Arithmétique

I Arithmétique des entiers

A Divisibilité

1 Division euclidienne

Définition : On dit que a divise b si $\exists k \in \mathbb{Z}, b = a \cdot k$.
On le note $a \mid b$.

Théorème : Division euclidienne *(admis)*

Soient $a, b \in \mathbb{Z}$ et b non nul.
Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :

$$a = b \cdot q + r$$

Remarque : On dit que a divise b si le reste de la division euclidienne de b par a est nul.

2 Congruences

Définition : Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
On dit que a est congru à b modulo n si n divise $a - b$.
On le note $a \equiv b\ (mod\ n)$ ou encore $a \equiv b\ [n]$.

Petit théorème de Fermat : *(admis)*

Soient p un nombre premier et $a \in \mathbb{Z}$ tel que $p \nmid a$.
Alors on a que :

$$a^{p-1} \equiv 1\ [p]$$

En partiuclier, on a que : $a^p \equiv a\ [p]$.

Lemme : *(admis)*

Soit $x, y \in \mathbb{Z}$ et soit $p \in \mathbb{P}$.
Alors :

$$(x + y)^p \equiv x^p + y^p\ [p]$$

3 Critère de divisibilité

Proposition : Écriture des nombres relatifs *(admis)*

On a que $\forall n \in \mathbb{Z}, n = \sum_{i=0}^{k} a_i \cdot 10^i$ avec a_i un entier entre -9 et 9.

Pour pouvoir aller plus rapidement, on établit les critères de divisibilité suivants :

1. $2 \mid n \Leftrightarrow$ le dernier chiffre de n est pair.
2. $3 \mid n \Leftrightarrow 3 \mid$ la somme des chiffres de n.
3. $4 \mid n \Leftrightarrow 4 \mid 10 \cdot a_1 + a_0$ (*ie* si le nombre formé par les deux derniers chiffres de n est divisible par 4).
4. $9 \mid n \Leftrightarrow 9 \mid$ la somme des chiffres de n.

B Nombres premiers

1 Généralités

Définition : On dit que n est un nombre **premier** et on note $n \in \mathbb{P}$ *(non standard)* si les diviseurs de n sont n et 1.

Crible d'Eratosthène : *(admis)*

Pour trouver la liste des nombres premiers, on applique l'algorithme suivant :

1. On écrit la liste des nombres ;
2. On retire 1 ;
3. On retire tous les multiples de 2 *(sauf lui-même)* ;
4. De même avec le nombre suivant 2 non barré, et ainsi de suite.

Théorème fondamental de l'arithmétique : *(admis)*

Tout entier naturel $n \geq 2$ s'écrit de manière unique (à l'ordre près des facteurs) comme un produit de nombres premiers.

Plus formellement, $\forall n \geq 2, \exists!(p_1, p_2, \dots, p_k) \in \mathbb{P}^k$ et $\forall i \in [1, k] \cap \mathbb{N}, \exists! \alpha_i \in \mathbb{N}^*$ tels que :

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

Corollaire : *(admis)*

Soit $n \in \mathbb{N}$.
Si $n \notin \mathbb{P}$, alors n a forcément un facteur premier p tel que $p \leq \sqrt{n}$.

2 PGCD et PPCM

Définition : Le **plus grand commun diviseur** (PGCD) de deux entiers a et b est le plus grand entier qui divise à la fois a et b.
On le note $pgcd(a, b)$ ou $a \wedge b$.

Définition : On dit de deux nombres qu'ils sont **premiers entre eux** si leur PGCD vaut 1.

Théorème de Bézout : *(admis)*

Soient $a, b \in \mathbb{Z}$.
Il existe des entiers $u, v \in \mathbb{Z}$ tels que :

$$a \cdot u + b \cdot v = pgcd(a, b)$$

En particulier on a l'**identité de Bézout** : a, b sont premiers entre eux $\Leftrightarrow \exists u, v \in \mathbb{Z}, a \cdot u + b \cdot v = 1$.

Définition : Le **plus petit commun multiple** (PPCM) de deux entiers a et b est le plus petit entier qui est multiple à la fois de a et de b.
On le note $ppcm(a, b)$ ou $a \vee b$.

Lemme :

Soient $a, b, k \in \mathbb{Z}$.
Alors on que $pgcd(a - k \cdot b, b) = pgcd(a, b)$.

Lemme de Gauss :

Soient $a, b, c \in \mathbb{N}$.

$$\begin{cases} a \mid b \cdot c \\ a \wedge b = 1 \end{cases} \Rightarrow a \mid c$$

Lemme d'Euclide :

Soient $a, b \in \mathbb{N}$ et $p \in \mathbb{P}$.

$$p \mid a \cdot b \Rightarrow (p \mid a \text{ ou } p \mid b)$$

II Résolution dans $\mathbb{Z}$ d'équations diophantiennes

Définition : Une **équation diophantienne** est une équation *(polynomiale)* dont les solutions recherchées sont des entiers relatifs.
On s'intéressera ici aux équations de la forme $a \cdot x + b \cdot y = c$ avec $a, b, c \in \mathbb{Z}$.

Étapes de résolution :

Étape 1 Étape 2 Étape 3

Note de rédaction : WIP