Arithmétique dans $\mathbf{Z}$

Division euclidienne
Pour $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$, il existe un unique couple $(q, r) \in \mathbf{Z}^2$ tel que

$$a = bq + r \text{ avec } r \in [\![0, b-1]\!].$$

Divisibilité : $d|a \iff a \in d\mathbf{Z}$.

1. $|$ est une relation d'ordre partielle sur $\mathbf{N}$ (mais pas sur $\mathbf{Z}$).
2. $d|a$ et $d|b \Rightarrow d|au + bv$ pour tous entiers u et v.
3. $d|a$ et $d|a' \Rightarrow dd'|aa'$.
4. $d|a$ et $k \in \mathbf{N} \Rightarrow k|a^k$.

PGCD :

1. $a \wedge b$ est le plus grand diviseur commun à a et b.
   - au sens de $\leqslant$ dans $\mathbf{Z}$,
   - au sens de $|$ dans $\mathbf{N}$.
2. $d|a$ et $d|b \iff d|a \wedge b$.
3. $\frac{a}{a\wedge b} \wedge \frac{b}{a\wedge b} = 1$.
4. si $a = bq + r$, alors $a \wedge b = b \wedge r$.
5. (*égalité de Bezout*) il existe $(u_1, u_2, \cdots, u_n) \in \mathbf{Z}^n$ tel que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$.
6. *homogénéité :* pour $k \neq 0$, $(ka_1) \wedge (ka_2) \wedge \cdots \wedge (ka_n) = |k|\,(a_1 \wedge a_2 \wedge \cdots \wedge a_n)$.

PPCM :

1. $a \wedge b$ est le plus petit multiple commun positif à a et b.
   - au sens de $\leqslant$ dans $\mathbf{Z}$,
   - au sens de $|$ dans $\mathbf{N}$.
2. $a|m$ et $b|m \iff a \vee b|m$.
3. *homogénéité :* pour $k \neq 0$, $(ka) \vee (kb) = |k|(a \vee b)$.

Lien PPCM - PGCD : $(a \wedge b)\,(a \vee b) = ab$.

Entiers premiers entre eux : $a \wedge b = 1$.
Théorème de Bezout : (réciproque fausse pour $a \wedge b \neq 1$)

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbf{Z}^2,\ au + bv = 1.$$

Lemme de Gauss : $a|bc$ et $a \wedge b = 1 \Rightarrow a|c$.
Entiers premiers entre eux deux à deux : $\forall i \neq j,\ a_i \wedge a_j = 1$.
Entiers premiers entre eux dans leur ensemble : $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$.

1. Si pour tout $i \in [\![1, k]\!]$, $a_i \wedge n = 1$, alors $a_1a_2 \cdots a_k \wedge n = 1$.
2. Si $\forall i \in [\![1, k]\!]$, $a_i|n$, et si les a_i sont premiers entre eux **deux à deux**, alors $a_1a_2 \cdots a_k|n$.

Nombres premiers : $p \geqslant 2$ premier s'il admet exactement deux diviseurs : 1 et p.
Si p premier, alors $p|ab \Rightarrow p|a$ ou $p|b$.

Théorème fondamental de l'arithmétique :
$\forall a \in \mathbf{N}^*$, a se décompose de manière unique comme produit de facteurs premiers.

$$a = \prod_{k=1}^{n} p_k^{\alpha_k} = \prod_{p \in \mathcal{P}} p^{v_p(a)}.$$

$v_p(a)$ est la valuation p-adique de a.

- $v_p(ab) = v_p(a) + v_p(b)$.
- $a|b \iff \forall p \in \mathcal{P},\ v_p(a) \leqslant v_p(b)$.
- $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.
- $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Relation de congruence $a \equiv b\ [n] \iff a - b \in n\mathbf{Z} \iff (\exists q \in \mathbf{Z},\ a = nq + b)$.

1. $\equiv\ [n]$ est une relation d'équivalence sur $\mathbf{Z}$.
   Ses classes d'équivalences sont $\{r + n\mathbf{Z},\ r \in [\![0, n-1]\!]\}$.
2. Un nombre est congru à son reste modulo n.
3. La congruence est compatible avec la somme et le produit.
   - Si $a \equiv r_1\ [n]$ et $b \equiv r_2\ [n]$, alors $a + b \equiv r_1 + r_2\ [n]$.
   - Si $a \equiv r_1\ [n]$ et $b \equiv r_2\ [n]$, alors $ab \equiv r_1r_2\ [n]$.
   - Si $a \equiv r_1\ [n]$ et $k \in \mathbf{N}$, alors $a^k \equiv r_1^k\ [n]$.

Petit théorème de Fermat : Soit $p \in \mathcal{P}$, $a \in \mathbf{Z}$, $a^p \equiv a\ [p]$.
Et si a n'est pas divisible par p, alors $a^{p-1} \equiv 1\ [p]$.