Structure Discrète
IFT1065
Devoir 2
Récursivité et Preuves

Franz Girardin et Aiya

17 novembre 2023

Table des matières

Résolution de problèmes

PROBLÈME 1 · DIVISIBILITÉ

1. Montrez que a divise b si et seulement si an divise bn. Reformulez la proposition en langage logique, puis écrivez sa preuve en explicitant chaque technique utilisée.

Soit le proposition $P(a,b,n)$: a divise b **si et seulement si** an divise bn, nous pouvons réécrire $P(a,b,n)$ en language logique de la façon suivante :

$$P(a,b,n) ::= a|b \Leftrightarrow an|bn$$

Nous savons qu'une telle proposition biconditionnelle est une synthèse de **propositions conditionnelles** distinctes que nous appellerons P_r et P_s :

$$P_q ::= a|b \implies an|bn \tag{1.1}$$
$$P_r ::= an|bn \implies a|b \tag{1.2}$$

Pour montrer la véracité de $P(a,b,c)$, nous allons donc montrer que P_q et P_r sont vrais.

Proposition 1.1 (P_q)

$$a|b \implies an|bn$$

Preuve (P_q)

Nous allons montrer P_q par *preuve directe*. Supposons que a divise b. **Par définition**, cela signifie qu'il existe un nombre $c \in \mathbb{Z}$ tel que $b = ac$. Et, trivialement, $bn = acn$ Nous avons alors :

$$\begin{aligned} an|bn &\equiv an|(ac)\cdot n \\ &\equiv an|(an)\cdot c \\ &\equiv an|an\cdot c \end{aligned}$$

Autrement dit, si an divise $(an)\cdot c$, cela veut dire qu'il existe un nombre $d \in \mathbb{Z}$ tel que $an\cdot d = an\cdot c$. D'une part, cela implique que $d = c$. Par ailleurs, nous constatons que bn est un multiple de an, car bn peut être exprimé comme an multiplié par un entier c. Par conséquent, nous concluons que an divise bn. □

Proposition 1.2 (P_r)

$$an|bn \implies a|b$$

Preuve (P_r)

Nous voulons prouver que si an divise bn, **alors** a divise forcément b (P_r). Nous allons montrer P_r par *preuve directe*. Supposons que an divise bn. **Par définition**, cela signifie qu'il existe un entier $k \in \mathbb{Z}$ tel que $an\cdot k = bn$. En divisant les deux côtés de l'équation par n, nous obtenons $b = ak$. **Or**, si nous substituons la valeur que nous venons de dériver de b, nous avons :

$$a|b \equiv a|ak$$

Cette équivalence tient, puisque toute division de ak par a implique de diviser b par a. Autrement dit, ak est une multiple de a ; on peut obtenir ak en multipliant a par un facteur k. Cela revient à dire que b est un multiple de a et donc, **par définition**, $a|b$ Par conséquent, nous concluons que si $an|bn$, alors $a|b$, puisque b est un multiple de a. □

Nous venons de montrer que la proposition P_q et sa réciproque P_r sont toutes deux vraies Par la définition d'une *proposition biconditionnelle*, nous concluons que la proposition :

$$an|bn \Leftrightarrow a|b$$

est vraie. Autrement dit, $P(a,b,n) ::=$ *an divise bn si et seulement si a divise b* est vraie. □

2. Montrez que si n ne divise pas ab, alors n ne divise ni a, ni b. Reformulez la proposition en langage logique, puis écrivez sa preuve en explicitant chaque technique utilisée.

Soit la proposition $P'(a,b,n)$: si n ne divise pas ab, alors n ne divise ni a, ni b. Nous pouvons réécrire $P'(a,b,n)$ en language logique de la façon suivante :

$$P'(a,b,n) ::= n \nmid ab \implies (n \nmid a) \wedge (n \nmid b)$$

Nous faisons face à une proposition conditionnelle où le côté droit de l'implication contient une conjonction.

Proposition 1.3 ($P'(a,b,n)$)

$$n \nmid ab \implies (n \nmid a) \wedge (n \nmid b)$$

Preuve

Nous voulons prouver que si un nombre n ne divise pas ab, alors ce nombre ne divise ni a ni b. Nous allons montrer $P'(a,b,n)$ par *contraposé*. Supposon la négation du côté droit de l'implication. Autrement dit, supposons :

$$\neg\left((n \nmid a) \wedge (n \nmid b)\right)$$

Par **De Morgan**, nous avons

$$\neg\left((n \nmid a) \wedge (n \nmid b)\right) \equiv \neg(n \nmid a) \vee \neg(n \nmid b)$$
$$\equiv (n|a) \vee (n|b)$$

Nous allons alors prouver que si $n|a$ **ou** $n|b$, alors, $n|ab$, soit la **contraposée** de $P'(a,b,n)$.

$$(n|a) \vee (n|b) \implies n|ab \tag{1.3}$$

Note :

Intuitivement, nous savons déjà que si on nombre n divise un nombre a ou un nombre b, ce nombre n divise nécessairement, le produit ab.

Preuve par cas.

