8. Divisibilité dans $\mathbb{Z}$

Dans $\mathbb{Z}$ il y une notion de $\leq$ et une notion de divisibilité[13]. Au niveau des définitions les deux sont un peu similaires.

Définition 8.1. *Soient n, m deux entiers. On écrit $n \leq m$ (ou $m \geq n$) s'il existe un nombre* **naturel** *$r \in \mathbb{N}$ tel que $n + r = m$.*

Si $n \leq m$ on dit "n est plus petit que ou égal à m", ou "m est plus grand que ou égal à n".

Définition 8.2. *Soient n, m deux entiers. On écrit $n|m$ s'il existe un nombre* **entier** *$r \in \mathbb{Z}$ tel que $nr = m$.*

Si $n|m$ on dit que "n divise m", ou "m est divisible par n", ou "m est un n-multiple".

Voici quelques propriétés élémentaires.

Théorème 8.1. *Soient a, b, c trois nombres entiers.*
(i) Si $a \leq b$ et $b \leq c$ alors $a \leq c$.
(ii) Si $a \leq b$ alors $a + c \leq b + c$.
(iii) Si $a \leq b$ et $b \leq a$ alors $a = b$
(iv) Si $a \leq b$ et $c \in \mathbb{N}$ alors $ac \leq bc$
(v) Si $a \leq b$ alors $-b \leq -a$.

Théorème 8.2. *Soient a, b, c trois nombres entiers.*
(i) Si $a|b$ et $b|c$ alors $a|c$.
(ii) Si $a|b$ alors $ac|bc$ et $a|bc$.
(iii) Si $a|b$ et $b|a$ alors $|a| = |b|$.
(iv) Si $a|b$ et $a|c$ alors $a|(b + c)$.

Démonstration. (i) Si $a \leq b$ et $b \leq c$ il existe $r, s \in \mathbb{N}$ tels que $a + r = b$ et $b + s = c$. Donc $a + (r + s) = b + s = c$ et $r + s \in \mathbb{N}$ donc $a \leq c$.

Si $a|b$ et $b|c$ il existe $r, s \in \mathbb{Z}$ tels que $ar = b$ et $bs = c$. Donc $a(rs) = bs = c$ et $rs \in \mathbb{Z}$ donc $a|c$.

(ii) Si $a \leq b$ alors il existe $r \in \mathbb{N}$ tel que $a + r = b$. Donc $(a + c) + r = b + c$ et $a + c \leq b + c$.

Si $a|b$ alors il existe $r \in \mathbb{Z}$ tel que $ar = b$. Donc $(ac)r = bc$ et $ac|bc$. Aussi $a|ac$ donc par (i) : $a|bc$.

(iii) Si $a \leq b$ et $b \leq a$, ils existent $r, s \in \mathbb{N}$ tels que $a + r = b$ et $b + s = a$. Donc $a + r + s = b + s = a$ et $r = -s$. Mais $r, s \in \mathbb{N}$, donc $r = s = 0$, ou $a = b$.

Si $a|b$ et $b|a$, ils existent deux entiers r, s tels que $ar = b$ et $bs = a$. Donc $ars = bs = a$ et $a(rs - 1) = 0$. Si $a = 0$, alors $b = ar = 0$ aussi. Si $a \neq 0$ alors $rs = 1$ donc $r = s = 1$ ou $r = s = -1$. Donc $a = b$ ou $a = -b$.

13. Voir [R, §2.3]

(iv Si $a \leq b$ il existe $r \in \mathbb{N}$ tel que $a + r = b$. Si aussi $c \in \mathbb{N}$ alors $rc \in \mathbb{N}$ et $ac + rc = (a + r)c = bc$, donc $ac \leq bc$.

Si $a|b$ et $a|c$ alors il existe $r, s \in \mathbb{Z}$ tels que $ar = b$ et $as = c$. Donc $a(r+s) = ar+as = b+c$ et $a|(b + c)$.

(v) Si $a \leq b$, il existe $r \in \mathbb{N}$ tel que $a + r = b$. Donc $-b + r = -a$ et $-b \leq -a$.

□

Exemple 8.1. Soit $n \in \mathbb{Z}$.

(i) On a $n \in \mathbb{N}$ si et seulement si $0 \leq n$.

(ii) Toujours : $1|n$ et $n|0$.

