26

Utilisation des congruences et des anneaux $\mathbb{Z}/n\mathbb{Z}$

26.1 Équations diophantiennes $ax \equiv b\ (n)$

Soient n un entier supérieur ou égal à 2, a un entier supérieur ou égal à 1 et b un entier relatif. On veut résoudre dans $\mathbb{Z}$ l'équation diophantienne :

$$ax \equiv b\ (n) \tag{26.1}$$

Dans le cas où $b = 1$, cette équation a des solutions si, et seulement si $\overline{a}$ est inversible dans $\mathbb{Z}_n$, ce qui équivaut à dire que a est premier avec n. Dans ce cas l'algorithme d'Euclide nous permet de trouver une solution $x_0 \in \mathbb{Z}$ de (26.1). Si $x \in \mathbb{Z}$ est une autre solution, alors $a(x - x_0)$ est divisible par n qui est premier avec a et le théorème de Gauss nous dit que n doit diviser $x - x_0$. Réciproquement on vérifie facilement que pour tout $k \in \mathbb{Z}$, $x_0 + kn$ est solution de (26.1). En définitive, dans le cas où a et n sont premiers entre eux, l'ensemble des solutions de $ax \equiv 1\ (n)$ est :

$$S = \{x_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Dans le cas où les entiers a et n sont premiers entre eux et b est un entier relatif quelconque, pour toute solution particulière u_0 de l'équation $ax \equiv 1\ (n)$ l'entier $x_0 = bu_0$ est solution de (26.1). Comme précédemment, on en déduit que l'ensemble des solutions de (26.1) est :

$$S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Considérons maintenant le cas général.

On note δ le pgcd de a et n et on a $a = \delta a'$, $n = \delta n'$ avec a' et n' premiers entre eux.

Théorème 26.1 *L'équation diophantienne* (26.1) *a des solutions entières si, et seulement si, δ divise b. Dans ce cas, l'ensemble des solutions de cette équation est :*

$$S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$$

où x'_0 est une solution particulière de $a'x \equiv 1$ modulo n'

Démonstration. Si l'équation (26.1) admet une solution $x \in \mathbb{Z}$ alors $\delta n'$ divise $\delta a' - b$ et δ divise b.

Si b est un multiple de δ, il s'écrit $b = \delta b'$ et toute solution de $a'x \equiv b' \ (n')$ est aussi solution de (26.1) .

On a vu que les solutions de $a'x \equiv b' \ (n')$ sont de la forme $x = b'x'_0 + kn'$ où x'_0 est une solution de $a'x \equiv 1 \ (n')$ et k est un entier relatif. Réciproquement on vérifie facilement que pour tout entier $k \in \mathbb{Z}$, $x = b'x'_0 + kn'$ est solution de (26.1) . ∎

26.2 Équations diophantiennes $x \equiv a \ (n)$, $x \equiv b \ (m)$

On s'intéresse ici aux système d'équations diophantiennes :

$$\begin{cases} x \equiv a \ (n) \\ x \equiv b \ (m) \end{cases} \tag{26.2}$$

où n, m sont deux entiers naturels supérieur ou égal à 2.

Théorème 26.2 (chinois) *Soient n, m deux entier supérieur ou égal à 2 premiers entre eux. Quels que soient les entiers relatifs a et b le système* (26.2) *a une infinité de solutions dans $\mathbb{Z}$.*

Démonstration. Comme n et m sont premiers entre eux on peut trouver une infinité de couples d'entiers relatifs (u, v) tels que :

$$nu + mv = 1.$$

En posant $x = bnu + amv$ on obtient une infinité de solutions de (26.2) . ∎

Ce théorème peut aussi s'exprimer en disant que le morphisme d'anneaux introduit dans la démonstration du théorème 25.11, $\varphi : k \mapsto \left(\dot{k}, \ddot{k}\right)$, est surjectif de $\mathbb{Z}$ dans $\mathbb{Z}_n \times \mathbb{Z}_m$. Son noyau étant $nm\mathbb{Z}$, on retrouve l'isomorphisme de $\mathbb{Z}_{nm}$ sur $\mathbb{Z}_n \times \mathbb{Z}_m$.

Dans le cas où n et m sont premiers entre eux on vient de voir que si (u_0, v_0) est solution de $nu + mv = 1$ (un tel couple peut être obtenu par l'algorithme d'Euclide) alors $x_0 = bnu_0 + amv_0$ est une solution particulière de (26.2) . À partir d'une telle solution on déduit toutes les autres. En effet, si $x \in \mathbb{Z}$ est solution de (26.2) alors x est congru à x_0 modulo n et modulo m, soit :

$$x - x_0 = pn = qm.$$

Mais m est premier avec n, le théorème de Gauss nous dit alors que m divise p. On a donc $x = x_0 + knm$ avec $k \in \mathbb{Z}$. Et réciproquement on vérifie que pour tout entier relatif k, $x_0 + knm$ est solution de (26.2) . En définitive, si n et m sont premiers entre eux, alors l'ensemble des solutions de (26.2) est :

$$S = \{x_0 + knm \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (26.2) .

