Quelques notions d'Arithmétique (plan de travail)

H. Le Ferrand

25 novembre 2017

Table des matières

1 Raisonnement par récurrence

Nous allons nous placer dans les ensembles $\mathbb{N}$ et $\mathbb{Z}$. Si un sous-ensemble A de $\mathbb{N}$ contient 0 et si le **successeur** de tout élément de A est dans A, on va dire que $A = \mathbb{N}$. Ceci est en fait un des axiomes de Peano [1] qui définissent en quelque sorte l'ensemble $\mathbb{N}$. Rappelons le principe suivant dit *principe d'induction* :

Soit une propriété $P(n)$ (soit vraie, soit fausse) si

(a) $P(0)$ est vraie ;

(b) si $P(n)$ est vraie alors $P(n+1)$ vraie,

on a $P(n)$ vraie pour tout $n \in \mathbb{N}$.

Il faut noter deux difficultés :

— il faut avoir une idée de ce que l'on veut prouver !

— le passage « si $P(n)$ est vraie alors $P(n+1)$ vraie » peut être réellement difficile à établir.

A titre d'exemple étudions la somme des cubes des n premiers entiers naturels. On commencera par faire un tableau indiquant dans deux colonnes, pour les premiers entiers n, les sommes $\sum_{k=1}^{n} k$ et $\sum_{k=1}^{n} k^3$.

2 Division euclidienne. Congruences

2.1 Division euclidienne

Soient a et b deux entiers, on dit que b divise a si a est de la forme bq, $q \in \mathbb{Z}$. L'Arithmétique sur $\mathbb{Z}$ est fondée sur le résultat fondamental suivant :

Théorème 2.1 Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}$ non nul, il existe un unique couple (q, r) d'entiers vérifiant :

$$a = bq + r,\ 0 \leq r < b \text{ (ou } r \in [[0; b-1]]). \tag{1}$$

On dit que $a = bq + r$ est la **division euclidienne de a par b**, que q est le quotient et r le reste. Par exemple la division euclidienne de 125 par 13 est :

$$125 = 13 \times 9 + 8. \tag{2}$$

2.2 Congruences

On fixe un entier $n \geq 2$. L'idée de ce qui suit est que l'on ne veut plus distinguer deux entiers dont les restes dans la division par n sont égaux. On dit que a et b (des entiers) sont **congrus modulo** n si $a - b$ est divisible par n. On écrit alors :

$$a \equiv b \pmod{n}.$$

1. Giuseppe Peano(1858-1932), mathématicien italien.

Remarquons déjà que $a \equiv b \pmod{n}$ si et seulement si a et b ont même reste dans la division euclidienne par n. En effet, il suffit de voir que si $a = nq + r$, $b = nq' + r'$, avec $r \in [[0; n-1]]$ et $r \in [[0; n-1]]$, n divise $a - b$ si et seulement si n divise $r - r'$. Or $r - r'$ appartient à $[[-(n-1); n-1]]$, ce qui permet de conclure. Choisissons par exemple $n = 5$. Un entier naturel va donc être congru modulo 5 à un entier (et un seul) de l'ensemble $0, 1, 2, 3, 4$. On forme ainsi une **partition de l'ensemble** $\mathbb{Z}$.

On peut mener des calculs sur les congruences. On a en effet :

Théorème 2.2 Si $a \equiv b \pmod{n}$, si $c \equiv d \pmod{n}$ et si k est un entier naturel, alors :

$$a + c \equiv b + d \pmod{n},\ ac \equiv bd \pmod{n},\ a^k \equiv b^k \pmod{n}. \tag{3}$$

Calculons par exemple 2^{21} modulo 37. (réponse : $2^{21} \equiv 29 \pmod{37}$.)

Si n est un entier déterminons l'entier r tel que $7^n \equiv r \pmod{8}$. On peut raisonner à partir de $7 \equiv -1 \pmod{8}$ ou de $7^2 \equiv 1 \pmod{8}$.

On peut aussi obtenir facilement certains critères de divisibilité. Par exemple un entier naturel est divisible par 9 si la somme de ses chiffres est divisible par 9. En effet, partant du fait que $10 \equiv 1 \pmod{9}$, on a pour tout entier naturel k, $10^k \equiv 1 \pmod{9}$.

3 Algorithme d'Euclide. Relation de Bézout

3.1 Algorithme d'Euclide et gcd

Si a et b sont deux entiers naturels, l'ensemble de leurs diviseurs communs possède un plus grand élément. On le nomme **le plus grand diviseur commun de** a **et** b et on le notera $\gcd(a, b)$. Par exemple, l'ensemble des diviseurs communs à 14 et 21 est

$$\{1, 2, 7, 14\} \cap \{1, 3, 7, 21\} = \{1, 7\}, \tag{4}$$

donc $\gcd(14, 21) = 7$.

Pour l'instant, rien ne nous dit qu'un diviseur commun à a et à b divise $\gcd(a, b)$.

On dira que a et b sont **premiers entre-eux** si $gcd(a, b) = 1$.

On a va voir à présent une méthode efficace pour calculer le $gcd(a, b)$ pour $a > b > 0$. Il s'agit du célèbre **algorithme d'Euclide**.

Quel est le « moteur » de cet algorithme ? Remarquons que si l'on effectue la division euclidienne de a par b, $a = bq + r$ avec $r \in [[0; b-1]]$, alors :

$$\gcd(a, b) = \gcd(b, r). \tag{5}$$

Ainsi pour calculer $\gcd(a, b)$ on effectue des divisions euclidiennes successives et $\gcd(a, b)$ sera le dernier reste non nul (la suite des reste étant une suite d'entiers naturels strictement décroissantes).

Mettons en oeuvre cet algorithme pour calculer $\gcd(17, 11)$, puis $\gcd(600, 124)$.

3.2 Identité de Bézout

Si a et b sont deux entiers, on peut en utilisant une **méthode de remontée** dans l'algorithme trouver une relation linéaire entre a, b et $\gcd(a, b)$. Précisement, on a :

Théorème 3.1 Soit a et b deux entiers, il existe un couple $(u, v) \in \mathbb{Z} \times \mathbb{Z}$, non nécessairement unique, tel que :

$$au + bv = \gcd(a, b). \tag{6}$$

L'égalité (6) est appelée **indentité de Bézout** [2]. On a $\gcd(600, 124) = 4$, déterminons u et v tels que $600u + 124v = 4$.

Comme conséquences du théorème précédent, on a :

1. Si d divise a et b, d divise $\gcd(a, b)$.
2. Les entiers a et b sont premiers entre-eux ($\gcd(a, b) = 1$) si et seulement si il existe deux entiers u et v tels que $au + bv = 1$.
3. Si $d = gcd(a, b)$, alors $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.
4. Si a divise le produit bc et si $\gcd(a, b) = 1$ alors a divise c (lemme de Gauss).

Le lemme de Gauss permet de trouver tous les couples (u, v) tels que $au + bv = \gcd(a, b)$. Par exemple, $\gcd(16, 10) = 2$ et $16 \times 2 - 10 \times 3 = 2$. Ainsi on a :

$$\begin{aligned} 16u + 10v &= 2 && (7)\\ 16u + 10v &= 16 \times 2 + 10 \times (-3) && (8)\\ 16(u - 2) &= -10(v + 3) && (9)\\ 8(u - 2) &= -5(v + 3). && (10) \end{aligned}$$

Or $\gcd(8, 5) = 1$ donc 5 divise $u - 2$, etc.

2. Etienne Bézout (1730-1783), mathématicien français.