(iii) Très important : Si $n|a$ et $n|b$ alors pour tous les entiers r et s on a

$$n|(ra + sb).$$

8.1. **Nombres premiers et composés.** Deux définitions :

Définition 8.3. *Un nombre naturel $p > 1$ est un nombre appelé* premier *si les seuls diviseurs positifs sont* 1 *et p.*

Un nombre naturel $n > 1$ est un nombre appelé composé *si n n'est pas premier.*

En particulier, 1 n'est pas considéré comme un nombre premier, ni -2. Des nombres premiers sont par exemple :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

Des nombres composés :

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 21, 22, 24, 25, 26, 27, 28 \ldots$$

Théorème 8.3. *Pour chaque nombre naturel $n > 1$ il existe un entier $s \geq 1$ et des nombres premiers p_1, $p_2, \ldots, p_s$ tels que*

$$n = p_1 p_2 \ldots p_s$$

On dit : "Une décomposition en facteurs premiers existe".

Par exemple : $36 = 2 \cdot 2 \cdot 3 \cdot 3$: ici $s = 4$, $p_1 = 2$, $p_2 = 2$, $p_3 = 3$ et $p_4 = 3$.

Il y a aussi un aspect d'unicité que nous allons énoncer et montrer plus tard.

Démonstration. Posons $P(n) :=$ "il existe un $s \geq 1$ et des nombres premiers $p_1, \ldots, p_s$ tels que $n = p_1 p_2 \cdots p_s$".

Début : $P(2)$ est vraie, parce que $2 = p_1$ ou $s = 1$ et $p_1 = 2$ est un nombre premier.

Étape d'induction : Soit $n \geq 2$ et pour chaque $2 \leq a \leq n$ on suppose $P(a)$ vraie.

Si $n + 1$ est premier, alors $n + 1 = p_1$ avec $s = 1$ et $p_1 = n + 1$ premier ; ce qui montre que $P(n + 1)$ est aussi vraie.

Si $n + 1$ n'est pas premier, alors il existe un diviseur $d > 0$ inégal à 1 ou $n + 1$. Donc il existe un q suppose que $P(d)$ et $P(q)$ sont vraies. Donc $d = p_1 p_2 \ldots p_s$ et $q = p'_1 p'_2 \ldots p'_{s'}$ où

$s, s' > 0$ et les p_i et p'_i des nombres premiers. Alors $n = dq = p_1 p_2 \dots p_s p'_1 p'_2 \dots p'_{s'}$ est un produit de $s + s'$ nombres premiers. Donc $P(n+1)$ est aussi vraie.

Par le principe d'induction généreuse $P(n)$ est vraie pour chaque entier $n \geq 2$. $\square$

8.2. **Division avec reste.** On ne peut pas toujours diviser dans $\mathbb{Z}$, mais on a un alternatif très fiable. C'est essentiellement la longue division de l'école primaire : une divison partielle avec un petit reste à la fin.

Théorème 8.4 (Division-avec-reste)**.** *Soit $m > 0$ un nombre naturel non-zéro fixé.*

Pour chaque $n \in \mathbb{Z}$ il existe deux uniques nombres entiers q, r tels que simultanément :

(i) $n = qm + r$

(ii) $0 \leq r < m$.

On dit : r est le *reste* et q le *quotient* de la division partielle de n par m.

Remarque. Soient n et $m > 0$ deux nombres naturels. Considérons la fraction $\frac{n}{m}$. Alors il y un unique nombre naturel q tel que $q \leq \frac{n}{m} < q + 1$. C'est le q du théorème. Ce q est donc presque $\frac{n}{m}$.

Démonstration. La preuve se déroule en plusieurs étapes.

(a) Pour $n \in \mathbb{Z}$ définissons la fonction propositionnelle

$$P(n) := \exists q \in \mathbb{Z}\ \exists r \in \mathbb{Z}\ ([n = qm + r] \wedge [0 \leq r < m]).$$

Montrons d'abord $P(n)$ vraie pour chaque $n \in \mathbb{N}$, par induction généreuse.

Début : Pour $0 \leq n < m$, prenons $q = 0$ et $r = n$, dans ce cas en effet $n = qm + r = 0m + n$ et $0 \leq r < m$ sont vraies.

