Arithmétique

Chapitre 1

I. Divisibilité

$\boxed{a|b \Leftrightarrow b = ka}$
$a|b \text{ et } b|c \Rightarrow a|c$
$a|b \text{ et } a|c \Rightarrow a|kb + k'c$
$a|b \Leftrightarrow ac|bc$

<u>Division euclidenne de a par b :</u>
$\exists!\ (q,r) \in \mathbb{N}^2, a = bq + r, 0 \leq r < b$

II. Congruences

$\boxed{a \equiv b\ [n] \Leftrightarrow n|a - b}$
$a \equiv b\ [n] \text{ et } c \equiv d\ [n] \Rightarrow a + c \equiv b + d\ [n]$
$a \equiv b\ [n] \text{ et } c \equiv d\ [n] \Rightarrow ac \equiv bd\ [n]$
$a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n]$

III. Critères de divisibilité

$2|N \Leftrightarrow a_0 \equiv 0\ [2]$
$5|N \Leftrightarrow a_0 \equiv 0\ [5]$

$4|N \Leftrightarrow \overline{a_1 a_0} \equiv 0\ [4]$
$25|N \Leftrightarrow \overline{a_1 a_0} \equiv 0\ [25]$

$3|N \Leftrightarrow$ somme des chiffres $\equiv 0\ [3]$
$9|N \Leftrightarrow$ somme des chiffres $\equiv 0\ [9]$

$11|N \Leftrightarrow$ somme alternées des chiffres $\equiv 0\ [11]$

IV. PGCD et PPCM

$\boxed{d = a \wedge b \Rightarrow d|a \text{ et } d|b}$
$k|d \Leftrightarrow k|a \text{ et } k|b$
$\boxed{(a \wedge b)(a \vee b) = ab}$

<u>Théorème d'Euclide :</u>
$a \wedge b = b \wedge r$

<u>Théorème de Bézout :</u>
$a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2, au + bv = 1$

<u>Théorème de Gauss :</u>
$\boxed{a|bc \text{ et } a \wedge b = 1, a|c}$
$a|n \text{ et } b|n \text{ et } a \wedge b = 1 \Rightarrow ab|n$

$$\boxed{d = a \wedge b \Leftrightarrow \left[\begin{array}{l} d|a \\ d|b \\ \dfrac{a}{d} \wedge \dfrac{b}{d} = 1 \end{array}\right. \Leftrightarrow \left[\begin{array}{l} d|a \\ d|b \\ \exists (u,v) \in \mathbb{Z}^2, au + bv = d \end{array}\right.}$$

V. Équation diophantiennes

$$\boxed{ax + by = c} \quad (d = a \wedge b)$$

Cette équation admet une solution si c = kd (d|c)

Si c = 1 :

- On trouve une solution particulière (x_0, y_0) *(Bézout)*
- $a(x - x_0) + b(y - y_0) = 0$ *(par différence entre l'équation et celle avec la sol part)*
- Résolution :

$a \mid b(y - y_0)$	$b \mid a(x - x_0)$
$a \mid y - y_0$	$b \mid x - x_0$
$\boxed{y = ak + y_0}$	$\boxed{x = bk' + x_0}$

- On remplace pour trouver un lien entre k et k'

Si c = d : (d ≠ 1)

- Résoudre comme au-dessus avec l'équation $\frac{a}{d}x + \frac{b}{d}y = 1$

Si c = kd : (d et k ≠ 1)

- $ax + by = c \Leftrightarrow \frac{a}{d}x + \frac{b}{d}y = k$
- On trouve une solution particulière de l'équation $\frac{a}{d}x + \frac{b}{d}y = 1$ (u, v) *(Bézout)*
  La solution particulière de l'équation est donc (x_0, y_0) avec $\boxed{x_0 = ku}$ et $\boxed{y_0 = kv}$
- Puis on résout simplement comme au-dessus

VI. Nombres premiers

Soit p un nombre premier

$p \mid ab \Rightarrow p \mid a$ ou $p \mid b$

Petit théorème de Fermat :
p premier, a pas multiple de p
$\boxed{a^{p-1} \equiv 1\ [p]}$

Corollaire :
Si p premier
$\boxed{a^p - a \equiv 0\ [p]}$