RUNSER Laura — Maths 4 · Amphi 4 — 17.02.2021

I/ Congruences

Def : Soient $a, b \in \mathbb{Z}$ et $n > 1$ un entier.

On dit que a est congru à b modulo n si n divise $b-a$

Prop :

1) $a \equiv a \mod n$
2) Si $a \equiv b \mod n$ alors $b \equiv a \mod n$
3) Si $a \equiv b \mod n$ et $b \equiv c \mod n$ alors $a \equiv c \mod n$
4) Si k divise n et $a \equiv b \mod n$ alors $a \equiv b \mod k$

Prop : Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ $\quad (n \neq 0)$

1) $a + c \equiv b + d\ [n]$
2) $a - c \equiv b - d\ [n]$
3) $ac \equiv bd\ [n]$
4) $a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n]$

⚠ $2 \times 3 \equiv 0\ [6]$

↳ il n'y a pas forcément un terme nul dans un produit qui donne 0.

$ab \equiv ac\ [n] \not\Rightarrow b \equiv c\ [n]$

Théorème

Soient $a, b, n \in \mathbb{Z}$, $n \neq 0$, a et n 1ers entre eux

Alors il existe une solution à $ax \equiv b\ [n]$ et cette solution est unique modulo n.

Prop : Soient $a, b \in \mathbb{Z}$, $n > 1$ et $d = \text{PGCD}(a, n)$

$ax \equiv b\ [n]$

a des solutions <u>ssi</u> $d \mid b$ et dans ce cas, les solutions sont les mêmes que celles de l'équation

$a'x \equiv b'\ [n']$ avec $a' = a/d$, $b' = b/d$, $n' = n/d$

Théorème des restes chinois

Soient $m, n \in \mathbb{Z}$ non nuls et premiers entre eux.
Soient $a, b \in \mathbb{Z}$ quelconques

Soient $u, v \in \mathbb{Z}$ tq $um + vn = 1$ (existent d'après Bezout)

Alors $x = bum + avn$ est la solution du système $\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$

et cette solution est unique modulo mn.