7. Arithmétique

7.1 Opération sur les multiples

Théorème 1 : Soit trois entiers relatifs a, b et c.

Si a divise b et c alors a divise $b + c$, $b - c$ ou toute combinaison linéaire de b et de c.

Démonstration : On sait que a divise b et c, donc il existe deux entiers relatifs k et k' tels que :

$$b = ka \quad \text{et} \quad c = k'a$$

On a alors :

$$b + c = (k + k')a \quad , \quad b - c = (k - k')a \quad \text{et} \quad \alpha b + \beta c = (\alpha k + \beta k')a$$

Donc a divise $b + c$, $b - c$ et $\alpha b + \beta c$

7.2 Compatibilité avec la congruence

Théorème 2 : Soit n un entier naturel ($n \geqslant 2$), a, b, c, d des entiers relatifs vérifiant :

$$a \equiv b\ (n) \quad \text{et} \quad c \equiv d\ (n)$$

La congruence est compatible :

1. avec l'addition :
$$a + c \equiv b + d\ (n)$$
2. avec la multiplication :
$$ac \equiv bd\ (n)$$
3. avec les puissances :
$$\forall\, k \in \mathbb{N} \quad a^k \equiv b^k\ (n)$$

Démonstration :

1. Compatibilité avec l'addition.
On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc $(a - b)$ et $(c - d)$ sont des multiples de n. Il existe donc deux entiers relatifs k et k' tels que :
$$a - b = kn \quad \text{et} \quad c - d = k'n$$
En additionnant ces deux égalités, on obtient :
$$a - b + c - d = kn + k'n$$
$$(a + c) - (b + d) = (k + k')n$$
Donc $(a + c) - (b - d)$ est un multiple de n, donc d'après le théorème 2, on obtient :
$$a + c \equiv b + d\ (n)$$
2. La compatibilité avec la multiplication.
On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc, il existe deux entiers relatifs k et k' tels que :
$$a = b + kn \quad \text{et} \quad c = d + k'n$$
En multipliant ces deux égalités, on obtient :
$$ac = (b + kn)(d + k'n)$$
$$ac = bd + k'bn + kdn + kk'n^2$$
$$ac = bd + (k'b + kd + kk'n)n$$
$$ac - bd = (k'b + kd + kk'n)n$$
Donc $(ac - bd)$ est un multiple de n, donc d'après le théorème 2, on a :
$$ac \equiv bd\ (n)$$
3. Compatibilité avec les puissances.
On prouve cette compatibilité par récurrence sur k, à l'aide de la compatibilité avec la multiplication.

7.3 Le théorème de Bezout

Théorème 3 : Égalité de Bezout

Soit a et b deux entiers non nuls et $D = PGCD(a, b)$
Il existe alors un couple (u, v) d'entiers relatifs tels que :

$$au + bv = D$$

Ce théorème est admis

Théorème 4 : Théorème de Bezout

Deux entiers relatifs a et b sont premiers entre eux **si et seulement si**, il existe deux entiers relatifs u et v tels que :

$$au + bv = 1$$

Démonstration :

Dans le sens $\Rightarrow$: Immédiat grâce à l'égalite de Bezout.

Dans le sens $\Leftarrow$:
On suppose qu'il existe deux entiers u et v tels que : $au + bv = 1$.
Si $D = PGCD(a, b)$ alors D divise a et b donc D divise $au + bv$.
Donc D divise 1. On a bien $D = 1$.

Théorème 5 : Corollaire du théorème de Bezout

L'équation $ax + by = c$ admet des solutions entières **si et seulement si** c est un multiple du $PGCD(a, b)$.

Démonstration :

Dans le sens $\Rightarrow$
$ax + by = c$ admet une solution (x_0, y_0).
Comme $D = PGCD(a, b)$ divise a et b il divise $ax_0 + by_0$.
D divise donc c

Dans le sens $\Leftarrow$
c est un multiple de $D = PGCD(a, b)$.
Donc il existe un entier relatif k tel que : $c = kd$
De l'égalité de Bezout, il existe deux entiers relatifs u et v tels que :

$$au + bv = D$$

En multipliant par k, on obtient :

$$auk + bvk = kD \Leftrightarrow a(uk) + b(vk) = c$$

Donc il existe $x_0 = uk$ et $y_0 = vk$ tels que $ax_0 + by_0 = c$

7.4 Le théorème de Gauss

Théorème 6 : Soit a, b et c trois entiers relatifs non nuls.
Si a divise le produit bc et si a et b sont premiers entre eux alors a divise c.

Démonstration :

Si a divise le produit bc, alors il existe un entier k tel que :

$$bc = ka$$

Si a et b sont premiers entre eux, d'après le théorème de Bezout, il existe deux entiers u et v tels que :

$$au + bv = 1$$

En multiplient par c, on a :

$$\begin{aligned} acu + bcv &= c \qquad \text{or } bc = ka \text{, donc :} \\ acu + kav &= c \\ a(cu + kv) &= c \end{aligned}$$

Donc a divise c.

Propriété 1 : Soit a, b et c trois entiers non nuls.
Si b et c divise a et si b et c sont premiers entre eux alors bc divise a

Démonstration : Si b et c divise a, il existe $(k, k') \in \mathbb{Z}^2$ tel que : $a = kb = k'c$

c divise donc kb et comme b et c sont premiers entre eux, d'après le théorème de Gauss, c divise k.

Il existe donc $k'' \in \mathbb{Z}$ tel que : $k = k''c$. On a alors : $a = k''bc$. bc divise alors a.

7.5 Infinité des nombres premiers

Théorème 7 : Il existe une infinité de nombres premiers

Démonstration : Supposons qu'il existe un nombre fini de nombres premiers : p_1, p_2,…, p_i, …, p_n.

Posons $N = p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n + 1$

D'après le critère d'arrêt, N admet un diviseur premier. Soit p_i ce diviseur premier.
p_i divise $p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n$ et N.
Il divise donc la différence $N - (p_1 \times p_2 \times \cdots \times p_i \times \cdots \times p_n) = 1$.
Ceci est impossible, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est absurde.