7- Arithmétique des nombres entiers

Jean-François Culus
26 / 05 / 2017

Plan (Déclic TS)

Cours

- Divisibilité
  Applications: Congruences
- Nombres premiers
- PGCD
  Nombres premiers entre eux
  Applications

Algorithmes

- Division euclidienne dans N, Z
- Crible d'Eratostène
  Test de primalité
- Calcul du PGCD
  Coefficients de Bezout
-

I. Multiples, diviseurs, division euclidienne

Soient a et b deux entiers relatifs, avec b non nul.

- Def: On dit que b divise a s'il existe un entier relatif k tel que a=bk.
  On dit que b est un diviseur de a ou que a est un multiple de b.
- Conséquences:
  Tout entier divise 0
  Si a non nul, alors 1, -1, a et –a sont des diviseurs de a.

- Propriété: Soient a, b et c trois entiers relatifs non nuls.
  - Si c divise b et b divise a, alors c divise a.
  - Si a divise b et b divise a, alors a=b ou a=-b.
  - Si c|a et c|b, alors c|(a+b), c| (a-b)
    et c | (au+bv) où u et v sont des entiers quelconque.

Démontration

- Théorème: Division euclidienne dans N
  Pour tout entier naturel a et pour tout entier naturel non nul b, il existe un unique couple (q,r) d'entiers naturels tel que
  $a=bq+r$ et $0 \leq r < b$.

Démontration Algorithme

- Théorème: Division euclidienne dans Z
  Pour tout couple d'entiers relatifs a et b avec b non nul, il existe un unique couple (q,r) d'entiers relatifs tel que
  $a= bq+r$ et $0\ 0 \leq r < |b|$.

- Proposition: Lien divisibilité / division euclidienne
  a est divisible par b si et seulement si le reste de la division euclidienne de a par b est nul.

Démontration

Application: Congruences

On désigne par n un entier $n \geq 2$.

- Définition: Soient a et b deux entiers relatifs. On dit que a est congru à b modulo n (noté $a \equiv b \bmod(n)$) si a et b ont même reste dans la division euclidienne par n.

- Propriétés:
  $a \equiv b \bmod(n)$ si et seulement si $n \mid (b-a)$.
  $a \equiv 0 \bmod(n)$ si et seulement si $n \mid a$.
  Si $a \equiv b \bmod(n)$ et $b \equiv c \bmod(n)$ alors $a \equiv c \bmod(n)$

  Démontration

- Théorème: Compatibilité des opérations algébriques avec la relation de congruence
  Si $a \equiv b \bmod(n)$ et $c \equiv d \bmod(n)$ alors $a+c \equiv b+d \bmod(n)$
  $a\,c \equiv b\,d \bmod(n)$

  Démontration

- Corollaire:
  Si $a \equiv b \bmod(n)$ alors $a + k \equiv b + k \bmod(n)$
  $a\,k \equiv b\,k \bmod(n)$
  $a^k \equiv b^k \bmod(n)$

II. Nombres premiers

- Définition: Un entier naturel n est dit premier s'il admet exactement deux diviseurs dans N: 1 et lui-même.
- Exemples: 2,3,5,7 sont des nombres premiers
  1,4,6,8,9 et 10 ne sont pas premiers.

Algorithme

- Propriété: n est premier si et seulement si n n'a pas de diviseur premier inférieur ou égal à $\sqrt{n}$
- Propriété: Tout entier naturel ≥ 2 admet un diviseur premier.

- Crible d’Eratosthène

  Algorithme

- Proposition: L’ensemble des nombres premiers est infini.

  Démontration

- Théorème: Décomposition en produit de facteurs premiers

Tout entier naturel $n \geq 2$ s'écrit de manière unique (à l'ordre des facteurs près) comme produit de nombres premiers, ie.

$n = p_1^{a1} p_2^{a2} \ldots p_k^{ak}$ ou les p_i sont des nombres premiers et ai des entiers naturels non nuls.

Démontration

III. PGCD

- Définition: Soient a et b deux entiers relatifs dont au moins l'un est non nul. Alors l'ensemble des diviseurs communs de a et b admet un plus grand élément. On appelle plus grand commun diviseur de a et b celui-ci, noté PGCD(a,b).

- PGCD(a,0)=a PGCD(a,1)=1 PGCD(a,a)=|a|
  Si b | a alors PGCD(a,b)=|b|

- Si k>0, PGCD(ka,kb)=k PGCD(a,b)

- Définition: On dit que les entiers a et b sont premiers entre eux si PGCD(a,b)=1.
- Proposition: Si D=PCGD(a,b) alors $\frac{a}{D}$ et $\frac{b}{D}$ sont premiers entre eux
- Théorème de Bezout
  Soient a et b deux entiers relatifs et D=pgcd(a,b)
  Alors il existe deux entiers relatifs u,v tels que au+bv=D.

  Démontration
- Identité de Bezout
  a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que au+bv=1.

  Démontration

- Théorème de Gauss:
  Soient a,b et c trois entiers relatifs non nuls.
  Si a|bc et PGCD(a,b)=1, alors a|c.

  Démontration

- Application: Equation diophantienne / Cryptographie