Cours d'arithmétique

Marc Soret

Université de Tours, France

Leçon 0 : Rappels, fondements de l'arithmétique principe de récurrence et aperçu du programme

Plan de la leçon 0

Rappels des notions de base et domaines abordés ce semestre

- Définitions de $\mathbb{N}$ et principe de récurrence
- de $\mathbb{N}$ à $\mathbb{Z}$ puis à $\mathbb{Q}$ et au-delà
- *Nombres premiers*
- Equations *diophantiennes*
- *Congruences, puissances et racines*
- *Fonctions arithmétiques*
- Méthode *RSA* de cryptage inviolable (jusqu'ici) et implémentation en python

Biblio non exhaustive !!

1. Jean-Marie De Koninck et Armel Mercier *1001 problèmes en théorie des nombres* 1994
2. Jean-Marie De Koninck *Introduction à la théorie des nombres* 1994
3. J. Silverman *A friendly introduction to number theory* 2006
4. Wiki
5. ....
6. reference : théorie axiomatique des ensembles, Krivine, theorie des ensembles Bourbaki
7. Logicomix

Quelques propriétés des entiers "naturels" : $\mathbb{N}$

- 0 est un entier
- chaque entier x a un successeur : $x + 1$
- $\mathbb{N}$ est munie de 2 **opérations** : une addition $+$ et une multiplication $\cdot$
- d'une **relation d'ordre stricte** notée $<$ et d'une relation d'ordre au sens large notée $\leq$ (totales)
- Tout sous-ensemble de $\mathbb{N}$ a un **plus petit élément**
- **Principe de récurrence** :

- Soit $P(n)$ n'importe quelle propriété de (l'entier) n. Si $P(0)$ est vraie et si $\forall n (P(n) \implies P(n+1))$ est vraie alors $P(n)$ est vrai pour tout $n \in \mathbb{N}$
ou $P(x)$ une **variable propositionnelle**

Quelques propriétés des entiers "naturels" : $\mathbb{N}$

- 0 est un entier
- chaque entier x a un successeur : $x + 1$
- $\mathbb{N}$ est munie de 2 **opérations** : une addition $+$ et une multiplication $\cdot$
- d'une **relation d'ordre stricte** notée $<$ et d'une relation d'ordre au sens large notée $\leq$ (totales)
- Tout sous-ensemble de $\mathbb{N}$ a un **plus petit élément**
- **méthode de récurrence** :

- Soit $P(n)$ est une propriété de (l'entier) n. Si $P(0)$ est vraie et si $\forall n(P(n) \implies P(n+1))$ est vraie alors $P(n)$ est vrai pour tout ensemble fini de $\mathbb{N}$
ou $P(x)$ une **variable propositionnelle**

Définition axiomatique de $\mathbb{N}$ (Axiomes de Peano *)

1. $0 \in \mathbb{N}$
2. si x est dans $\mathbb{N}$ alors le successeur de x, noté $s(x)$ ($= x+1$) est dans $\mathbb{N}$
3. $s(x) = s(y)$ ssi $x = y$
4. 0 est le successeur d'aucun élément de $\mathbb{N}$ et tout autre élément $x \neq 0$ a un prédécesseur $\exists y : x = s(y)$ (et $y = x-1$).
5. Si $P(0)$ et $\forall n\ (P(n) \implies P(n+1))$ alors $\forall\ n \in \mathbb{N}\ P(n)$

Proposition. l'axiome 5 (pr. de récurrence) $\iff$ Tout sous-ensemble de $\mathbb{N}$ a un plus petit élément ($\mathbb{N}$ est bien ordonné)

$\Longleftarrow$

Preuve: Soit P tel que $P(0)$ et $\forall x(P(x) \implies P(x+1))$.
S'il existe un plus petit x_0 tel que $P(x_0)$ soit faux
$x_0 \neq 0$ par hypothèse.
Donc par l'axiome 4 x_0 a un prédécesseur $(x_0 - 1)$ Mais $P(x_0 - 1)$ est faux car sinon par l'hypothèse $P(x_0)$ serait vrai.
Donc x_0 ne serait pas le plus petit élément tq $P(x)$ soit faux.
contradiction.
Donc $P(x)$ est vrai pour tout x
ie le principe de récurrence est vrai.