Cas 1 : $n|a$ **Cas 2** $n|b$.
Sans perte de généralité, si $n|a$, **alors** il existe un entier $k \in \mathbb{Z}$ tel que $nk = a$. Donc, $ab = (nk) \cdot b$. Et pour diviser ab, il faut que n divise $n \cdot (kb)$; autrement dit, **pour que** n **divise** ab, **il suffit que que** n **divise** n, ce qui est toujours vrai pour tous $n \in \mathbb{Z}^*$.

$$n|ab \equiv n|(nk) \cdot b$$
$$\equiv n|n \cdot (kb)$$
$$\equiv n|nkb$$

Par conséquent, nkb est un multiple de n et nous concluons alors que n divise ab, puisque par substitutions n divise ab.

Ayant, indiqué que le **Cas 2** se traite de façon similaire au **Cas 1**, nous concluons que, dans les deux cas, n divise ab. Nous venons donc de prouver la contraposée de $P'(a,b,n)$. Puisque la contraposée de $P'(a,b,n)$ est vraie, il s'ensuit que $P'(a,b,n)$ est aussi vraie. Nous concluons alors que si un entier n ne divise pas un produit ab, alors cet entier n ne divise ni a ni b. □

3. Remarquez que la réciproque de (2.) n'est pas vraie. Donnez un contre-exemple.

La récirpoque de $P'(a,b,n)$, $Q'(a,b,n)$ peut être réécrite comme suit :

$$Q'(a,b,n) ::= (n \nmid a) \wedge (n \nmid b) \implies n \nmid ab$$

Et cela revient à affirmer que *si un nombre n ne divise pas un nombre a ni un nombre b, alors ce nombre n ne divise pas le produit ab*. Cette proposition est fausse.

Preuve

Nous allons prouver que la réciproque de $P'(a,b,n)$ est fausse par *contre-exemple*. Pour réfuter $Q'(a,b,n)$, nous allons montrer qu'il existe des entiers $a,b,n \in \mathbb{Z}$ tels que $n \nmid a$ et $n \nmid b$ et pourtant $n|ab$. Soit $n = 4$, $a = 2$, $b = 6$, et $ab = 12$. Nous savons que 4 ne divise pas 2. Nous savons également que 4 ne divise 6. Or, 4 divise 12. Nous avons donc un exemple de $a,b,n \in \mathbb{Z}$ qui contredit $Q'(a,b,n)$. Nous concluons que $Q'(a,b,n)$ est faux. □

4. Montrez que n divise a et b si et seulement si n divise pgcd(a ; b). Reformulez la proposition en langage logique, puis écrivez sa preuve en explicitant chaque technique utilisée.

Soit la proposition $P''(a,b,n)$: n divise a **et** b **si et seulement si** n divise $pgcd(a,b)$, nous pouvons réécrire $P''(a,b,n)$ en language logique de la façon suivante :

$$P''(a,b,n) ::= (n|a) \wedge (n|b) \Leftrightarrow n|pgcd(a,b)$$

Nous savons qu'une telle proposition biconditionnelle est une synthèse de **propositions conditionnelles** distinctes que nous appellerons P''_r et P''_s :

$$P''_q ::= (n|a) \wedge (n|b) \implies n|pgcd(a,b) \tag{1.4}$$
$$P''_r ::= n|pgcd(a,b) \implies (n|a) \wedge (n|b) \tag{1.5}$$

Pour montrer la véracité de $P''(a,b,c)$, nous allons donc montrer que P''_q et P''_r sont vrais.

Proposition 1.4 ($P''_q(a,b,n)$)

$$(n|a) \wedge (n|b) \implies n|pgcd(a,b)$$

Preuve

Nous voulons montrer que si n divise a et n divise b, **alors**, n divise le plus grand commun diviseur de a et b. Nous allons montrer $P''_q(a,b,n)$ par *preuve directe*.

Lemme 1

Le pgcd(a,b) est un multiple de n'importe quel diviseur commun de a et b.

Ce Lemme découle de la définition du pgcd, qui est le plus grand diviseur commun de a et b, impliquant qu'il est un multiple de tous les autres diviseurs communs.

Supposons que n divise a et n divise b. **Par définition**, n est un diviseur commun de a et b :

$$n ::= dc(a,b)$$

Or, si n est un diviseur commun de a et b, **il faut** que n divise le plus grand diviseur commun de a et b, par le

Lemme 1. En effet, si n est bien un diviseur commun de a et b, il y a deux cas possibles. Soit :

— n est l'unique diviseur commun de a et b et donc n est est le plus grand commun diviseur de a et b. **Par définition** :

$$n = pgcd(a, b)$$

— n n'est pas l'unique diviseur de a et b et il existe un pgcd(a,b), tel que

$$n \neq pgcd(a, b)$$

Dans le premier cas, on sait que n divise le $pgcd(a, b)$, par le **Lemme 1**. Dans le deuxième cas, on sait que n divise $pgcd(a, b)$ puisque n'importe quel nombre $n \in \mathbb{Z}^*$ peut se diviser lui-même.

Par conséquent, nous concluons que si n divise a et n divise b, alors n divise nécessairement le plus grand commun diviseur de a et b. □

Proposition 1.5 ($P''_r(a, b, n)$)

$$n|pgcd(a, b) \implies (n|a) \wedge (n|b)$$

Preuve

Nous voulons montrer que si n divise le plus grand commun diviseur de a et b **alors**, n divise a **et** n divise b. Nous allons montrer $P''_r(a, b, n)$ par *preuve directe*.

Supposons que n divise le plus grand commun diviseur de a et b. **Alors**, n est un facteur de $pgcd(a, b)$ et il existe un entier $k \in \mathbb{Z}$ tel que $nk = pgcd(a, b)$.

