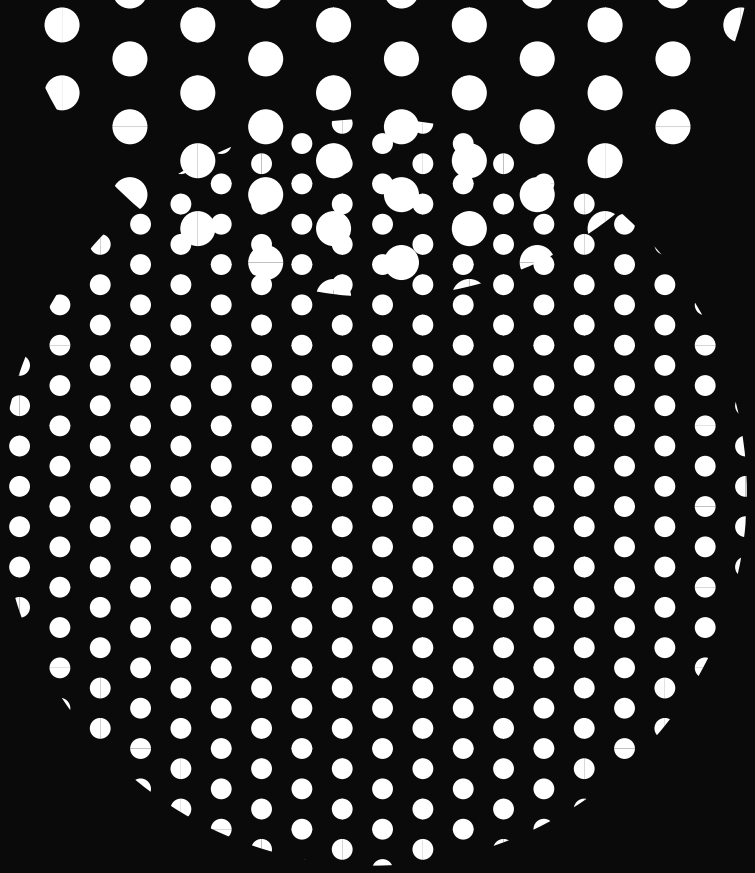


Prop 2.3: Tout entier $a \neq 0$ est le successeur d'un unique entier c

Dem. c est unique par l'axiome 2
Maintenant l'axiome d'existance
On introduit un ensemble $E = \{0\} \cup S(\mathbb{N})$
On voit bien que $0 \in E$, de plus $E \subset \mathbb{N} \subset S(E) \subset S(\mathbb{N})$
Or $S(\mathbb{N}) \subset E$, donc $S(E) \subset S(\mathbb{N}) \subset E$
Donc l'axiome 3 s'applique et $E = \mathbb{N}$
On en déduit que $S(\mathbb{N}) = E \setminus \{0\} = \mathbb{N} \setminus \{0\}$
Donc pour tout $a \in \mathbb{N} \setminus \{0\}$ quelconque,
il existe un entier c unique tel que $a = S(c)$

Théorème 2.5: Soit $P(n)$ une propriété définie pour tout $n \in \mathbb{N}$

On suppose que $P(0)$ est vrai et $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$

Dém.
On introduit un ensemble E des nombres entiers pour lesquels la propriété P est vrai.

Or $P(0)$ est vrai, donc $0 \in E$

Or $P(n) \Rightarrow P(n+1)$ $\forall n \in \mathbb{N}$.
et on sait que $n+1 = S(n)$ $\forall n \in \mathbb{N}$
donc $S(E) \subset E$

Or $0 \in E$ et $S(E) \subset E$ donc $E = \mathbb{N}$
et $P(n)$ est vrai pour tout $n \in \mathbb{N}$
(l'axiome A3 s'applique)

Prop 2.3 Tout entier $a \neq 0$ est le successeur d'un unique entier c

Dém. L'unicité de c est prouvé par l'axiome A2

Démontrons l'existance :
Introduisons l'ensemble $E := \{0\} \cup s(\mathbb{N})$
$0 \in E$
$E \subset \mathbb{N} \Rightarrow s(E) \subset s(\mathbb{N})$
Or $s(\mathbb{N}) \subset E$ donc $s(E) \subset s(\mathbb{N}) \subset E$
Donc $E = \mathbb{N}$ par l'axiome A3

On en déduit que $s(\mathbb{N}) = E \setminus \{0\} = \mathbb{N} \setminus \{0\}$
Donc tout $a \in \mathbb{N} \setminus \{0\}$ est le successeur d'un unique entier $c \in \mathbb{N}$

Théorème 2.5 Soit $P(n)$ est une propriété définie pour tout $n \in \mathbb{N}$
On suppose que $P(0)$ est vrai
et $P(n)$ implique $P(n+1)$

Dém.