$\mathbb{N}$ en théorie des ens. (Zemerlo Frankel)

$0 := \emptyset$
$1 := 0 \cup \{0\} = \{0\},$
$2 := 1 \cup \{1\} = \{0\} \cup \{1\} = \{0,1\},$
$3 := 2 \cup \{2\} = \{0,1\} \cup \{2\} = \{0,1,2\} \cdots\cdots\cdots$

Le *successeur* de x, $s(x)$ est défini par $s(x) = x \cup \{x\}$.

Une classe est *hériditaire* si elle comprend $\emptyset$ et le successeur de chacun de ses éléments.

Axiome de l'infini : il existe un ensemble hériditaire et le plus petit (= à l'intersection de tous les ens. hériditaires)est par définition $\mathbb{N}$.

De plus on a une relation d'ordre totale et d'ordre strict totale : $x \leq y \iff x \subset y \quad , x < y \iff x \in y$.

Dans la théorie ZF , le principe de récurrence n'est plus un axiome mais un théorème.

On peut aussi démontrer que tout sous-ensemble de $\mathbb{N}$ a un plus petit élément.

Le principe de récurrence est vrai sur $\mathbb{N}$

Preuve: Soit $P(x)$ une proposition et supposons que $P(0)$ et que $\forall x(P(x) \implies P(x+1))$
Soit $F = \{x : P(x)\}$.
F est héridtaire par définition
donc par l'axiome à l'infini, il contient $\mathbb{N}$;
donc $P(x)$ est vrai pour tout $x \in \mathbb{N}$.

On peut compter avec $\mathbb{N}$!

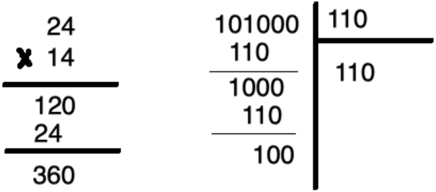
On définit une **rel. d'équivalence** sur les ensembles:
A "a même cardinal que" $B \iff$ il existe une bijection $A \leftrightarrow B$.
Une classe d'équivalence est appelé cardinal.
Un ensemble de cardinal n est en bijection avec l'ensemble n et a donc n éléments.
• $m + n$ est le cardinal de l'union disjointe d'un ensemble à m elements et d'un ensemble à n elements
• $m.n$ est le cardinal du produit cartesien d'un ensemble à m élements et d'un ensemble à n éléments

Représenter des entiers : numération de position

$n = [a_k a_2 \cdots a_0]_m \iff n = \sum_{l=0}^{k} a_l m^l$ où

$0 \leq a_i < m \quad \forall \quad i = 0, ..., k$

Exercice feuille trouvée sur le bureau d'un informaticien :



Traduire en base 10

De $\mathbb{N}$ à $\mathbb{Z}$

Diophante (Arithmétique : ~ 250 ?) : " .... un négatif multiplié par un négatif donne un positif tandis qu'un négatif par un positif donne un négatif et le signe négatif sera symbolisé par un ψ inversé ...Comme je viens de vous expliquer la multiplication, les puissances etc, ce serait une bonne chose pour le débutant de faire des exercices impliquant l'addition ou la soustraction et multiplication d'expressions algébriques, qui est positif qui est négatif ... "
Les nombres négatifs étaient utilisés par Diophante pour des calculs intermédiaires ou pour simplifier des expressions.
Remarque De même, le nombre "imaginaire" i a été introduit par Cardan pour simplifier l'expression algébrique des racines réelles d'équations cubiques $ax^3 + bx^2 + cx + d = 0$ (montrer qu'il en existe toujours au moins une racine réelle!)

