Arithmétique

Divisibilité dans $\mathbb{Z}$.

Soient a et b deux entiers relatifs, b étant non nul. On dit que b divise a si et seulement si il existe un entier relatif k tel que a=kb. La phrase « a divise b » se note a|b.

Propriétés.

• Pour tout entier relatif non nul a, a|a.
• Pour tous entiers relatifs non nuls a, b et c, si a|b et b|c alors a|c.
• Soient a, b et c trois entiers relatifs, a étant non nul. Si a|b et a|c, alors pour tous entiers relatifs λ et μ, a|(λb+μc).

Division euclidienne dans $\mathbb{Z}$.

Soient a et b deux entiers naturels, b étant non nul. Il existe un couple (q, r) d'entiers naturels et un seul tel que a = bq + r et r < b≤q est le quotient et r le reste de la division euclidienne de a par b.

Congruences dans $\mathbb{Z}$.

Soit n un entier naturel supérieur ou égal à 2. Soient a et b deux entiers relatifs. On dit que a est congru à b modulo n si et seulement si b – a est divisible par n. On écrit dans ce cas a≡ b (n) ou a ≡ b (modulo n).

Propriétés.

Soit n un entier relatif supérieur ou égal à 2.
• Pour tout entier relatif a, a ≡ a (n).
• Pour tous entiers relatifs a et b, si a ≡ b (n) alors b ≡ a (n).
• Pour tous entiers relatifs a, b et c, si a ≡ b (n) et b ≡ c (n) alors a ≡ c (n).
• (Compatibilité avec l'addition) Pour tous entiers relatifs a, b et c, si a ≡ b (n) alors a + c ≡ b + c (n).
• (Compatibilité avec la multiplication) Pour tous entiers relatifs a, b et c, si a ≡ b (n) alors a × c ≡ b × c (n).

Nombres premiers.

Décomposition en facteurs premiers.

Soit n un entier supérieur ou égal à 2, n est premier si et seulement si n admet exactement deux diviseurs à savoir 1 et n. Il existe une infinité de nombres premiers.

Théorème fondamental de l'arithmétique.

Tout entier naturel supérieur ou égal à 2 se décompose en produit de nombres premiers. Cette décomposition est unique à l'ordre près des facteurs.

PPCM, PGCD.

Soient a et b deux entiers naturels supérieurs ou égaux à 2.

On suppose que $a = p_1^{\alpha 1} \times p_2^{\alpha 2} \times \cdots \times p_n^{\alpha n}$, $b = p_1^{\beta 1} \times p_2^{\beta 2} \times \cdots \times p_n^{\beta n}$ avec $p_1 < p_2 < \cdots < p_n$ où $p_1, \ldots, p_k$ sont k nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_k$ sont des entiers naturels.

On note m_1 le plus petit des deux nombres α_1 et β_1 et M_1 le plus grand. On note m_2 le plus petit des deux nombres α2 et β2 et M2 le plus grand. . . Le PGCD (plus grand commun diviseur) de a et b est p_1^{m1} 1. . . p_k^{mk} K et le PPCM (plus petit commun multiple) de a et b est p_1^{M1}. . . p_k^{Mk}.

Exemple. $48 = 2^4 \times 3$ et $36 = 2^2 \times 3^2$. Donc PGCD(36, 48) = $2^2 \times 3 = 12$ et PPCM(36, 48) = $2^4 \times 3^2 = 144$.

$\forall (a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$, PPCM(a , b) = $PPCM\ (|a|, |b|)$

$\forall (a, b) \in IN^* \times IN^*$, PPCM(a , b) = a ⟺⇒ a ∈ b $\mathbb{Z}$

$\forall (a, b) \in IN^* \times IN^*$, max(a, b) ⩽ PPCM(a , b) ⩽ a × b

Soit (a, b) ∈ $IN^* \times IN^*$, et μ = PPCM(a , b) On a ; a $\mathbb{Z}$ ∩ b $\mathbb{Z}$ = μ $\mathbb{Z}$

$\forall (a, b, k) \in (IN^*)^3$, PPCM(k × a , k × b) = k × PPCM(a , b)

Pour tout couple (a, b) ∈ $\mathbb{Z}^* \times \mathbb{Z}^*$, on a : PGCD(a , b) × PPCM(a , b) = |a| × |b|,

Si a et b sont premiers entre eux, alors $PPCM\ (a, b) = PPCM\ (|a|, |b|)$

Algorithme d'Euclide.

On a le résultat préliminaire suivant : si a et b sont deux entiers naturels non nuls tels que b < a et si a = bq + r où q et r sont deux entiers naturels tels que 0 ≤ r < b, alors PGCD(a, b)=PGCD(b,r).

On veut maintenant le PGCD de a et de b.

On pose la division euclidienne de a par b. Si r = 0, le PGCD de a et de b est r0 = r.

Sinon, on pose la division euclidienne de b par $r_0 = r$: b = qr + r_1 avec $0 \le r_1 < r_0$. Si $r_1 = 0$ le PGCD de b et de r_0 est r_0 et donc le PGCD de a et de b est r_0.

Sinon, on pose la division euclidienne de r_0 par r_1. . .

Cet algorithme s'arrête quand on trouve un reste nul, ce qui se produit toujours. Le PGCD de a et b est le dernier reste non nul.

Théorème de Bézout.

Soient a et b deux entiers relatifs non nuls.

a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que au +bv=1.

Théorème de Gauss.

Soient a, b et c trois entiers relatifs, a et b étant non nuls.

Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Anneau ($\mathbb{Z}$ /n $\mathbb{Z}$,+,×)

On dit qu'un anneau commutatif A est intègre si et seulement si ∀x ∈A, ∀y ∈A; x × y = 0 ⇒ x = 0 ou y = 0 .

Soit (n, p) ∈ IN, Si n ⩾ 2 et 1 < p < n, p est inversible dans $\mathbb{Z}$ /n $\mathbb{Z}$ ⟺⇒ PGCD(n, p) = 1

Soit a, b, c ∈ $\mathbb{Z}$. S'il existe u ∈ $\mathbb{Z}$ tel que ua ≡ 1 [n] alors ab ≡ ac [n] ⇒ b ≡ c [n]

Soit a ∈ $\mathbb{Z}$. Il existe u ∈ $\mathbb{Z}$ tel que au ≡ 1 [n] si et seulement si PGCD(a , n) = 1 , c'est-à-dire a et n sont premiers entre eux.