CHAPITRE 5

Théorie des nombres

5.1 Division euclidienne

Théorème 1. Théorème — Division euclidienne
Soient $a, b \in \mathbb{Z}$, $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r, \qquad 0 \leq r \leq |b| - 1.$$

L'entier naturel r ainsi obtenu est appelé *le reste de la division euclidienne* de a par b.

— **Divisibilité :** b divise a s'il existe un entier b tel que $a = bq$, i.e. le reste est 0.

Exercice 5.1.
- Trouver tous les entiers ≥ 1 tels que $\dfrac{n^3+3}{n^2+7}$ soit un entier.
- Soient a et b deux entiers. Montrer qu'on a : $a - b \mid a^n - b^n$ et $a + b \mid a^n + b^n$ si n est impair.

Nombres premiers

Définition 1. Soit $p \geq 2$ un entier. Le nombre entier p est *premier* si ses seuls diviseurs positifs sont 1 et p.
Un entier $n \geq 2$ est dit *composé* (non premier) si $n = ab$ avec $a \geq 2$ et $b \geq 2$.

Fait 1. Tout entier $n \geq 2$ admet un diviseur premier.

Fait 2. Si p premier, $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Fait 3. Théorème fondamental de l'arithmétique
Tout entier supérieur ou égal à 2 peut être représenté comme produit de facteurs de nombres premiers, de manière unique.

Exercice 5.2.
- Montrer qu'un nombre premier supérieur à 3 est de la forme $6n \pm 1$.
- Soient a et b deux entiers. Montrer que $a^4 + 4b^4$ n'est pas un nombre premier (pour $a, b > 1$).

5.2 PGCD et PPCM

D'après les **Fait 1**, **Fait 3** et l'un des principes extrémaux, les définitions suivantes ont un sens :

Définition 2. Soient a et b deux entiers tels que $(a, b) \neq (0, 0)$. Le plus grand des diviseurs positifs communs à a et b existe et sera noté par $\text{PGCD}(a, b)$. Tandis que le plus petit des multiples communs à a et b sera noté par $\text{PPCM}(a, b)$. En particulier, si $\text{PGCD}(a, b) = 1$, on dit dans ce cas que a et b sont premiers entre eux.

Fait 4. $\text{PGCD}(a, b) = \text{PGCD}(b,\ a - b) = \text{PGCD}(b,\ r)$ où $a = bq + r$.

Fait 5. $|ab| = \text{PGCD}(a, b) \cdot \text{PPCM}(a, b)$.

Fait 6. *Théorème de Bézout*
Soient a et b deux entiers non tous nuls. Alors, ils existent deux entiers x et y tels que $\text{PGCD}(a, b) = ax + by$.
En particulier, si a et b sont premiers entre eux si et seulement si on a : $ax + by = 1$.

Exercice 5.3.

- Soient n un entier. Calculer $\text{PGCD}(5n+2,\ 12n+5)$ et $\text{PGCD}(9n + 4,\ 2n - 1)$.

- Soient a et b deux entiers non tous nuls. Supposons qu'ils existent trois entiers c, x et y tels que $c = ax + by$. Alors, on a : $\text{PGCD}(a, b)$ divise c.

5.3 Congruences

Définition 3. Soit $n \in \mathbb{N}^*$. Considérons deux entiers a et b. On dit que a et b sont congrus modulo n (noté $a \equiv b \pmod{n}$) si a et b admettent le même reste après division euclidienne par n.

Fait 7. Si $\text{PGCD}(c, n) = 1$ et $ca \equiv cb \pmod{n}$, alors $a \equiv b \pmod{n}$.

Fait 8. Soit f un polynôme à coefficients dans $\mathbb{Z}$. Si $a \equiv b \pmod{n}$, alors $f(a) \equiv f(b) \pmod{n}$.

Fait 9. *Petit théorème de Fermat*
Soient a un entier et p premier, on a :

$$a^p \equiv a \pmod{p}.$$

Exercice 5.4.
- Montrer que l'équation $15x^2 - 7y^2 = 9$ n'admet pas de solutions entières.
- Montrer qu'il n'existe pas de polynôme à coefficients entiers tel que $f(7) = 11$ et $f(11) = 13$.

5.4 Partie entière

D'après l'un des principes extrémaux, la définition suivante a un sens :

Définition 4. Soit $x \in \mathbb{R}$. le plus petit entier inférieur ou égal à x noté par $\lfloor x \rfloor$ ou $E(x)$, est appelé la partie entière de x.

Exercice 5.5. Soient x, y deux nombres réels et n un entier naturel non nul.
- Montrer : $E(x) + E(y) \leq E(x + y)$.
- Montrer : $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$.
- $\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$.
- Calculer $\left\lfloor \sqrt{1} \right\rfloor + \left\lfloor \sqrt{2} \right\rfloor + \cdots + \left\lfloor \sqrt{2026} \right\rfloor$.

5.5 Problèmes

Problème 5.1 — *8.* Soit $A = 3^{105} + 4^{105}$. Montrer que 7 divise A. Calculer $A \pmod{11}$ et $A \pmod{13}$.)

Problème 5.2 — *17.* Montrer que si p est un nombre premier, on a $p^2 \equiv 1 \pmod{24}$.

Problème 5.3 — *97.* Trouver les trois derniers chiffres décimaux de 7^{9999}.

Problème 5.4 — *118.* Montrer que l'équation $y^2 = x(x+1)(x+2)(x+3)$ n'admet pas de solutions entières toutes positives.