De $\mathbb{N}$ à $\mathbb{Z}$

Comme Diophante, on introduit de nouveaux éléments à $\mathbb{N}$ en étendant les opérations d'addition et multiplication. Reste à tester la consistence de ces nouveaux objets.

• L'addition sur $\mathbb{N}$ est définie récursivement : pour tout x

$x + 0 := x$ et $x + s(y) := s(x + y)$.

(le principe de récurrence implique que $+$ est définie sur tout $\mathbb{N}$

Théorème Si $x \leq y$, il existe z tel que $y = x + z$

Definition :

$\mathbb{Z} := \mathbb{N}^* \cup \{0\} \cup (-\mathbb{N}^*)$ où l'addition et multiplication sont étendues à $\mathbb{Z}$ par :

Si $b \leq a$, $a + (-b) := c$ où $a = b + c$ (L' existence de c découle du théorème précédent).

Si $b > a$, $a + (-b) := -c$ où $a = b + c$.

$(-a) + (-b) := -(a + b)$

$a.(-b) := -(ab), (-a).(-b) := a.b$

On vérifie que $(\mathbb{Z}, +, .)$ est un **anneau commutatif**

de $\mathbb{Z}$ à $\mathbb{Q}$ et au-delà : des entiers exotiques

De la même façon on peut introduire de nouveaux éléments à $\mathbb{Z}$ et former de nouveaux ensembles dits **extensions** qui sont encore des anneaux .

1. $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\} \subset \mathbb{C}$: entiers de Gauss
2. $\mathbb{Z}[\sqrt{2}] = \{m + \sqrt{2}n : m, n \in \mathbb{Z}\} \subset \mathbb{R}$
3. $\mathbb{Z}[\sqrt{d}] = \{m + \sqrt{d}n : m, n \in \mathbb{Z}\} \subset \mathbb{R}$ d n'étant pas un carré : entiers quadratiques

ou de nouveaux **corps**

1. $\mathbb{Q} := \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}^*\}/\{\frac{a}{b} \equiv \frac{c}{d} \iff ad = bc\}$ où $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}, \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$
   (preferer la notation plus générale $a \cdot b^{-1}$ à $\frac{a}{b}$)
2. $\mathbb{Q}[i] = \{r + is : r, s \in \mathbb{Q}\} \subset \mathbb{R}$.
3. $\mathbb{Q}[\sqrt{d}] = \{m + \sqrt{d}n : m, n \in \mathbb{Q}\} \subset \mathbb{R}$ d n'étant pas un carré : corps quadratiques

Nombres premiers

Definition : un nombre est premier s'il n'est divisible que par un élément inversible ou lui-même.

• Décomposition "unique" dun entier en produit de facteurs premiers, **pgcd** et **algorithme d'Euclide** (performant) .
• Cribles et autres obtentions " non performantes" de nombres premiers (le plus grand premier connu d'après Wiki : $2^{82589933} - 1$ (combien de chiffres?)
• Premiers de Mersenne (de la forme précédente)
• Tests de **primalité** (Rabin-Miller) et construction de nombres **pseudo-premiers** (premiers avec une tres forte probabilité)
• nombres premiers et congruences

Nombres premiers : 2 conjectures célèbres

• Il existe une infinité de premiers p tels que $p+2$ est aussi premier (premiers jumeaux)
Il existe une infinité de premiers séparés d'au plus 7000000 Yitang Zhang 2013)
• Tout nombre pair est la somme de deux premiers (Goldbach)

Equations diophantiennes

Pb : trouver les solutions entières (sur $\mathbb{Z}$) d'équations algébriques

Des algorithmes des études de congruences ou des extensions nous permettront de résoudre