Or, s'il existe bien un nombre qui se trouve à être le plus grand commun diviseur de a et b, n est alors un facteur de a tout en étant un facteur de b. Autrement dit, il est possible d'obtenir a en multipliant $pgcd(a, b)$ par un entier $l \in \mathbb{Z}$ et il est possible d'obtenir b en multiple $pgcd(a, b)$ par un eniter $m \in \mathbb{Z}$.

Similairement, il est possible d'obtenir a en multipliant n par kl et il est possible d'obtenir b en multiplant n par km :

$$a = pgcd(a, b) \cdot l = nkl$$
$$b = pgcd(a, b) \cdot m = nkm$$

Par définition, n est donc un facteur de a tout en étant un facteur de b. Ainsi, n divise a et n divise b. Nous concluons que si n divise $pgcd(a, b)$ n divise également a et b.

Nous venons de montrer que la proposition $P''_q(a, b, n)$ et sa récriproche $P''_q(a, b, n)$ sont toutes deux vraies. Par la définition d'une *proposition biconditionnelle*, nous concluons que la proposition :

$$n|pgcd(a, b) \Leftrightarrow (n|a) \wedge (n|b)$$

est vraie. Autrement dit, $P''(a, b, n)$ ::= *n divise le plus grand commun diviseur de a et b si et seulement si n divise a et n divise b* est vraie.

5. Montrez que $pgcd(an; bn) = n \times pgcd(a; b)$. Reformulez la proposition en langage logique, puis écrivez sa preuve en explicitant chaque technique utilisée. (Indice : Montrez que $n \times pgcd(a; b)$ divise $pgcd(an; bn)$. Qu'en déduisez-vous ?)

Soit la proposition $P(a, b, n, d, d')$: $pgcd(an, bn) = n \times pgcd(a, b)$, nous pouvons réécrire $P(a, b, n, d, d')$ en language logique de la façon suivante :

$$P(a, b, n, d') ::= \left(d' = pgcd(an, bn)\right) \implies \left(d = n \times pgcd(a, b)\right),$$
$$a, b, n, d' \in \mathbb{Z}$$

Nous allons procéder en montrant que le nombre d' divise $n \times pgcd(a, b)$ et que $n \times pgcd(a, b)$ divise le nombre d', ce qui montre que les deux expressions sont égales. Nous commençons par prouver le Lemme suivant.

Lemme 2

Si $a|b$ et $b|a$, **alors**, $a = b$ ou $a = -b$, pour tout $a, b \in \mathbb{Z}$

Preuve

Nous procédons par *preuve directe*. Supposons que $a|b$ et $b|a$. Alors, il existe des entiers k et $l \in \mathbb{Z}$ tels que $ak = b$ et $bl = a$. Donc nous avons :

$$\begin{aligned} a &= bl \\ &= (ak) \cdot l \\ &= akl \end{aligned}$$

Et donc, nous avons également :

$$\begin{aligned} a - akl &= 0 \\ a(1 - kl) &= 0 \\ 1 - kl &= 0 \\ 1 &= kl \end{aligned}$$

Sachant que k et l appartiennent à $\mathbb{Z}$, les seuls nombres qui satisfont la dernière égalité est $k = l = 1$ ou $k = l = -1$.

— Si $k = l = 1$, $a = bl = b \cdot 1 = b$. Et $b = ak = a \cdot 1 = a$

— Si $k = l = -1$, $a = bl = b \cdot -1 = -b$. Et $b = ak = a \cdot -1 = -a$

Donc, nous concluons que si $a|b$ et $b|a$, il s'ensuit que $a = b$ ou $a = -b$. □

Le corollaire de ce lemme est que si nous considérons uniquement des entiers $a, b, k, l \in \mathbb{N}$, $a|b$ et $b|a$ implique que $a = b$. Par ailleurs, nous pouvons faire ce saut logique, puisque le problème implique la notion de pgdc qui, par définition, est un entier positif.

Lemme 3

Si $a|b$ et $b|a$, **alors**, $a = b$, pour tous $a, b \in \mathbb{N}$

Avant de montrer $P(a, b, n, d')$, nous introduisons un autre Lemme qui nous permettra de résoudre le problème.

Lemme 4

Si $a|c$ et $b|c$ et $pgcd(a, b)$, **alors**, $ab|c$

Preuve

Supposons que $a|c$ et $b|c$ et $pgcd(a, b) = 1$. Alors, il existe des entiers k et l formant une combinaison linéaire de a et b égale à 1 ; $ak + bl = 1$ (Conséquence du **Théorème de Bézout**). **Par conséquent** $cak + cbl = c$:

$$\begin{aligned} ak + bl &= 1 \\ c(ak + bl) &= 1 \cdot c \\ cak + cbl &= c \end{aligned}$$

Par ailleurs, puisque $a|c$ et $b|c$, doit exister des entiers m et $p \in \mathbb{Z}$ tels que $c = ma$ et $c = pb$. Nous avons donc $(pb)ak + (ma)bl = c$:

$$\begin{aligned} (pb)ak + (ma)bl &= c \\ pbak + mabl &= c \\ ab(pb) + ab(ml) &= c \\ ab(pb + ml) &= c \end{aligned} \tag{1.6}$$

Puisque ab divise le côté gauche de l'équation (1.6) ($ab|ab(pb + ml)$), ab divise nécessairement le côté droit de l'équation, c'est-à-dire c. Nous venons de montrer que si $a|c$ et $b|c$ et $pgcd(a, b) = 1$, **alors** $ab|c$. □

Nous avons prouvé le **Lemme 4** en supposant que $pgcd(a, b) = 1$. Cependant, même si le $pgcd$ de a et b n'est pas 1, nous pouvons toujours trouver un entier n tel que $abn = c$, car c est une multiple de a et b. Donc si $a|c$ et $b|c$, même si $pgcd(a, b) \neq 1$, ab divisera c.