Dans le cas général où m et n ne sont pas nécessairement premiers entre eux on note δ le pgcd de n et m, $n = \delta n'$, $m = \delta m'$ avec n', m' premiers entre eux et on note μ le ppcm de n et m.

Théorème 26.3 *L'équation diophantienne* (26.2) *a des solutions entières si, et seulement si, $a - b$ est multiple de δ. Dans ce cas, l'ensemble des solutions de* (26.2) *est :*

$$S = \{x_0 + k\mu \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Démonstration. Si $x \in \mathbb{Z}$ est une solution de (26.2) alors δ qui divise n et m va diviser $x-a$ et $x-b$, il divise donc $a-b$.

Réciproquement, supposons que $a-b$ est multiple de δ, c'est à dire que $b-a=\delta c'$. Les entiers n' et m' étant premiers entre eux, le théorème de Bézout nous dit qu'il existe des entiers u_0 et v_0 tels que $n'u_0+m'v_0=1$. En posant :

$$x_0 = bn'u_0 + am'v_0,$$

on a :

$$\begin{aligned} x_0 &= b\,(1-m'v_0) + am'v_0 = b - m'v_0\,(b-a) \\ &= b - m'v_0\delta c' = b - mv_0c' \equiv b \ (m)\,. \end{aligned}$$

De manière analogue on voit que x_0 est congru à a modulo n. L'entier x_0 est donc une solution de (26.2) .

Si $x \in \mathbb{Z}$ est solution de (26.2) alors x est congru à x_0 modulo n et modulo m, soit :

$$x - x_0 = pn = qm = p\delta n' = q\delta m'.$$

Il en résulte que $\dfrac{x-x_0}{\delta}$ est un entier et :

$$\frac{x-x_0}{\delta} = pn' = qm'.$$

Comme m' est premier avec n', le théorème de Gauss nous dit que m' doit diviser p. On a donc :

$$\frac{x-x_0}{\delta} = kn'm'$$

avec $k \in \mathbb{Z}$. Ce qui peut aussi s'écrire :

$$x - x_0 = knm' = k\frac{nm}{\delta} = k\mu$$

avec $k \in \mathbb{Z}$.

Réciproquement on vérifie facilement que pour tout entier relatif k, $x_0 + k\mu$ est solution de (26.2) . En définitive, l'ensemble des solutions de (26.2) est :

$$S = \{x_0 + k\mu \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation. ■

26.3 Critères de divisibilité

Les anneaux $\mathbb{Z}/n\mathbb{Z}$ peuvent être utilisés pour obtenir des critères de divisibilité des entiers par $2, 3, 5, 9$ et 11.

Soit a un entier naturel non nul d'écriture décimale $a = \overline{a_p \cdots a_1 a_0}^{10}$, où les a_k sont des entiers compris entre 0 et 9, le coefficient a_p étant non nul.

– Comme 10 est congru à 0 modulo 2 (resp. modulo 5) on déduit que a est congru à a_0 modulo 2 (resp. modulo 5) et donc a est divisible par 2 (resp. par 5) si et seulement si son chiffre des unités a_0 est pair, c'est-à-dire égal à $0, 2, 4, 6$ ou 8 (resp. multiple de 5, c'est-à-dire égal à 0 où 5).

- Du fait que 10 est congru à 1 modulo 3 (resp. modulo 9) on déduit que 10^k est congru à 1 modulo 3 (resp. modulo 9) pour tout entier k et a est congru à $\sum_{k=0}^{p} a_k$ modulo 3 (resp. modulo 9). Donc a est divisible par 3 (resp. par 9) si et seulement si la somme de ses chiffres est divisible par 3 (resp. par 9).
- Enfin du fait que 10 est congru à -1 modulo 11 on déduit que 10^k est congru à $(-1)^k$ modulo 11 pour tout entier k et a est congru à $\sum_{k=0}^{p} (-1)^k a_k$ modulo 11. Donc a est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

En remplaçant 10 par une base $b \geq 2$, on a de manière plus générale les résultats suivants, où on a noté $a = \overline{a_p \cdots a_1 a_0}^b$ l'écriture en base b d'un entier a (les a_k sont compris entre 0 et $b-1$ et a_p est non nul) :

- si d est un diviseur de b alors a est divisible par d si, et seulement si a_0 est divisible par d :
- si d est un diviseur de $b-1$ alors a est divisible par d si, et seulement si $\sum_{k=0}^{p} a_k$ est divisible par d ;
- a est divisible par $b+1$ si, et seulement si $\sum_{k=0}^{p} (-1)^k a_k$ est divisible par $b+1$.