1. $ax + by = c$ et $a_1x_1 + \cdots a_nx_n = c$
2. Si $a_i \geq 0$ quel est le plus petit N pour lequel il n' a pas de solutions positives de $a_1x_1 + \cdots a_nx_n = N$ (problème des pièces de Frobenius)
3. $x^2 - dy^2 = 1$ (équation de Pell) , $x^2 + y^2 = z^2$
   $c = x^2 + y^2$ (quels sont les nombres c qui sont somme de deux carrés?)
4. $x^4 + y^4 = z^4$

exo : trouver $m, n > 0$ tels que $(m + n - 5)^2 = 9mn$

Une équation diophantienne par Diophante:

Pb : trouver x, y tels que $x^2 + y^2 = a^2$

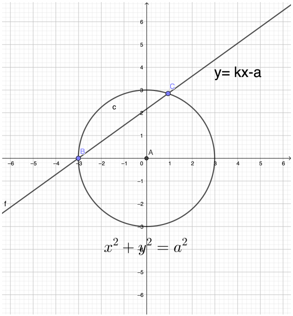
On remarque que $(0, -a)$ solution; on remplace y par $kx - a, k \in \mathbb{Q}$ et on résoud sur $\mathbb{Q}$

$a^2 = x^2 + (kx - a)^2 \implies ((1 + k^2)x - 2ka)x = 0$

$x = a\frac{2k}{1+k^2}, \implies y = a\frac{k^2-1}{1+k^2}, \quad k \in \mathbb{Q}$

Infinité de solutions entières de $x^2 + y^2 = z^2$

$x = 2ka, y = a(k^2 - 1), z = a(1 + k^2), k \in \mathbb{N}$



Résolutions de quelques équations **modulo m**

Définition $x \equiv y$ modulo m si. $x - y$ est divisible par m
relation d'équivalence

1. $ax + b \equiv c \mod m$
2. Système $\{ a_1 x \equiv b_1 \bmod m_1, \cdots, a_n x \equiv b_n \bmod m_n \}$
3. $x^2 \equiv c$ modulo p ?
4. Trouver des racines : $x^k \equiv a \mod m$ pour certains k, m $(a, m) = 1, (k, \phi(m)) = 1$

Application historique de 2: " On a un certain nombre de choses mais on ne sait pas combien exactement. Si nous les comptons par 3 il en reste 2. Si nous les comptons par 5 il en reste 3, si nous les comptons par 7 il en reste 2. Combien y-a-t-il de choses?" (Sun zi $\sim$ 300)
Bonne nouvelle: On a un algorithme performant de résolution de TOUTE équation algébrique modulo m!!

Fonctions arithmétiques

Définition Une fonction arithmétique est une fonction de $\mathbb{N}$ (ou $\mathbb{N}^*$) à valeurs dans un ensemble de nombres et telle que $\phi(1) = 1$.

Un exemple :l'indicatrice d'Euler

$\phi(m) := \{\text{le nombre d'entiers } 1 \leq k \leq m \text{ premiers avec } m\}$
$= .\#\{k \; : \; 0 \leq k \leq m : (k, m) = 1\}$

a	1	2	3	4	5	6	7	8	9	10
$\phi(a)$	1	1	2	2	4	2	6	4	6	4

Formules remarquables :

$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \sum_{d|n} \phi(d) = n$

Exposant remarquable :

si $(a, m) = 1$ alors $a^{\phi(m)} \equiv 1 \mod m$

Complexité des multiplications itérées mod m

Nombres pseudoaléatoires Pour de "bonnes" valeurs de m, a, c, s, on définit une suite de nombres semblant aléatoires récursivement:

$$u_0 = s, u_{n+1} \equiv a \cdot u_n + c \mod m$$

Générateur de nombres pseudoaléatoires x_0 = s, x_n = ax_{n-1}+c mod m Bon choix pour a, c, m????