Lemme 5

Si $a|c$ et $b|c$, **alors**, $ab|c$

Proposition 1.6 ($P_q(a, b, n, d')$)

$$d' = pgcd(an, bn) \implies d' \textbf{ divise } n \times pgcd(a, b), \quad a, b, n, d' \in \mathbb{N}$$

Preuve

Nous procédons par *preuve directe*. Supposons que d' est le plus grand commun diviseur de an et bn, pour an et $bn \in \mathbb{N}$; $d' = pgcd(an, bn)$. Et soit $d = pgcd(a, b)$ Alors, nous savons que d' divise toutes les **combinaisons linéaires** de an et bn, **par la définition d'un** $pgcd$. Si d est effectivement le $pgcd(a, b)$, alors d est une combinaison linéaire de a et b, par le théorème de Bézout. Autrement dit, $d = ax + by = pgcd(a, b)$. En multipliant cette combinaison linéaire (d) par n, on obtient l'équation $nd = n \times pgcd(a, b) = n(ax + by)$ Et on peut l'expandre en $nd = nax + nbx$. Cette dernière équation est simplement une combinaison linéaire de an et bn.

$$\begin{aligned} d = pgcd(a, b) &= ax + by && \text{(Bézout)} \\ n \times d &= n(ax + by) \\ n \times d &= nax + nby \\ n \times d &= (an)x + (bn)y \end{aligned}$$

Puisque d' divise toutes les combinaisons linéaire de an et bn et que nd est peut être reformulé en combinaison linéaire de an et bn, nous concluons que d' divise nd. Autrement dit, $pgcd(an, bn)$ divise $n \times pgcd(a, b)$

Proposition 1.7 ($P_r(a, b, n, d')$)

$$d = n \times pgcd(a, b) \implies \textbf{divise } pgcd(an, bn), \quad a, b, n, d \in \mathbb{N}$$

Preuve

Nous procédons par *preuve directe*. Supposons que d est le plus grand commun diviseur de a et b, pour a et $b \in \mathbb{N}$. Et soit $d' = pgcd(an, bn)$. Alors, d' est une combinaison linéaire de an et bn. et nous pouvons exprimer d' comme suit $d = anx + bny$ ou $n(ax + by)$. Aisi, nous savons que n divise $d' = n(ax + by)$.

Prouvons maintenant que d divise d'. Par définition, d divise toutes les combinaisons linéaire de a et b. Donc, d divise un combinaison linéaire telle que $ax + by$. En multipliant cette combinaison linéaire par n, on obtient $a(nx) + b(nx)$, ce qui est aussi une combinaison linéaire de a et b. Or, nous avons dit que d' peut être reformulé

en $n(ax+by) = a(nx) + b(nx)$, qui est toujours une combinaison linéaire de a et b. Ainsi, nous concluons que d divise d'.

Nous avons montré que n divise d' et que d divise d'. Par le **Lemme 5**, le produit nd divise donc d'. □

En montrant, $P_q(a,b,n,d')$ et $P_r(a,b,n,d')$, nous avons montré que $pgcd(an,bn)$ divise $n \times pgcd(a,b)$ et que $n \times pgcd(a,b)$ divise $pgcd(an,bn)$. Par le **Lemme 3**, nous concluons donc que $P(a,b,n,d')$ tient. Autrement dit :

$$pgcd(an,bn) = n \times pgcd(a,b)$$

parce que

— $pgcd(an,bn)$ **divise** $n \times pgcd(a,n)$ **et**

— $n \times pgcd(a,n)$ **divise** $pgcd(an,bn)$

□

PROBLÈME 1 · SIERPASKAL

1. Rappelez la définition récursive de $\binom{i}{j}$.

$$\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 5 & & 10 & & 10 & & 5 & & 1 &
\end{array}$$

FIGURE 1.1 – Triangle de Pascal

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5}
\end{array}$$

FIGURE 1.2 – Représentation du Triangle de Pascal

Concept.
En observant le Triangle de Pascal, on observe deux **cas extrêmes**. Le premier cas est lorsque $\binom{n}{k}$ est tel que $\binom{n}{0}$; Il s'agit de chacune des premières entrées du triangle à la rangée n (considérant qu'il existe une rangée 0). Le Le second cas est lorsque $\binom{n}{k}$ est tel que $\binom{n}{n}$ et donc $k = n$. Il s'agit de chacune des dernières entrées du triangle à la rangé n.

Note :
Par définition, $\binom{n}{0}$ est **le nombre** de sous-ensemble de longueur 0 il est possible de former en sélectionnant 0 élément d'un ensemble de longueur n. Dans ces conditions, **on peut seulement former l'ensemble vide**, $\emptyset$, et ce **nombre** est donc 1. Par ailleurs, $\binom{n}{n}$ est le **nombre** de sous-ensemble de longueur n il est possible d'obtenir en sélectionnant n éléments d'un ensemble de n éléments. **Le seul sous-ensemble possible selon ses conditions** est l'ensemble original de n élément, et le nombre $\binom{n}{n}$ est donc égale à 1.

