorème de Fermat, $x^p - x \equiv 0 \bmod p$. Autrement dit, p divise $x^p - x = x(x^{p-1} - 1)$. Or p étant premier et ne divisant pas x, il est premier à x. Le théorème de Gauss montre que donc p divise $x^{p-1} - 1$, ce qui signifie que $x^{p-1} \equiv 1 \bmod p$.

Exemple :

Calculons $7^{241} \bmod 13$. Puisque 13 est un nombre premier et que 13 ne divise pas 7, on obtient $7^{12} \equiv 1 \bmod 13$. Comme 241 = 12 × 20 + 1, on en déduit que $7^{241} \equiv 7^{12\times 20+1} \equiv (7^{12})^{20} \times 7 \equiv 1^{20} \times 7 \equiv 7 \bmod 13$.