Entrée [71]:
```
def nbrePseudAleatoire(a,c,m,s,n):
   maListe =[]
   for k in range(n):
       if k==0 : maListe.append(s)
       else :maListe.append((a*maListe[k-1]+c)%m)
   return maListe
def listeFormatee(l):
   if len(l)<20 : return l
   else:
       return [l[20*i:i*20  +20]  for i in range(int(len(l)/20)+1)]
```

Entrée [74]:
```
print(tabulate(listeFormatee(nbrePseudAleatoire(6,1,37,0,37))))
```

```
-  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
0  1  7  6  0  1  7  6  0  1  7  6  0  1  7  6  0  1  7  6
0  1  7  6  0  1  7  6  0  1  7  6  0  1  7  6  0
-  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
```

Entrée [75]:
```
print(tabulate(listeFormatee(nbrePseudAleatoire(5,1,37,0,37))))
```

```
--  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
 0   1   6  31   8   4  21  32  13  29  35  28  30   3  16   7  36  33  18  17
12  24  10  14  34  23   5  26  20  27  25  15   2  11  19  22   0
--  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
```

bonnes valeurs pour tester m= **231 -1** , **a = 75**

Elevation à une puissance mod m

#1 tableau des itérations de fonction puissances ; la ligne k correspond à l'élévation à la puissance k a --> a^k

Entrée [ ]:
```
nombres modulo 7 :
```

Entrée [76]:
```
print(tabulate(tableauPui(6,7)))
```

```
-  -  -  -  -  -
1  2  3  4  5  6
1  4  2  2  4  1
1  1  6  1  6  6
1  2  4  4  2  1
1  4  5  2  3  6
1  1  1  1  1  1
-  -  -  -  -  -
```

Entrée [ ]:
```
 Remarquer que tout nombre modulo 7 est égal à une puissance de 3; on dit que 3 est racine primitive modulo 7
    Remarquer aussi que a^6 est toujours égal à 1  modulo 7 ( petit théorème de Fermat)
```

Entrée [77]:
```
print(tabulate(tableauPui(7,8)))
```

```
-  -  -  -  -  -  -
1  2  3  4  5  6  7
1  4  1  0  1  4  1
1  0  3  0  5  0  7
1  0  1  0  1  0  1
1  0  3  0  5  0  7
1  0  1  0  1  0  1
1  0  3  0  5  0  7
-  -  -  -  -  -  -
```

... moins joli....

Méthode de cryptage RSA

• Description d' un algorithme de calcul des puissances sur un nombre de a^n modulo m dont le temps d'execution de est en $\log(n)$ (comme l'algorithme d'Euclide)
• RSA utilise cet algorithme pour chiffrer et déchiffer des messages Les codes ainsi obtenus sont incassables actuellement . Mais cela nécessite la construction de 2 nombres premiers d'une centaine de chiffres. Nous implémenterons en python la méthode de codage-décodage RSA avec avec un générateur de pseudo-premiers

Opérations

Définition : une opération $\star$ sur $\mathbb{N}$est une application

$$\star : \begin{pmatrix} \mathbb{N}\times\mathbb{N} & \to \mathbb{N} \\ (a,b) & \mapsto a\star b \end{pmatrix} \tag{1}$$

(notation infixe) $+$ et $\cdot$ sont des opérations sur $\mathbb{N}$.
$\cup$ et $\cap$ sont des opérations sur $\mathcal{P}(\mathbb{N})$
Propriétés : $\forall xyz$:

- commutativité
  $x\star y = y\star x$
- élément neutre pour $\star$
  $x\star e = x\forall x$
- distributivité de $\star/\circ$
  $x\star(y\circ z) = (x\star y)\circ(x\star z)$
- associativité :
  $(x\star y)\star z = x\star(y\star z)$

$\square$

Relations

Définition : une relation sur E est définie par un sous-ensemble $\Gamma \subset E \times E$ et en notation infixe : $x\mathcal{R}y$ ssi $(x, y) \in \Gamma$.
Définition : une relation d'ordre vérifie

1. $x\mathcal{R}x$ reflexivité
2. $x\mathcal{R}y$ et $y\mathcal{R}x$ alors $x = y$: anti-symétrie
3. $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$: transitivité

Exemples : $\leq$ est une relation d'ordre totale sur $\mathbb{N}$.
La relation "divise" notée $|$ sur $\mathbb{N}$
(et définie par : $a|b \iff \exists c \in \mathbb{N} : b = a \cdot c$) est une relation d'ordre partielle sur $\mathbb{N}$

$|$ est une relation d'ordre sur $\mathbb{N}$mais pas sur $\mathbb{Z}$

Etudions l'anti-symétrie:

Proposition: Si $d|d'$ et $d'|d$ alors $d' = ad$ avec a inversible

Proof.