Nous postulons alors que les **cas extrêmes** du triangle de Pascal sont de bon candidat pour des **cas de base** d'une définition récursive. Considérons alors la définition partielle suivante.

Définition 1 Cas de base de $C(n,k)$
$\binom{n}{k} ::= \binom{n}{0} = 1$ **et** $\binom{n}{n} = 1$

D'après le triangle de Pascal, nous savons que chaque entré à la rangée n est égal à l'entrée à la somme de la $k-1$-*ième* entrée à la rangé $n-1$ et de la k-*ième* entrée à la rangée $n-1$. Autrement, dit

Définition 2 Cas constructeur $C(n,k)$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, k \neq n, k \neq 0$$

Définition 1.1

Le nombre $C(n,k)$ est défini comme suit :

$$C(n,k) ::= \begin{cases} 1 & \text{si } k = 0 \textbf{ ou} \\ & \text{si } k = n, \\ C(n-1,k-1) + C(n-1,k) & \text{si } 0 < k < n. \end{cases}$$

1. Montrez que pour tous naturels n et m et tout entier k,
$\sum_{j=0}^{k} \binom{m}{k-j} \binom{n}{j} = \binom{m+n}{k}$.
Commencez par reformuler la proposition en langage logique. Faites-en ensuite une preuve par induction mathématique sur la valeur de n.

Nous devons prouver la prosition suivante :

Proposition 1.8 $(P(j,k,m,n))$

$$\forall n, m \in \mathbb{N}, k \in \mathbb{Z},$$
$$\sum_{j=0}^{k} \binom{m}{k-j} \binom{n}{j} = \binom{m+n}{k}$$

Preuve

Nous allons montrer $P(j,k,m,n)$ par *induction mathématique*.

Notre preuve par induction commencer en vérifiant la validité de la proposition pour une valeur de base de n. Nous expliquons pourquoi n (plutôt que j ou k ou m) limite le cas de base.

Cas de base (n = 0)

Lorsque $n = 0$, la somme $\sum_{j=0}^{k} \binom{m}{k-j}\binom{0}{j}$ présente trois scénarios.

1. *Si* $j > 0$,

alors la somme devient simplement

$$\sum_{j=0}^{k} R \times \binom{0}{j} = \sum_{j=0}^{k} R \times 0 = 0$$

puisque le nombre le nombre de sous-ensemble de longeur $j > 0$ il est possible d'obtenir en sélectionnant $j > 0$ éléments d'un ensemble de 0 élément est 0. En considérant les termes de gauches et les termes de droite de la proposition, nous avons :

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{0}{j} = 0 = \binom{m+0}{k}$$

Puisque le terme de gauche de la proposition $P(j,k,m,n)$ est égal à zéro, le terme de droite doit nécessairement être égal à zéro, et la proposition tient donc pour le cas de base $n = 0$ pour tout $j > 0$.

2. *Si* $j = 0$,

alors la somme devient simplement

$$\sum_{j=0}^{k} \binom{m}{k-0} \times \binom{0}{0} = \sum_{j=0}^{k} \binom{m}{k} \times 1$$

puisque le nombre le nombre de sous-ensemble de longeur $j = 0$ il est possible d'obtenir en sélectionnant $j = 0$ éléments d'un ensemble de 0 élément est 0. En considérant les termes de gauches et les termes de droite de la proposition, nous avons :

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{0}{0} = \binom{m+0}{k} \times 1 = \binom{m+n}{k}$$

la proposition tient donc pour le cas de base $n = 0$ lorsque $j = 0$.

3. *Si* $j < 0$,

alors, similairement au cas 1, la somme est égale à 0 puisque le nombre le nombre de sous-ensemble de longeur **négative** $j < 0$ il est possible d'obtenir en sélectionnant $j < 0$ éléments d'un ensemble de 0 élément est 0.

Note :

Par définition, un ensemble ne peut pas être de cardinal négatif et le plus petit ensemble possible est l'ensemble vide, $\emptyset$.

Puisque le côté gauche de la proposition (la sommation) est zéro le côté droit de la proposition doit nécessairement être zéro et le proposition tient donc pour les cas de base $n = 0$ et pour tout $j \leq 0$.

Note :

Nous aurions pu omettre de montrer que la proposition tient pour le cas de base $n = 0$ et les $j < 0$, puisque la sommation débute à $j = 0$.

Nous venons de montrer que le cas de base est $n = 0$ Peu importe la valeur du paramètre j de la sommation, l'égalité donné par $P(j,k,m,n)$ tient pour le cas de base $n = 0$.

Hypothèse d'induction

Supposons que $\sum_{j=0}^{k} \binom{m}{k-j}\binom{n}{j} = \binom{m+n}{k}$ est vrai pour un certain entier naturel n. Nous devons prouver que le fait que la proposition tient pour n implique que la proposition tient pour $n+1$.