Étape d'induction : Soit $n \in \mathbb{N}$. Supposons $P(a)$ vraie pour chaque $0 \leq a \leq n$. À montrer que $P(n+1)$ serait vraie aussi.

Si $0 \leq n < m - 1$ alors $1 \leq n + 1 < m$ et on a déjà montré au début de l'induction que $P(n+1)$ est vraie, ce que nous voulions montrer.

Dans l'autre cas, supposons que $n \geq m - 1$. Prenons $a = n + 1 - m$, alors $0 \leq a \leq n$. Donc par l'hypothèse d'induction généreuse $P(a)$ est supposé vraie. C.-à-d., il existe des nombres entiers q_0 et r_0 tels que $n + 1 - m = a = q_0 m + r_0$ et $0 \leq r_0 < m$. Donc $n + 1 = (q_0 + 1)m + r_0$. En prenant $q = q_0 + 1$ et $r = r_0$ on obtient $n + 1 = qm + r$ et $0 \leq r < m$. Alors $P(n+1)$ serait aussi vraie.

Par induction on conclut $P(n)$ vraie pour chaque $n \in \mathbb{N}$.

(b) Maintenant on veut montrer $P(n)$ si $n < 0$. Soit $n < 0$. Alors $-n > 0$ et nous savons maintenant que $P(-n)$ est vraie : Il existe des entiers q_0 et r_0 telles que $-n = q_0 m + r_0$ et $0 \leq r_0 < m$. Deux cas : $r_0 = 0$ et $r_0 \neq 0$.

- Dans le premier cas $n = (-q_0)m + 0$ est la décomposition voulu et $P(n)$ est vraie.

• Dans l'autre cas : posons $r = -r_0 + m$ et $q = -q_0 - 1$. Alors $0 \leq -r_0 + m < m$ implique $0 \leq r < m$ et $n = (-q_0 - 1)m + (-r_0 + m) = qm + r$. Ce qui montre que $P(n)$ est vraie aussi. Conclusion : $\forall n \in \mathbb{Z}\ P(n)$ vraie.

(c) Il reste encore de montrer l'unicité de q et r. Supposons $n = qm + r = q_1 m + r_1$ et $0 \leq r < m$ et $0 \leq r_1 < m$. Alors $qm + r = q_1 m + r_1$, ou $r - r_1 = (q_1 - q)m$.

Sans perte de généralité nous pouvons supposer que $r \geq r_1$. Et donc $0 \leq r - r_1 < m$.

Ça implique que $0 \leq (q_1 - q)m < m$ et donc $0 \leq q_1 - q < 1$.

Mais en général si $0 \leq N < 1$ et N entier, implique $N = 0$.

Donc $q_1 = q$ et $r = n - qm = n - q_1 m = r_1$. □

8.3. **Le** pgcd **et le** ppcm**.** Soient a et b deux entiers. Posons

$$\mathrm{pgcd}(a, b),$$

le plus grand commun diviseur de a et b, pour le plus grand nombre naturel d qui divise a et b simultanément. Et posons

$$\mathrm{ppcm}(a, b),$$

le plus petit commun multiple de a et b, pour le plus petit nombre naturel m qui est un a-multiple et un b-multiple simultanément.

On dit que a et b sont *relativement premier* si le $\mathrm{pgcd}(a, b) = 1$.

Si $a \geq 1$, alors $\mathrm{pgcd}(0, a) = a$ et $\mathrm{pgcd}(1, a) = 1$.

Exemple : $\mathrm{pgcd}(10, 16) = 2$, $\mathrm{ppcm}(10, 16) = 80$. Ici, $\mathrm{pgcd}(10, 16)\,\mathrm{ppcm}(10, 6) = 10 \cdot 6$. Un accident ?

$\mathrm{pgcd}(10, -21) = 1$ donc 10 et -21 sont relativement premier.

Un premier lemme[14] :

Lemme 8.1. *Soit $m > 0$ et n deux entiers. Par division avec reste il existe des entiers q et r tels que $n = qm + r$ et $0 \leq r < m$.*

Alors $\mathrm{pgcd}(n, m) = \mathrm{pgcd}(m, r)$. *Si $r = 0$ alors* $\mathrm{pgcd}(n, m) = m$.

8.4. **L'algorithme d'Euclide.** Le lemme suggère un façon de calculer le plus grand commun diviseur $d = \mathrm{pgcd}(n, m)$ par récurrence ($m > 0$).