$d|d' \implies \exists a : d' = ad$

$d'|d \implies \exists b : d = bd' \implies d' = abd' \implies$

$ab = 1$ ou $d = d' = 0$

Dans le cas 2. la prop. est vraie.

dans le premier cas a est inversible et $d' = ad$ avec a inversible $\square$

Montrons la transitivité de $|$:

Proof.

$d|d' \implies \exists a : d' = ad$

$d'|d" \implies \exists b : d" = bd' \implies d" = (ab)d \implies d|d"$

$\square$

Corollaire : $|$ est une relation d'ordre (au sens large) sur $\mathbb{N}$ (mais pas sur $\mathbb{Z}$

Relations d'ordre stricte

Définition : une relation d'ordre stricte vérifie

1. on a au plus une seule des 3 éventualités : $x\mathcal{R}y, y\mathcal{R}x, x = y$: anti-symétrie
2. $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$: transitivité

Exemples : $<$ est une relation d'ordre stricte (et totale) sur $\mathbb{N}$ $\square$

majorant, minorant, plus petit élément pour $(E, \leq)$ si existence et unicité

Définition : m est un minorant $E \subset \mathbb{N}$ si $\forall y \in E \quad m \leq y$
Définition : M est un majorant $E \subset \mathbb{N}$ si $\forall y \in E \quad y \leq M$
Définition : x est le plus petit élément de $E \subset \mathbb{N}$ (ou minimum) si
$x \in E$ et $\forall y \in E \quad x \leq y$
Définition : le plus grand des minorant est l'infimum (dit inf) de E dans $\mathbb{N}$
Définition : le plus petit des majorants est le supremum (dit sup) de E dans $\mathbb{N}$
Exemples : • Soit $E := \{1/n\}_{n \in \mathbb{N}^*} \subset \mathbb{Q}$ n' a pas de minimum mais $\inf_{\mathbb{Q}} E = 0$
• 0 (resp. 1)est le maximum (resp. minimum) de $\mathbb{N}$ pour la relation |
Exercice: montrer que sur $(\mathbb{N}, |)$ $\inf_{\mathbb{N}}\{12, 18\} = 6$ et $\sup_{\mathbb{N}}\{12, 18\} = 36$ $\square$

Rappels terminologie en logique

Définition : P est une proposition logique si elle est vraie ou fausse

Exemples ou contre-exemples:

• 2 est impair

• $2 - 3$

• il y a une infinité de nombres premiers x tels que x+2 soit aussi premier

•$\forall x \exists y \exists z \exists t \exists u \quad x = y^2 + z^2 + t^2 + u^2$

• Quels sont les nombres qui sont sommes de deux carrés?

• $\exists x \quad : x + y = 0$

Définition : $P(x)$ est une variable propositionnelle si par substitution de la variable x par un entier , la proposition devient logique

Exemples :

• $4|5^n - 1$; $n^2 - 1 = (n-1)(n+1) \cdots$ $\square$

Logique et théorie des ensembles

Toute proposition logique "définit" un ensemble et réciproquement : $F := \{x : P(x)\} \quad x \in F \iff P(x)$

Correspondance entre opérateurs logiques et opérations sur les ensembles; par exemple :

