Congruences

Résolution de l'équation diophantienne $Ay + Bzy = N$, avec $A, B, N \in \mathbb{Z}$.

1ère étape : Existence de solutions. On effectue l'algorithme d'Euclide pour calculer $\mathrm{pgcd}(A, B)$. Il est clair que si $Ay + Bz = N$ avec A, B, y, z, N entiers, alors $\mathrm{pgcd}(A, B)$ divise N. Donc si $\mathrm{pgcd}(A, B)$ ne divise pas N, il n'y a pas de solution.

2ème étape : Solution particulière. Soit $d = \mathrm{pgcd}(A, B)$ et $A'd = A$, $B'd = B$ et $N'd = N$. Alors $N'y + B'z = N'$. On remonte l'algorithme d'Euclide pour calculer les coefficients de Bézout. Soient donc s et t deux entiers relatifs avec $As + Bt = d$, et $AsN' + BtN' = dN' = N$. Ainsi $(y_0, z_0) = (sN', tN')$ est une solution particulière.

3ème étape : Solution générale. Si (y, z) est une solution quelconque, alors

$$A'(y - y_0) + B'(z - z_0) = (A'y + B'z) - (A'y_0 + B'z_0) = N' - N' = 0.$$

Ainsi $A'(y - y_0) = -B'(z - z_0)$, d'où $A' \mid -B'(z - z_0)$ et $A' \mid B'(y - y_0)$. Puisque $\mathrm{pgcd}(A', B') = 1$, d'après le lemme de Gauss $A' \mid z - z_0$ et $B' \mid y - y_0$. Soit k entier tel que $A'k = z - z_0$. Alors

$$-B'(z - z_0)k = A'(y - y_0)k = A'k(y - y_0) = (z - z_0)\,(y - y_0)$$

et $y - y_0 = -B'k$. On a donc $y = y_0 - B'k$ et $z = z_0 + A'k$. Réciproquement, il est facile que pour tout entier $k \in \mathbb{Z}$,

$$A(y_0 - B'k) + B(z_0 + A'k) = Ay_0 + Bz_0 - A'dB'k + B'dA'k = N.$$

Ainsi l'ensemble des solutions est $\{(y_0 - B'k, z_0 + A'k) : k \in \mathbb{Z}\}$.

Attention, il faut bien travailler avec a' et b' pour trouver l'ensemble des solutions.

Résolution de la congruence $ax \equiv b \mod n$, pour $a, b, n \in \mathbb{Z}$, $n \geq 2$.

$ax \equiv b \mod n$ si et seulement s'il y a $y \in \mathbb{Z}$ avec $ax - b = ny$, c'est à dire $ax + (-n)y = b$. On se retrouve avec une équation diophantienne, avec $A = a$, $B = -n$ et $N = b$. En particulier, si $\mathrm{pgcd}(a, n)$ ne divise pas b, il n'y a pas de solution.

On ne s'intéresse qu'a la première coordonnée x de la solution de l'équation diophantienne.

Résolution du système de conguences $x \equiv a \mod n$ et $x \equiv b \mod k$, avec $a, b, n, k \in \mathbb{Z}$, $n, k \geq 2$.

Le système est équivalent à l'existence de $y, z \in \mathbb{Z}$ avec $x - a = yn$ et $x - b = zk$. Ainsi

$$ny + a = x = kz + b.$$

Alors $ny + (-k)z = b - a$ est notre équation diophantienne, avec $A = n$, $B = -k$ et $N = b - a$. En particulier, si $\mathrm{pgcd}(n, k)$ ne divise pas $b - a$ il n'y a pas de solution. Si on a une solution (y_0, z_0) de l'équation diophantienne, alors $x_0 = y_0 n + a$ est une solution de notre système de congruences. Maintenant si x est une autre solution, alors $x - x_0 \equiv a - a = 0 \mod n$ et $x - x_0 \equiv b - b = 0 \mod k$, donc $n | x - x_0$ et $k | x - x_0$. Cela signifie que $\mathrm{ppcm}(n, k) | x - x_0$ et $x = x_0 + \ell \mathrm{ppcm}(n, k)$, avec $\ell \in \mathbb{Z}$. On rappelle que $\mathrm{ppcm}(n, k) = |n \cdot k| / \mathrm{pgcd}(n, k)$.