Soit $n = qm + r$ et $0 \leq r < m$. Si $r = 0$ alors $d = m$ et on est prêt avec le calcul.

Sinon $0 < r < m$ et $d = \mathrm{pgcd}(m, r)$. Soit $m = q_1 r + r_1$ et $0 \leq r_1 < r$. Si $r_1 = 0$, alors $d = \mathrm{pgcd}(m, r) = r$ et on est prêt.

Sinon $0 < r_1 < r < m$ et $d = \mathrm{pgcd}(r, r_1)$. Soit $r = q_2 r_1 + r_2$. Si $r_2 = 0$, alors $d = \mathrm{pgcd}(r, r_1) = r_1$ et on est prêt.

Sinon $0 < r_2 < r_1 < r < m$ et $d = \mathrm{pgcd}(r_1, r_2)$. Soit $r_1 = q_3 r_2 + r_3$. Si $r_3 = 0$, alors $d = \mathrm{pgcd}(r_1, r_2) = r_2$ et on est prêt.

Sinon ...

14. Voir [R, p. 119]

Les restes deviennent de plus en plus petit, et après moins que m étapes un reste, disons r_{i+1}, devient 0. Et alors le pgcd est $d = r_i$.

C'est *l'algorithme d'Euclide.*

Exemple 8.2. Calculons $\mathrm{pgcd}(1351, 1064)$ avec l'algorithme d'Euclide [15]. On calcule la suite des restes

$$\begin{aligned}
1351 &= 1 \cdot 1064 + 287 \\
1064 &= 3 \cdot 287 + 203 \\
287 &= 1 \cdot 203 + 84 \\
203 &= 2 \cdot 84 + 35 \\
84 &= 2 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7 + 0.
\end{aligned}$$

Donc ici les restes sont : $r = 287$, $r_1 = 203$, $r_2 = 84$, $r_3 = 35$, $r_4 = 14$, $r_5 = 7$ et $r_6 = 0$.

Ici : $7 =$ le dernier reste non-zero $= \mathrm{pgcd}(1351, 1064)$.

Et

$$\begin{aligned}
\mathrm{pgcd}(1351, 1064) &= \mathrm{pgcd}(1064, 287) = \mathrm{pgcd}(287, 203) = \mathrm{pgcd}(203, 84) = \\
&= \mathrm{pgcd}(84, 35) = \mathrm{pgcd}(35, 14) = \mathrm{pgcd}(14, 7) = \\
&= \mathrm{pgcd}(7, 0) = 7
\end{aligned}$$

8.5. **Modulo m.** Pour des entiers a, b, m ($m \neq 0$) nous allons écrire

$$a \equiv_m b \quad \text{si} \quad m|(a - b).$$

On dit "a est équivalent à b modulo m". C'est une *relation d'équivalence*, c.-à-d :

Lemme 8.2. *Fixons $m \neq 0$ un entier. $\equiv_m$ est une relation d'équivalence sur $\mathbb{Z}$, c.-à.d,*

(i) $n \equiv_m n$ pour chaque $a \in \mathbb{Z}$;

(ii) Si $n_1 \equiv_m n_2$, alors $n_2 \equiv_m n_1$, pour chaque $n_1, n_2 \in \mathbb{Z}$;

(iii) Si $n_1 \equiv_m n_2$ et $n_2 \equiv_m n_3$ alors $n_1 \equiv_m n_3$ pour chaque $n_1, n_2, n_3 \in \mathbb{Z}$;

Démonstration. (i) $n \equiv_m n$ parce que $n - n = 0$ et $m|0$.

(ii) Supposons $n_1 \equiv_m n_2$, c.-à-d., $m|(n_1 - n_2)$: il existe $r \in \mathbb{Z}$ tel que $rm = n_1 - n_2$. Alors $(-r)m = n_2 - n_1$ et $-r \in \mathbb{Z}$, donc par définition $m|(n_2 - n_1)$ et $n_2 \equiv_m n_1$.