$F \cap G = \{x \ : \ x \in F \quad \text{et} \quad x \in G\}$

$F \cup G = \{x \ : \ x \in F \quad \text{ou} \quad x \in G\}$

relation d'ordre : $F \subset G$ ssi $\forall x \ (x \in F \implies x \in G)$

On peut donc donner une version ensembliste de la récurrence. $\square$

Logique et théorie des ensembles

Toute proposition logique "définit" un ensemble et réciproquement : $F := \{x : P(x)\} \quad x \in F \iff P(x)$

Correspondance entre opérateurs logiques et opérations sur les ensembles; par exemple :

$F \cap G = \{x \ : \ x \in F \quad \text{et} \quad x \in G\}$

$F \cup G = \{x \ : \ x \in F \quad \text{ou} \quad x \in G\}$

relation d'ordre : $F \subset G$ ssi $\forall x \ (x \in F \implies x \in G)$

On peut donc donner une version ensembliste de la récurrence. $\square$

démonstration de la méthode de récurrence dans le cas fini

Proposition Soit $N \in \mathbb{N}$

Si $\quad P(0) \quad$ et $\quad \forall n \, (P(n) \implies P(n{+}1)) \quad$ alors $\quad \forall n \leq \; N \; P(n)$

Preuve :
Comme $P(0)$ et comme $(P(0) \implies P(1))$ alors $\quad P(1)$
Comme $P(1)$ et comme $(P(1) \implies P(2))$ alors $\quad P(2)$
$\dots$
Si $P(n_0 - 1)$ et $(P(n_0 - 1) \implies P(n_0))$ alors $\quad P(n_0)$
Donc $(P(0)$ et $P(1)$ et $\cdots \mathrm{P}(\mathrm{n}_0))$
On a démontré que : $\forall n \leq n_0 . P(n)$ $\square$

Variantes équivalentes du principe de recurrence

1. Si $P(0)$ et si $\forall x(P(x) \implies P(x+1))$ alors $\forall x \in \mathbb{N} \quad P(x)$
2. si $P(x_0)$ et si $\forall x(P(x) \implies P(x+1))$ alors $\forall x \geq x_0 \quad P(x)$ $\square$
3. Si E est un sous-ensemble de $\mathbb{N}$ tel que $0 \in E$ et tel que $x \in E \implies x+1 \in E$ alors $E = \mathbb{N}$
4. si $P(0)$ et si $(\forall m \leq n \ P(m)) \implies P(n+1)$ alors $\forall x \quad P(x)$ $\square$
5. si $P(0), P(1), \cdots P(k)$ et si $(\forall m : n-k \leq m \leq n \ P(m)) \implies P(n+1)$ alors $\forall x \quad P(x)$

Il existe d'autres énoncés en rapport qui sont "équivalents"

1. Tout sous-ensemble **non vide** de $\mathbb{N}$ a un plus petit élément
2. Méthode de la descente infinie de Fermat

Descente infinie d'après Euclide

On ne peut pas trouver d'entiers (> 0) tels que $b^2 = 2a^2$: supposons que de tels entiers existent;

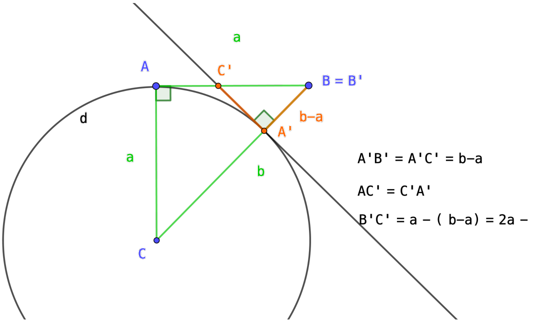


Figure: $\triangle(a, a, b) \mapsto \triangle(b - a, b - a, 2a - b) = \triangle(a', a', b')$

$\square$

La méthode de récurrence dans la pratique : Elle permet :

- de bien définir les suites ou fonctions récursivement :

Exemples:

∘ $covid(0) = 1, covid(n+1) = covid(n).R_0$

∘ Lapins de Fibonacci $u_1 = 1, u_2 = 1, u_n = u_{n-1} + u_{n-2}$

- de démontrer des formules par héridité :

$\forall n \quad covid(n) = R_0^n$ et $\forall n \quad u_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$

- $covid(n) = R_0^n \implies covid(n+1) = R_0^{n+1}$

- $u_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$ et

$u_{n+1} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \implies$

$u_{n+2} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+2}$ $\square$

Récursivité en informatique

Le principe de récurrence assure que les fonctions suivantes sont respectivement définies sur $\mathbb{N}$ et sur $\mathbb{N} \times \mathbb{N}$

```
def fact(x):
    if x==0 : return 1
    return x *fact(x-1)
def quiSuisJe(x,y):
    if y==0 : return x
    return quiSuisJe(y, x%y)
def fibo(x):
    if x==0 : return 1
    elif  x==1: return 1
    return  fibo(x-1)+fibo(x-2)
```

Remarque 1: la récurrence semble descendante

Remarque 2: definition 3 à eviter

Récursivité qques exos Démontrer que :

1. $\forall\, n \quad 4|5^n - 1$
2. $\forall\, n > 3 \quad 2^n \leq n!$
3. le principe des tiroirs I : si $n+1$ chaussettes sont dans n tiroirs alors un tiroir contient au moins 2 chaussettes
4. le principe des tiroirs II : si n chaussettes sont dans m tiroirs avec $m < n$ alors un tiroir contient au moins 2 chaussettes

$\square$

Relations d'équivalence

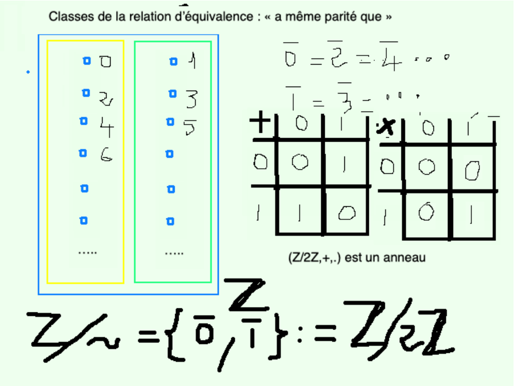
Définition : une relation d'équivalence est caractérisée par

1. $x\mathcal{R}x$ reflexivité
2. $x\mathcal{R}y$ ssi $y\mathcal{R}x$:symétrie
3. $x\mathcal{R}y$ et. $y\mathcal{R}z$ alors $y\mathcal{R}z$: transitivité

Exemples :
• $=$ est une relation d'équivalence (sur $\mathbb{N}$)
• la relation "a même parité que" ou $x \equiv y$ mod 2
• Plus généralement $x \equiv y$ mod m ssi x et y divisés par m ont même reste

Remarque Une relation d'équivalence sur $E \iff$ une partition de $E = \bigcup_{i \in . I} A_i$
et $x\mathcal{R}y$ ssi x et y appartiennent à une " même classe " A_i $\square$

la relation d'équivalence $x \equiv y \bmod 2$ et opérations sur les classes



Equivalence des variantes I

$1 \implies 2$:On pose $Q(n) = P(n_O + n)$
$P(n_0)$ et $\forall n \geq n_0 (P(n) \implies P(n+1))$ devient
$Q(0)$ et $\forall n \geq 0 (Q(n) \implies Q(n+1))$.
Donc du principe de récurrence nous déduisons : $\forall n \; Q(n)$
C'est à dire
$\forall \; n \; \geq n_0 \; P(n)$
$1 \implies 4$: On pose $Q(n) = (\forall l \leq n \; P(l))$
$P(0)$ et si $(\forall m \leq n \; P(m)) \implies P(n+1)$ devient
$Q(0)$ et $(Q(n) \implies Q(n+1))$.
Donc du principe de récurrence nous déduisons : $\forall n Q(n)$
C'est à dire $\forall n \; P(n)$

$\square$