IV Nombres premiers

1 Généralités

Définition 1

Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si :

- **Remarques:** • 1 n'est pas un nombre premier. • l'ensemble des nombres premiers sera noté $\mathbb{P}$.
- **Remarque.** $n \geq 2$ n'est pas premier s'il peut s'écrire :

Exemple 1 *Lemme d'Euclide* ♥ — Soient $a, b \in \mathbb{Z}$ et $p \in \mathbb{P}$. On suppose que $p \mid ab$. Montrer que $p \mid a$ ou $p \mid b$.

Exemple 2 ♥ — Soit $n \in \mathbb{N}$, on pose $M_n = 2^n - 1$. Montrer que si M_n est premier, alors n est premier.

Théorème 1

Tout entier $n \geq 2$ possède au moins :

Exercice 1 — Démontrer ce théorème par récurrence forte sur n.

Théorème 2

L'ensemble $\mathbb{P}$ des nombres premiers est :

Exercice 2 — Démontrer ce théorème par l'absurde.

2 Petit théorème de Fermat

Exercice 3 ♥ *Ex. 86.2a), banque INP* — Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.

Théorème 3 : Petit théorème de Fermat

Soit $n \in \mathbb{Z}$ et soit $p \in \mathbb{P}$: 1. 2.

Exercice 4 ♥ *Ex. 86.2b) et 2c), banque INP* — Démontrer ce théorème pour $n \in \mathbb{N}$ à l'aide du résultat de l'ex. 3

3 Valuation p-adique

Définition 2

Soient $a \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La *valuation p-adique* de a, notée $v_p(a)$, est le plus grand $k \in \mathbb{N}$ tel que p^k divise a.

Autrement dit, $v_p(a) = k$ ssi : • ou encore •

Exemple 3 — Pour 84 : • $v_2(84) =$ • $v_3(84) =$ • $v_7(84) =$ • Si $p \in \mathbb{P} \setminus \{2, 3, 7\}$: $v_p(84) =$

Exercice 5 *Additivité des valuations p-adiques* — Soit $a, b \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. Montrer : $v_p(ab) =$

Exercice 6 *Unicité de la décomposition en facteurs premiers* — Soit $a \in \mathbb{N}^*$ et $p_1, \ldots, p_n$ les diviseurs premiers de a. On suppose que : $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ pour certains $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. Montrer que pour tout $i \in [\![1, n]\!]$: $\alpha_i = v_{p_i}(a)$.

4 La décomposition en facteurs premiers

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme $a =$

où : • • •

Exemple 4 — 12 = 120 = 84 =

- **Retenir.** Pour tout $p \in \mathbb{P}$, $v_p(a)$ est l'exposant de p dans la décomposition en facteurs premiers de a.

Théorème 5 : Applications à la divisibilité

Soient $a, b \in \mathbb{N}^*$ et $p_1, \ldots, p_n$ les facteurs premiers apparaissant dans la décomposition de a ou de b.
On peut écrire : $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$ où $\alpha_i = v_{p_i}(a)$ et $\beta_i = v_{p_i}(b)$ pour tout $i \in [\![1, n]\!]$.

1. $b \mid a$ ssi les valuations p_i-adiques de b sont inférieures à celles de a :

   ou encore ssi :

2. • $a \wedge b =$ • $a \vee b =$

Exemple 5 — Calculer le PGCD de $a = 84$ et $b = 120$ selon deux méthodes.

Exemple 6 SF 10 — Soient $a, b \in \mathbb{N}^*$. Montrer que a divise b si et seulement si a^2 divise b^2.