(iii) Supposons $n_1 \equiv_m n_2$ et $n_2 \equiv_m n_3$, c.-à-d., $m|(n_1 - n_2)$ et $m|(n_2 - n_3)$: il existe $r_1, r_2 \in \mathbb{Z}$ tel que $r_1 m = n_1 - n_2$ et $r_2 m = n_2 - n_3$. Alors $(r_1 + r_2)m = (n_1 - n_2) + (n_2 - n_3) = n_1 - n_3$. Donc $m|(n_1 - n_3)$ et $n_1 \equiv_m n_3$. $\square$

15. Voir aussi [R, p.120]

Le théorème suivant donne une grande flexibilité [16] pour le calcul modulo m.

Théorème 8.5. *Soient a, b, c, d, m des nombres entiers.*
Si $a \equiv_m c$ et $b \equiv_m d$, alors $(a+b) \equiv_m (c+d)$ et $(ab) \equiv_m (cd)$.

Démonstration. Si $a \equiv_m c$ et $b \equiv_m d$ alors il existe des entiers r, s tels que $mr = (a-c)$ et $ms = (b-d)$. Donc $m(r+s) = (a-c)+(b-d) = (a+b)-(c+d)$ et $(a+b) \equiv_m (c+d)$.

Et aussi $a = c + mr$ et $b = d + ms$. Donc

$$ab - cd = (c+mr)(d+ms) - cd = m(rd + cs + mrs),$$

ce qui implique que $(ab) \equiv_m (cd)$. □

Une conséquence du Théorème 8.4.

Corollaire 8.1. *Soit $m > 0$ un nombre naturel.*
Pour chaque $n \in \mathbb{Z}$ il existe un unique nombre naturel r tel que $n \equiv_m r$ et $0 \leq r < m$.

Démonstration. Soit $n \in \mathbb{Z}$. Par le thm. 8.4 il existe deux entiers q et r tels que $n = qm + r$ et $0 \leq r < m$. Alors $m|(n-r)$ et $n \equiv_m r$.

Si $n \equiv_m r_1$ et $n \equiv_m r_2$ avec $0 \leq r_i < m$ pour chaque $i = 1, 2$. Alors il existe deux entiers q_1, q_2 tels que $n - r_i = q_i m$ ou $n = q_i m + r_i$, pour $i = 1, 2$. Par la partie "unicité" du thm : $r_1 = r_2$ (et $q_1 = q_2$).

Le reste de la preuve est une conséquence directe et est laissé.

□

8.6. **Exemple.** On va faire un autre exemple d'induction. On utilise "modulo 3 et "modulo 2".

Rappelons : Les *nombres de Fibonacci* $F(i)$, pour $i \in \mathbb{N}$, sont définis par induction.

Au début $F(0) = 0, F(1) = 1$.

Soit $n \geq 1$. Si $F(i)$ est défini pour chaque nombre naturel $0 \leq i \leq n$, alors on définit

$$F(n+1) = F(n) + F(n-1).$$

Montrer : $F(n)$ est pair si $n \equiv 0 \bmod 3$ et $F(n)$ est impair si $n \not\equiv 0 \bmod 3$.

Phase brouillon. Calculons quelques cas :

$$F(0) = 0, F(1) = 1, F(2) = 1,\ F(3) = 2, F(4) = 3, F(5) = 5,$$

$$F(6) = 8, F(7) = 13, F(8) = 21,\ F(9) = 34, F(10) = 55 \ldots$$

On remarque ici qu'au moins $F(0), F(3), F(6), F(9)$ sont pairs, et les autres impairs. Ça pourrait fonctionner !

Il faut montrer $F(3k)$ est toujours pair ($k \geq 0$) et les autres $F(3k+1)$ et $F(3k+2)$ cas impairs. Ça vient en forme de triples : $3k, 3k+1, 3k+2$? Semble plus naturel de faire induction sur k (les triples) plutôt que sur n ?

16. Voir [R, p.112]

La relation de récurrence qu'on voit est $F(n+1) = F(n) + F(n-1)$, qui fonctionne à partir que $n \geq 1$.

Idée : "pair plus impair est impair" et "impair plus impair est pair" et "impair plus pair est impair" ! Et on arrive à un triple plus tard !

Ah ça fonctionne. Maintenant je me sens prêt pour la version propre.

Phase version propre.

Démonstration. Il suffit de montrer que la fonction propositionnelle suivante est vrai pour $k \in \mathbb{N}$:

$$P(k) = \text{" } F(3k) \text{ est pair et } F(3k+1) \text{ et } F(3k+2) \text{ sont impairs."}$$

Début d'induction (pour $k = 0$). On a que $F(3 \cdot 0) = 0$ est pair et que $F(3 \cdot 0 + 1) = 1$ et $F(3 \cdot 0 + 2) = 1$ sont impairs. En effet $P(0)$ est vraie.