Introduisons E l'ensemble des nombres pour lesquels $P(n)$ est vrai
Or $P(0)$ est vrai, donc $0 \in E$

Or $P(n)$ implique $P(n+1)$ et $n+1 = s(n)$ donc $s(E) \subset E$

Or $0 \in E$ et $s(E) \subset E$, donc $E = \mathbb{N}$

Donc $P(n)$ est vrai $\forall n \in \mathbb{N}$ □

Lemme 2.7 Pour tout $a \in \mathbb{N}$, $a+0 = a = 0+a$

On définie une propriété $P(a) = a+0 = a = 0+a$ pour tout $a \in \mathbb{N}$

$P(0)$ est vrai car $0+0 = 0 = 0+0$

Supposons que $P(a)$ est vrai, donc $a+1$ doit aussi être vrai
$P(a) = a+0 = a = 0+a$
$P(a+1) = (a+1)+0 = a+(1+0) = a+(s(0)+0) = a+s(0+0) = a+s(0) = a+1$
$0+s(a) = s(0+a) = s(a) = a+1$

Donc $P(a)$ est vrai $\forall a \in \mathbb{N}$

(3) $\forall a,b,c \in \mathbb{N}$, $a+b = a+c \Rightarrow b=c$

Raisonnons par récurrence

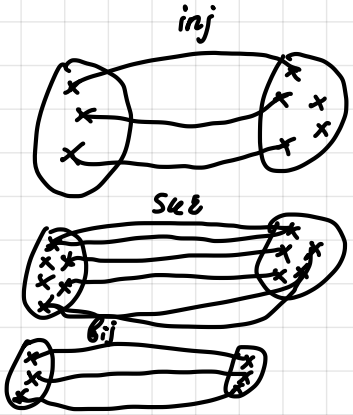
Introduisons une propriété $P(a)$: $a+b = a+c \Rightarrow b=c$

Initialisation: $P(0)$: $0+b = b$ par la lemme 2.7

$0+c = c$ par la lemme 2.7

donc $0+b = 0+c \Leftrightarrow b=c$

Par conséquence $P(0)$ est vrai



Hérédité:

$P(n)$: $n+b = n+c \Rightarrow b=c$

Supposons que $P(n)$ est vrai

$P(n+1)$: $n+1+b = n+1+c$

$\Leftrightarrow s(n)+b = s(n)+c$

$\Leftrightarrow s(n+b) = s(n+c)$ par l'axiome A2 (injectivité)

$\Leftrightarrow n+b = n+c \Rightarrow b=c$

Donc $P(a)$ est vrai

$a+b \geq a+c \Leftrightarrow b \geq c$

Démontrez

$b \geq c \Leftrightarrow b = n+c$ $^{n \in \mathbb{N}}$ par la définition

$\Leftrightarrow a+b = a+n+c$ par la règle de simplification

$\Leftrightarrow a+b \geq a+c$ par la définition de $(\geq)$

5) Si $q \geq p$ alors $n \cdot q \geq n \cdot p$ $\forall n,p,q \in \mathbb{N}$

<u>Dém.</u>

On suppose que $q \geq p \Leftrightarrow q = m+p$, $m \in \mathbb{N}$ par la déf. de $(\geq)$

$q = m+p$ (on multiplie par n)

$\Leftrightarrow n \cdot q = n(m+p)$

$\Leftrightarrow n \cdot q = n \cdot m + n \cdot p$ Soit $y = n \cdot m \in \mathbb{N}$

$\Leftrightarrow n \cdot q = y + n \cdot p$

$\Leftrightarrow n \cdot q \geq n \cdot p$ par la déf de $(\geq)$

$A \times B = \{(a,b) ; a \in A \text{ et } b \in B\}$

$\text{Card}(A \times B) = \text{Card}\, A \cdot \text{Card}\, B$

<u>Dém</u> Soit $A = \{a_1, \dots, a_n\}$ $B = \{b_1, \dots, b_m\}$

On commence par introduction d'un ensemble

$\{a_1\} \times B = \{(a_1, b) ; b \in B\}$

Or a_1 est un seul élément, disons constante, $\{a_1\} \times B$ contient exactement $\text{Card}\, B$ élément

Puis, on fait cela avec chaque élément de A

$\{a_2\} \times B$

$\vdots$

$\{a_n\} \times B$

Il est trivial que chaque ensemble contient $\text{Card}\, B$ élément et il y a $\text{Card}\, A$ ensemble.

Alors, $\text{Card}(A \times B) = \text{Card}\, A \cdot \text{Card}\, B$

$a | b \iff \exists n \in \mathbb{Z}$ tq $b = a \cdot n$

Supposons que $b \neq 0$

$0 | b \iff \exists n$ tq $b = 0 \cdot n \Rightarrow b = 0$, mais on a supposé que $b \neq 0$, absurd.

$a | b \Rightarrow b = a \cdot n \Rightarrow |a \cdot n = b| = |a \cdot n| = |b|$
$= |a| \cdot |n| \neq |b|$

$|a| \cdot 1 \leq |a| \cdot |n| = |b|$
$\iff |a| \leq |b|$

$a | b \Rightarrow \exists n \quad b = a \cdot n$

Soit $k, l \in \mathbb{Z}$ $ka + lb = ka + lan = a(k + ln)$ notons $k + ln = N$
$= aN$

Donc $ka + lb$ est divisible par a.

$a = a \cdot 1$, notons $n = 1$, donc $\forall a \in \mathbb{Z}$, $a = a \cdot n$ avec $n = 1$
donc par def $a \mid a$

$a \mid b \land b \mid c \Rightarrow a \mid c$

pv : $a \mid b \Rightarrow \exists n,\ b = a \cdot n$
$b \mid c \Rightarrow \exists k,\ c = b \cdot k$

Or $b = a \cdot n$, donc $c = b \cdot k$
$= a \cdot n \cdot k$

notons $N = n \cdot k$, donc $c = a \cdot N$
donc par déf $a \mid c$

$a \mid b \Rightarrow \exists n,\ b = an$
$b \mid a \Rightarrow \exists k,\ a = b \cdot k$

$a = a\, n \cdot k$

Or on peut pas diviser, donc $a \neq 0$ et $b \neq 0$

$a = a \cdot \underbrace{n \cdot k}_{l}$ par déf $a \mid a$ et $(n \cdot k) = l = 1$
$(n \cdot k = 1)$

Si : $d \mid a$ et $d \mid b$

donc $a = n \cdot d$ $\quad b = s \cdot d$

$a = qb + r$

$\Leftrightarrow n \cdot d = q \cdot s \cdot d + r$
$\Leftrightarrow$

$d \mid a$ ou $d \mid (qb + r)$
$\Leftrightarrow (qb + r) = q_2 d$
$q \cdot s \cdot d + r = q_2 d$

Exo 1

c) Déterminer tous $x \in \mathbb{Z}$ tel que $x-5 \mid x+7$

$\Leftrightarrow \quad x+7 \equiv 0 \ [x-5]$

$\Leftrightarrow \quad x+7-(x-5) \equiv 0 \ [x-5]$

$\Leftrightarrow \quad 12 \equiv 0 \ [x-5]$

$\Leftrightarrow \quad x-5 \mid 12$

$\Leftrightarrow \quad x-5 \in \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$

$\Leftrightarrow \quad x \in \{-7, -1, 1, 2, 3, 4, 6, 7, 8, 9, 11, 17\}$

Exo 2

$n \in \mathbb{N} \quad n+1 \mid n^2+1$

$\Leftrightarrow n^2+1 \equiv 0 \ [n+1]$

$\Leftrightarrow n^2+1-(n+1)^2 \equiv 0 \ [n+1]$

$\Leftrightarrow n^2+1-n^2-2n-1 \equiv 0 \ [n+1]$

$\Leftrightarrow -2n \equiv 0 \ [n+1]$

$\Leftrightarrow -2n+2(n+1) \equiv 0 \ [n+1]$

$\Leftrightarrow -2n+2n+2 \equiv 0 \ [n+1]$

$\Leftrightarrow 2 \equiv 0 \ [n+1]$

$\Leftrightarrow n+1 \mid 2$

$\Leftrightarrow n \in \{\ \ , 0, 1\}$

Exo 4

a) Montrer que $6 \mid n(n+1)(n+2) \quad \forall n \in \mathbb{N}$

Si $6 \mid n(n+1)(n+2)$

alors $n(n+1)(n+2)$ est divisible à la fois par 2 et par 3

Montrons :

(*) $2 \mid n(n+1)(n+2)$ ↘

(**) $3 \mid n(n+1)(n+2)$ → vrai car nombres consécutifs

$n(n+1)(n+2) \equiv 0 \ [3]$

Soit $n \equiv 0 \ [3]$

alors $n = 3n'$ div □

$n \equiv 1 \ [3]$

alors $n+2 = 3n'$ div □

$n \equiv 2 \ [3]$ alors $n+1 = 3n'$ div □

de même manière

c) $24 \mid n(n+1)(n+2)(n+3)$

$\Leftrightarrow 8 \mid n(n+1)(n+2)(n+3)$

$3 \mid n(n+1)(n+2)(n+3)$ démontré par (a)

(*) $2 \mid n(n+1)$ → chacun est divisible par 2 au moins une fois

$2 \mid (n+2)(n+3)$ → et un 2 fois

donc 2 et 4 toujours divise, donc

(*) vrai

Or $\text{pgcd}(8,3) = 1$ donc $\text{ppcm}(8,3) = 24$

donc 24 divise $n(n+1)(n+2)(n+3)$

d) montrer que $\forall p \geq 1$ $p! \mid n(n+1)(n+2)(n+3)\dots(n+p-1)$

$$n(n+1)(n+2)\dots(n+p-1) = \frac{(n-1+p)!}{(n-1)!} = \binom{n-1+p}{p} \cdot p!$$

Donc divisible par $p!$

Exo 7

2) $2^{17} \equiv ? \mod 3$

$2 \equiv 2 \mod 3$

$\Leftrightarrow 2 \equiv -1 \mod 3$

$\Leftrightarrow 2^{17} \equiv (-1)^{17} \mod 3$

$\Leftrightarrow 2^{17} \equiv -1 \mod 3$

$\equiv 2 \mod 3$

6) $5^5 \equiv \; ? \; [7]$

$5 \equiv -2 \; [7]$

$5^5 \equiv (-2)^5 \; [7]$

$5^5 \equiv -32 \; [7]$

$5^5 \equiv -4 \; [7]$

$5^5 \equiv 3 \; [7]$

Exo 9

Soit $a \in \mathbb{Z}$ tq $a \equiv 7 \ [12]$

$\Leftrightarrow a = 12 \cdot k + 7$

$12k + 7 \equiv 1 \mod [3]$

$a \equiv ? \ [48]$ $\quad a = 12k + 7$

$4a \equiv 28 \ [48]$

$a \equiv 7 \ [48]$

$12 \cdot 0 + 7 = 7 \equiv 7 \ [48]$

$12 \cdot 1 + 7 = 19 \equiv 19 \ [48]$

$12 \cdot 2 + 7 = 24 + 7 = 31 \equiv 31 \ [48]$

$12 \cdot 3 + 7 = 43 \equiv 43 \ [48]$

$12 \cdot 4 + 7 \equiv 7 \ [48]$

$a = 12k + 7 \ [15]$

$12 \cdot 0 + 7 = 7 \equiv 7 \ [15]$

$12 \cdot 1 + 7 = 19 \equiv 4 \ [15]$

$12 \cdot 2 + 7 = 31 \equiv 1 \ [15]$

$a = 3k + 1$

$3 \cdot 0 + 1 = 1 \equiv 1 \ [15]$

$3 \cdot 1 + 1 = 4 \equiv 4 \ [15]$

$3 \cdot 2 + 1 = 7 \equiv 7 \ [7]$

$3 \cdot 3 + 1 = 10 \equiv 10 \ [10]$

$3 \cdot 4 + 1 = 13 \equiv 13 \ [13]$

$3 \cdot 5 + 1 = 16 \equiv 16 \ [16]$

Exercice 11

Soit $n \in \mathbb{Z}$

déterminer tous les reste possible pour

$n^2 \equiv \mod 8$

$n \equiv \{0, 1, 2, 3, 4, 5, 6, 7\} \ [8]$

$n^2 \equiv \{0, 1, 4\} \ [8]$

Supposons que $n \equiv 7 \ [8] \Leftrightarrow$

$n = \{a^2 + b^2 + c^2 \quad a, b, c \in \mathbb{R}\}$

$a^2, b^2, c^2 \in \{0, 1, 4\} \mod 8$

$0^2 + 0^2 + 0^2 = 0$

$0 + 0 + 1 = 1$

$0 + 0 + 4 = 4$

$0 + 1 + 4 = 5$

$1 + 1 + 4 = 6$

$1 + 1 + 1 = 3$

$1 + 4 + 4 = 9 \equiv 1$

$4 + 4 + 0 = 8 \equiv 0$

$1 + 1 + 0 = 2$

$4 + 4 + 4 = 12 \equiv 4 \mod 8$

Aucune possibilité pour 7

Thm: pour $n \geq 2$