

Structure Discrète
IFT1065
Devoir 2
Récursivité et Preuves

Franz Girardin et Aiya

14 novembre 2023

Table des matières

2 | CHAPITRE 1 Résolution de problèmes

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 la proposition $P(a, b, n) : a \text{ divise } b \text{ si et seulement si } an \text{ divise } bn$, nous pouvons réécrire $P(a, b, n)$ en langage 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_q et P_r :

$$P_q ::= a|b \implies an|bn \quad (1.1)$$

$$P_r ::= an|bn \implies a|b \quad (1.2)$$

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 . \square

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 un 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 . \square

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, $P(a, b, n) ::= an \text{ divise } bn \text{ si et seulement si } a \text{ divise } b$ est vraie. \square

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 $P'(a, b, n) : \text{si } n \text{ ne divise pas } ab, \text{ alors } n \text{ ne divise ni } a, \text{ ni } b$. Nous pouvons réécrire $P'(a, b, n)$ en langage 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*. Supposons la négation du côté droit de l'implication. Autrement dit, supposons :

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

Par **De Morgan**, nous avons

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

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

$$(n|a) \vee (n|b) \implies n|ab \quad (1.3)$$

Note :

Intuitivement, nous savons déjà que si on a un nombre n qui 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 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 . \square

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

La réciproque 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 pas 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. \square

4. Montrez que n divise a et b si et seulement si n divise $\text{pgcd}(a, b)$. 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 $\text{pgcd}(a, b)$, nous pouvons réécrire $P''(a, b, n)$ en langage logique de la façon suivante :

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

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

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

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

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

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

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

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 $\text{pgcd}(a, b)$ 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 :

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

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 le plus grand commun diviseur de a et b .

Par définition :

$$n = \text{pgcd}(a, b)$$

- n n'est pas l'unique diviseur de a et b et il existe un $\text{pgcd}(a, b)$, tel que

$$n \neq \text{pgcd}(a, b)$$

Dans le premier cas, on sait que n divise le $\text{pgcd}(a, b)$, par le **Lemme 1**. Dans le deuxième cas, on sait que n divise $\text{pgcd}(a, b)$ 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 . \square

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

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

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 $\text{pgcd}(a, b)$ et il existe un entier $k \in \mathbb{Z}$ tel que $nk = \text{pgcd}(a, b)$.

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 $\text{pgcd}(a, b)$ par un entier $l \in \mathbb{Z}$ et il est possible d'obtenir b en multipliant $\text{pgcd}(a, b)$ par un entier $m \in \mathbb{Z}$.

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

$$a = \text{pgcd}(a, b) \cdot l = nkl$$

$$b = \text{pgcd}(a, b) \cdot m = nkm$$

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 $\text{pgcd}(a, b)$ n divise également a et b .

Nous venons de montrer que la proposition $P''_q(a, b, n)$ et

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

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

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

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

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

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

Nous allons procéder en montrant que le nombre d' divise $n \times \text{pgcd}(a, b)$ et que $n \times \text{pgcd}(a, b)$ 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 :

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

Et donc, nous avons également :

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

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 $a = -b$. \square

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 pgcd 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 $\text{pgcd}(a, b)$, alors, $ab|c$

Preuve

Supposons que $a|c$ et $b|c$ et $\text{pgcd}(a, b) = 1$. 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 $(pb)ak + (ma)bl = c$:

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

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 $\text{pgcd}(a, b) = 1$, alors $ab|c$. \square

Nous avons prouvé le Lemme 4 en supposant que $\text{pgcd}(a, b) = 1$. 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 $\text{pgcd}(a, b) \neq 1$, ab divisera c .

Lemme 5

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

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

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

Preuve

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

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

Puisque d' divise toutes les combinaisons linéaires 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, $\text{pgcd}(an, bn)$ divise $n \times \text{pgcd}(a, b)$

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

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

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 $d' = \text{pgcd}(an, bn)$. 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 linéaires de a et b . Donc, d divise une 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' . \square

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

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

parce que

- $\text{pgcd}(an, bn)$ **divise** $n \times \text{pgcd}(a, b)$ **et**
- $n \times \text{pgcd}(a, b)$ **divise** $\text{pgcd}(an, bn)$

PROBLÈME 1 · SIERPASKAL

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

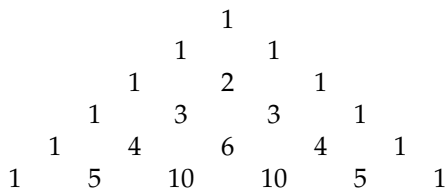


FIGURE 1.1 – Triangle de Pascal

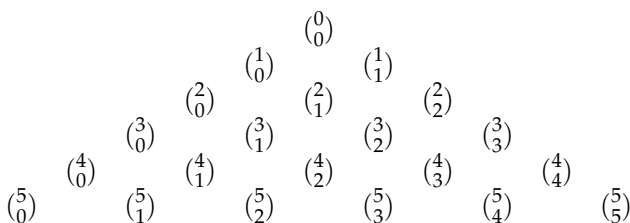


FIGURE 1.2 – Représentation du Triangle de Pascal

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 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 rangée 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 $C(n, k)$

$$\binom{n}{k} ::= \binom{n}{0} = 1 \text{ et } \binom{n}{n} = 1$$

D'après le triangle de Pascal, nous savons que chaque entrée à la rangée n est égal à l'entrée à la somme de la $k - 1$ -ième entrée à la rangée $n - 1$ 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 :

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