Étape d'induction : Soit $k \geq 0$. Supposons $P(k)$ vraie, c.-à-d., supposons

$F(3k)$ est pair et $F(3k+1)$ et $F(3k+2)$ sont impairs.

Pour montrer $P(k+1)$ vraie, il faut vérifier trois cas :

• On a $F(3(k+1)) = F(3k+2) + F(3k+1)$ par définition des nombres de Fibonacci. Par l'hypothèse d'induction $F(3k+2)$ et $F(3k+1)$ sont impairs, donc il suit que $F(3(k+1))$ est pair.

• Puis $F(3(k+1)+1) = F(3(k+1)) + F(3k+2)$. Par induction $F(3k+2)$ est impair, et on vient de montrer que $F(3(k+1))$ est pair. Donc il suit que $F(3(k+1)+1)$ est impair.

• Puis $F(3(k+1)+2) = F(3(k+1)+1) + F(3(k+1))$. On vient de montrer que $F(3(k+1)+1)$ est impair et que $F(3(k+1))$ est pair, donc il suit que $F(3(k+1)+2))$ est impair.

Nous venons de montrer que si $P(k)$ vraie alors $P(k+1)$ est vraie aussi.

Par le principe d'induction $P(k)$ est vrai pour chaque $k \in \mathbb{N}$. Ce qui implique ce que nous voulions montrer. □

Une variation : À la place de faire induction sur les triples, on peut décider d'utiliser l'induction généreuse sur n. La récurrence fonctionne à partir de $n = 1$, donc il faut commencer par deux cas spéciaux $n = 0, 1$. Le reste de la partie brouillon est pareil.

Démonstration. Il suffit de montrer que la fonction propositionnelle suivante est vrai pour $n \in \mathbb{N}$:

$$P(n) = \text{"}F(n) \text{ est pair si } n \equiv 0 \bmod 3 \text{ et } F(n) \text{ est impair si } n \not\equiv 0 \bmod 3\text{"}.$$

Début d'induction (pour $n = 0$ et $n = 1$). On a que $F(0) = 0$ est pair et que $F(1) = 1$ est impair. Et donc en effet $P(0)$ et $P(1)$ sont vraies.

Étape d'induction généreuse : Soit $n \geq 1$. Supposons $P(k)$ vraie pour chaque $0 \leq k \leq n$. Nous voulons montrer $P(n+1)$ vraie.

Il faut vérifier trois cas :

• Il existe un $k \geq 1$ tel que $n+1 = 3k$. Dans ce cas $n \not\equiv 0 \bmod 3$ et $n-1 \not\equiv 0 \bmod 3$, donc par l'hypothèse d'induction $F(n)$ et $F(n-1)$ sont impairs. Par la récurrence $F(n+1) = F(n) + F(n-1)$ il suit que $F(n+1)$ est pair.

• Il existe un $k \geq 1$ tel que $n+1 = 3k+1$. Dans ce cas $n \equiv 0 \bmod 3$ et $n-1 \not\equiv 0 \bmod 3$, donc par l'hypothèse d'induction $F(n)$ est pair et $F(n-1)$ est impair. Par la récurrence $F(n+1) = F(n) + F(n-1)$ il suit que $F(n+1)$ est impair.

• Soit $n+1 = 2$, soit il existe un $k \geq 1$ tel que $n+1 = 3k+2$. On a que $F(2) = F(1)+F(0) = 1$ est impair. Dans l'autre cas, $n \not\equiv 0 \bmod 3$ et $n-1 \equiv 0 \bmod 3$, donc par l'hypothèse d'induction $F(n)$ est impair et $F(n-1)$ est pair. Par la récurrence $F(n+1) = F(n)+F(n-1)$ il suit que $F(n+1)$ est impair.

Donc nous venons de montrer que si $P(n)$ vraie, $n \geq 1$, alors aussi $P(n+1)$ est vraie.

Par le principe d'induction (généreuse) il suit que $P(n)$ est vraie pour chaque $n \geq 0$. Ce qui finit la démonstration. $\square$

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA