Congruences

Résolution de l'équation diophantienne $ax + by = n$.

On effectue l'algorithme d'Euclide pour calculer $\text{pgcd}(a, b)$. Il est clair que si $ax + by = n$ avec a, b, x, y, n entiers, alors $\text{pgcd}(a, b)$ divise n. Donc si $\text{pgcd}(a, b)$ ne divise pas n, il n'y a pas de solution.

Sinon, soit $d = \text{pgcd}(a, b)$ et $a'd = a$, $b'd = b$ et $n'd = n$. Alors $a'x + b'y = n'$. 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 $(x_0, y_0) = (sn', tn')$ est une solution particulière.

Maintenant, si (x, y) est une solution quelconque, alors

$$a'(x - x_0) + b'(y - y_0) = (a'x + b'y) - (a'x_0 + b'y_0) = n' - n' = 0.$$

Ainsi $a'(x - x_0) = -b'(y - y_0)$, d'où $a' \mid -b(y - y_0)$ et $b' \mid a(x - x_0)$. Puisque $\text{pgcd}(a', b') = 1$, d'après le lemme de Gauss $a' \mid y - y_0$ et $b' \mid x - x_0$. Soit k entier tel que $a'k = y - y_0$. Alors

$$-b'(y - y_0)k = a'(x - x_0)k = a'k(x - x_0) = (y - y_0)\,(x - x_0)$$

et $x - x_0 = -b'k$. On a donc $x = x_0 - b'k$ et $y = y_0 + a'k$. Réciproquement, il est facile que pour tout entier $k \in \mathbb{Z}$,

$$a(x_0 - b'k) + b(y_0 + a'k) = ax_0 + by_0 - a'db'k + b'da'k = n.$$

Ainsi l'ensemble des solutions est $\{(x_0 - b'k, y_0 + b'k) : k \in \mathbb{Z}\}$.

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

Résolution de la congruence $ax \equiv b \mod n$.

Soir $d = \text{pgcd}(a, n)$. Si $ax \equiv b \mod n$, alors $n \mid ax - b$ et il y a un entier k tel que $nk = ax - b$, soit $b = ax - nk$. Ainsi $d \mid ax - nk = b$; si $\text{pgcd}(a, n)$ ne divise pas b, il n'y a pas de solution.

Sinon, il y a un entier b' avec $b = b'd$. D'après le théorème de Bézout il y a des entiers s, t tels que $as + nt = d$. Alors

$$asb' - b = (as - d)b' = -nt$$

et $asb' \equiv b \mod n$. Ainsi $x_0 = sb'$ est une solution particulière.

Soit x une solution quelconque de la congruence. Alors

$$a(x - x_0) \equiv b - b = 0 \mod n.$$

Il y a donc un entier k tel que $a(x - x_0) = kn$. Soient a', n' des entiers avec $a = a'd$ et $n = n'd$. Alors $a'(x - x_0) = n'k$. Puisque $\text{pgcd}(a', n') = 1$, d'après le lemme de Gauss, $n' \mid x - x_0$, et il y a un entier ℓ avec $n'\ell = x - x_0$. Réciproquement, on a

$$a(x_0 + n'\ell) = ax_0 + a'dn'\ell \equiv b + 0 = b \mod n.$$

L'ensemble des solutions est donc $\{x_0 + n'\ell : \ell \in \mathbb{Z}\}$.

Attention, il faut bien travailler avec n' pour trouver l'ensemble des solutions.

Résolution du système de conguences $x \equiv a \mod n$ et $x \equiv b \mod k$.

Soit $d = \text{pgcd}(n, k)$. Si x est une solution du système, il y a des entiers ℓ, m avec $x - a = \ell n$ et $x - b = mk$. Ainsi $a - b = (x - b) - (x - a) = mk - \ell n$, et $d \mid a - b$. Donc si $\text{pgcd}(n, k)$ ne divise pas $a - b$, il n'y a pas de solution.

Sinon, soit $a - b = dc$, et $n = dn'$, $k = k'd$. D'après le théorème de Bézout il y a des entiers s, t avec $sn + tk = d$. Ainsi $sn' + tk' = 1$. On pose $x_0 = bsn' + atk'$. Alors

$$x_0 = atk' + b(1 - tk') = (a - b)tk' + b = cdtk' + b = ctk + b \equiv b \mod k,$$
$$x_0 = a(1 - sn') + bsn' = a - (a - b)sn' = a - cdtn' = a - ctn \equiv a \mod n.$$

Donc x_0 est une solution particulière.

Si x est une solution quelconque, on a $x - x_0 \equiv a - a = 0 \mod n$ et $x - x_0 \equiv b - b = 0 \mod k$. Donc $a \mid x - x_0$ et $b \mid x - x_0$. Soit $D = \text{ppcm}(n, k)$. Alors $\mid x - x_0$, et $x = x_0 + \ell D$ pour un $\ell \in \mathbb{Z}$. Réciproquement, on voit facilement que $x_0 + \ell D \equiv a + 0 = a \mod n$ et $x_0 + \ell D \equiv b + 0 = b \mod k$. Ainsi l'ensemble des solutions est $\{x_0 + \ell\text{ppcm}(n, k) : \ell \in \mathbb{Z}\}$.

On rappelle que $\text{ppcm}(n, k) = nk/\text{pgcd}(n, k) = nk/d$.