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{n}{j} = \binom{m+n}{k} \implies \sum_{j=0}^{k} \binom{m}{k-j}\binom{n+1}{j} = \binom{m+n+1}{k}$$

Cas n+1

Nous devons montrer que l'égalité suivante est vraie (en supposant qu'elle est vraie pour n)

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{n+1}{j} = \binom{m+n+1}{k} \tag{1.7}$$

Selon le Triangle de Pascal (§Hammack 4.6),

$$\binom{n+1}{j} = \binom{n}{j-1} + \binom{n}{j} \tag{1.8}$$

Nous pouvons donc réécrire la sommation de (1.7) comme suit :

$$\sum_{j=0}^{k} \binom{m}{k-j} \times \left(\binom{n}{j-1} + \binom{n}{j}\right)$$

En calculant le produit, nous pouvons séparer l'équation en deux sommations :

$$\sum_{j=0}^{k} \binom{m}{k-j} \times \binom{n}{j-1} \quad + \quad \sum_{j=0}^{k} \binom{m}{k-j} \times \binom{n}{j} \tag{1.9}$$

Par l'hypothèse inductive, la seconde expression de (1.9), $\sum_{j=0}^{k} \binom{m}{k-j} \times \binom{n}{j}$, est simplement $\binom{m+n}{k}$. Nous avons donc

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{n}{j-1} \quad + \quad \binom{m+n}{k} \tag{1.10}$$

Nous allons maintenant reformuler la première expression de (1.9). Notons d'abord que $j = 0$, la somme partielle de (1.9) est 0 puisque :

$$\begin{aligned}\binom{m}{k-j}\binom{n}{0-1} &= \binom{m}{k-j}\binom{n}{-1} \\ &= \binom{m}{k-j} \times 0 \\ &= 0\end{aligned}$$

Par conséquent, nous pouvons commencer la sommation à l'index $j = 1$ puisque l'index $j = 0$ ne contribue pas à la somme.

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{n}{j-1}$$
$$\Updownarrow$$
$$\sum_{j=1}^{k} \binom{m}{k-j}\binom{n}{j-1}$$

Considérons un entier $i \in \mathbb{N}, i = j-1$. Nous allons présenter une sommation équivalente en utilisant i. Puisque lorsque $j = 1, i = j-1 = 0$. Et lorsque $j = k, i = j-1 = j-k$. Nous avons donc la sommation suivante.

$$\sum_{j=1}^{k} \binom{m}{k-j}\binom{n}{j-1}$$
$$\Updownarrow$$
$$\sum_{i=0}^{k-1} \binom{m}{k-(i-1)}\binom{n}{(i+1)-1}$$
$$\Updownarrow$$
$$\sum_{i=0}^{k-1} \binom{m}{(k-1)-i}\binom{n}{i}$$

Cette dernière équation a la même forme que l'hypothèse d'induction avec $k-1$ plutôt que k. Par l'hypothèse d'induction, nous pouvons donc déduire :

$$\sum_{i=0}^{k-1} \binom{m}{(k-1)-i}\binom{n}{i} = \binom{m+n}{k-1} \tag{1.11}$$

En combinant (1.7), (1.10). (1.11), nous avons :

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{n+1}{j} = \binom{m+n}{n-k} + \binom{m+n}{k} \tag{1.12}$$

Selon le Triangle de Pascal, nous avons alors $\sum_{j=0}^{k} \binom{m}{k-j}\binom{n+1}{j} = \binom{m+n}{n-k} + \binom{m+n}{k} = \binom{m+n+1}{k}$ Nous venons donc de montrer que la proposition tient également pour le cas $n+1$ Ainsi, par induction mathématique, nous concluons que $P(j,k,m,n)$ est vraie. Autrement dit, pour tout naturels n, m et tout entier m, l'égalité

$$\sum_{j=0}^{k} \binom{m}{k-j}\binom{n}{j} = \binom{m+n}{k}$$

est vraie. □

1. Démontrez, en utilisant l'identité de la question (2.), que pour tous naturels k et i et tout entier j,

$$P(i,j) = P(2^k + i, j) = P(2^k + i, 2^k + j)$$

Nous allons d'abord reformuler l'identité pour l'exprimer en termes de variables adaptées pour la démonstration qui suit. Pour tout naturel $i = m, 2^k = n, j = k$,

$$\sum_{r=0}^{j} \binom{i}{j-r}\binom{2^k}{r} = \binom{i+2^k}{j} \tag{1.13}$$

Nous avons deux égalités à prouver. Nous allons les prouver une à la fois. Considérons la proposition suivante.

Proposition 1.9 (P)

$$P(i,j) = P(2^k + i, j)$$

Preuve

Nous devons montrer que l'égalité donnée par P tient. Nous allons procéder par *preuve directe*.

Supposons que l'égalité de la proposition (1.9) est vraie. Le terme de droite de P peut être réécrit comme suit, en utilisant la version adapté de l'identité (équation 1.13) :

$$\begin{aligned} P(2^k + i, j) &= P(i + 2^k, j) && \text{Inversion de l'ordre} \\ &= \binom{i+2^k}{j} \bmod 2 && \text{Def. de P(i, j)} \\ &= \left(\sum_{r=0}^{j} \binom{i}{j-r}\binom{2^k}{r}\right) \bmod 2 && \text{Selon (1.13)} \end{aligned}$$

On a donc à prouver que

$$P(i,j) = \sum_{r=0}^{j} \binom{i}{j-r}\binom{2^k}{r} \bmod 2$$

Commençons par observer que si un nombre c divise une nombre a ou c divise un nombre b, alors c divise nécessairement le produit ab

Lemme 6

$$(c|a) \vee (c|b) \implies c|ab$$

Montrons que le Lemme 6 est vrai avec une *Preuve par cas*. Supposons que la prémisse du Lemme 6 est vraie. Nous faisons alors face aux deux cas suivants.

Cas $c|a$

Dans ce cas, il existe un $r \in \mathbb{Z}$ tel que $a = rc$ et affirmer que $c|ab$ revient à affirmer que $c|(rc)b$. Or, puisque ab est manifestement un multiple de c (sachant que $ab = (rc)b = c(rb)$), il s'ensuit que c divise ab.

Cas $c|b$

Sans perte de généralité, on peut montrer avec un raisonnement similaire au premier cas que $c|ab$ lorsque $c|b$.

Dans les deux cas, $c|ab$, et nous avons montré que si $c|a$ ou $c|b$, alors c divise nécessairement ab Nous concluons alors que le Lemme 6 est vrai. □

Un **corollaire** du **Lemme 6** est que si 2 divise une des expressions $a = \binom{i}{j-r}$ ou $b = \binom{2^k}{j}$ de la sommation $\sum_{r=0}^{j}\binom{i}{j-r}\binom{2^k}{j}$ pour toutes les valeurs possible de r, alors 2 divise le produit ab de cette sommation.

Investigation de $\sum_{r=0}^{j}\binom{i}{j-r}\binom{2^k}{j}$

Pour toutes les valeurs de r, sauf $r = 0$, le coefficient binomial $\binom{2^k}{r}$ sera un multiple de 2. Par conséquent le coefficient $\binom{2^k}{j}$ sera divisible par 2 et, par le **Lemme 6** le produit, $\binom{i}{j-r}\binom{2^k}{j}$ sera divisible par 2. Donc, pour tous les termes $r > 0$ de la sommation, leur contribution au modulo 2 sera nulle
Lorsque $r = 0$ on a alors $\binom{2^k}{0}$ et ce nombre est toujours un, peu importe la valeur de k. L'expression de sommation devient alors

$$\sum_{r=0}^{r=0} \binom{i}{j-0}\binom{2^k}{0} = \binom{i}{j} \times 1 = \binom{i}{j} \tag{1.14}$$

Nous venons de montrer que lorsque $r = 0$, nous avons la sommation :

$$\left(\sum_{r=0}^{r=0} \binom{i}{j-r}\binom{2^k}{r}\right) \bmod 2 = \binom{i}{j} \bmod 2$$

Nous venons de montrer que pour toutes autres valeurs de r, nous avons la sommation :

$$\left(\sum_{r=1}^{j} \binom{i}{j-r}\binom{2^k}{r}\right) \bmod 2 = 0$$

Or,

$$\left(\sum_{r=0}^{j}\binom{i}{j-r}\binom{2^k}{r}\right) \bmod 2 = \sum_{r=0}^{r=0}\binom{i}{j-0}\binom{2^k}{0} \bmod 2 + \sum_{r=1}^{j}\binom{i}{j-r}\binom{2^k}{r} \bmod 2$$

$$= \binom{i}{j} \bmod 2 + 0$$

$$= \binom{i}{j} \bmod 2$$

Par définition, $= P(i,j)$

Ainsi, la proposition (1.9) est vraie; $P(i,j) = P(2^k + i, j) = \binom{i}{j} \bmod 2$ □

Nous continuous la preuve en montrant que la seconde proposition est également vraie. Considérez la proposition suivante

Proposition 1.10 (Q)

$$P(i,j) = P(2^k + i, 2^k + j)$$

Preuve

Nous devons montrer que l'égalité donnée par Q tient. Nous allons procéder par *preuve directe*.

Supposons que l'égalité de la proposition (1.10) est vraie. Le terme de droite de Q peut être réécrit comme suit, en utilisant la version adapté de l'identité (équation 1.13) :

$$P(2^k + i, 2^k + j) = P(i + 2^k, j + 2^k) \quad \text{Inversion de l'ordre}$$

$$= \binom{i + 2^k}{j + 2^k} \bmod 2 \quad \text{Def. de P(i, j)}$$

$$= \left(\sum_{r=0}^{j+2^k}\binom{i}{(j+2^k)-r}\binom{2^k}{r}\right) \bmod 2$$

Investigation de $\sum_{r=0}^{j+2^k}\binom{i}{j+2^k-r}\binom{2^k}{j}$

Pour toutes les valeurs de r y compris $r = j$, et sauf $r = 2^k$, le coefficient binomial $\binom{2^k}{r}$ sera divisible par 2 et donc les $r \neq 2^k$ derniers termes de la sommation auront une contribution nulle au modulo 2.
Lorsque $r = 2^k$, on a alors $\binom{2^k}{2^k}$ pour l'une des expression de la sommation et nous pouvons la simplifier comme suit :

$$\sum_{r=0}^{r=2^k}\binom{i}{j+2^k-2^k}\binom{2^k}{2^k} = \binom{i}{j} \times 1 = \binom{i}{j} \qquad (1.15)$$

Or,

$$\left(\sum_{r=0}^{j+2^k}\binom{i}{j+2^k-r}\binom{2^k}{r}\right) \bmod 2 = \sum_{r=0}^{r=j-1}\binom{i}{j+2^k-r}\binom{2^k}{r} \bmod 2 + \binom{i}{j+2^k-j}\binom{2^k}{j} \bmod 2 + \sum_{r=j+1}^{2^k-1}\binom{i}{j-r}\binom{2^k}{r} \bmod 2 + \binom{i}{j+2^k-2^k}\binom{2^k}{2^k} \bmod 2$$

$$= 0 + 0 + 0 + \binom{i}{j} \bmod 2$$

$$= \binom{i}{j} \bmod 2$$

Par définition, $= P(i,j)$

Ainsi, la porposition (1.10) est vraie; $P(i,j) = P(2^k + i, 2^k + j) = \binom{i}{j} \bmod 2$

En conclusion, les proposition 1.9 et 1.10 sont toutes deux vrais. Par conséquent, nous pouvons affirmer que l'identité est bien valide :

$$P(i,j) = \sum_{r=0}^{j}\binom{i}{j-r}\binom{2^k}{r} \bmod 2$$

□

1. Utilisez ce résultat pour expliquer la similarité observée entre le triangle de Sierpiński et le *triangle de Pascal modulo 2*.

Concept.

Dans le triangle de Pascal, chaque nombre est le résultat de la somme de deux nombres situés exactement au-dessus (*Figure 1.1*). Lorsqu'on calcule les coefficients binomiaux du triangle de Pascal modulo 2, on obtient des valeurs de 0 ou 1, puisque chaque nombre découlant d'un coefficient est soit pair ou impair, et donc chaque nombre découlant d'un coefficient est divisible par 2 ou

engendre un reste de 1 lorsqu'on le divise par deux.

La preuve que nous venons de compléter a montré que pour tout naturel i, 2^k, et j, le coefficient binomial $\binom{i+2^k}{j}$ mod 2 a les mêmes propriétés de divisibilité que $\binom{i}{j}$ mod 2. Autrement dit,

— **Égalité 1** Proposition (1.9)
Chaque nombre à la ligne i et la colonne j du *triangle de Pascal modulo 2* a une valeur équivalente au nombre présent à la ligne $i + 2^k$ et le colonne j.

— **Égalité 2** Proposition (1.10)
Chaque nombre à la ligne i et la colonne j du *triangle de Pascal modulo 2* a une valeur équivalente au nombre présent à la ligne $i + 2^k$ et la colonne $j + 2^k$

Dans le *triangle de Pascal modulo 2*, on peut conceptualiser chaque entrée `1` comme étant un **triangle plein** et chaque entrée `0` comme étant un triangle vide formant un approximation de Sierpinski. Par ailleurs, si une ligne i est elle que $2|i + 1$ il existe un *triangle complètement simétrique* de heuteur $i + 1$ composés de triangle pleins et de triangle vides.

Par exemple, la **ligne 3** est du *triangle de Pascal modulo 2* est telle que $2|3 + 1$. Et si on plaçait lest triangle de façon à former un *triangle complètement simétrique*, on obtiendrait un triangle de hauteur 4, une approximation du triangle de Sirpinski :

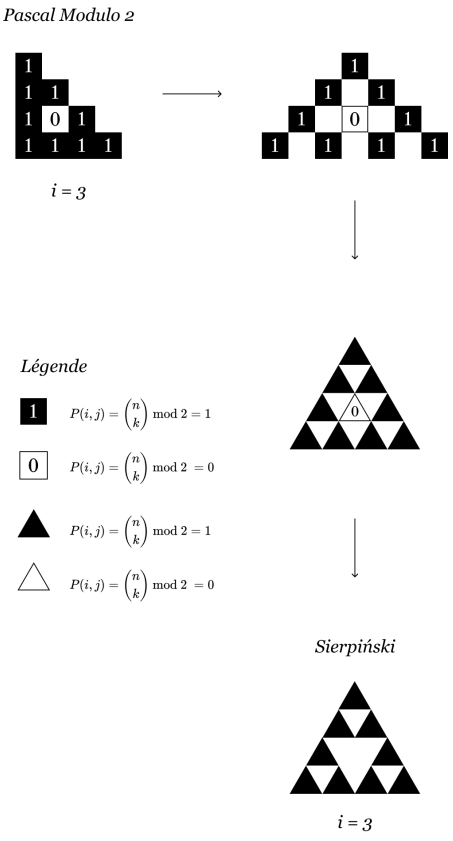

FIGURE 1.3 – Approximation de Sierpinski à partir de Pascal modulo 2

Cette propriété reflète la répétition et l'auto-similarité dans le triangle de Pascal modulo 2, qui sont des caractéristiques clés du triangle de Sierpiński.

On peut conceptualiser le triangle de Sierpinski comme étant un triangle récursif composé de triangles pleins et de triangle vide. Par ailleurs, en commeçant par la ligne 0, si une ligne i est telle que $2|i + 1$ il existe un *triangle complètement simétrique* de heuteur $i + 1$ composés de triangle pleins et de triangle vides. L'identité que nous avons prouvé suggère que chaque triangle à une position (i, j) aura la même propriété (plein ou vide) qu'un triangle situé à la position $(i + 2^k, j)$, où i et j représentent les lignes et les colonnes du triangle de Sierpinski, respectivement. De plus, par l'égalité de la proposition (1.10) que nous avons prouvé, un triangle situé à la position (i, j) aura la même propriété qu'un triangle situé à la position $(i + 2^k, j + 2^k)$.