TD 2

Nombres premiers

On rappelle la définition de nombre premier :

Un entier $p \geq 2$ est dit premier *si ses seuls diviseurs positifs sont* 1 *et* p.

Exercice 1.

(a) Soit $n \geq 2$ un entier. Montrer qu'il existe un nombre premier p qui divise n.

(b) (*Lemme de Gauss*) Soient $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$ et $\text{pgcd}(a, b) = 1$. Montrer que $a \mid c$.

(c) (*Lemme d'Euclide*) En déduire que si p est un nombre premier et $a, b \in \mathbb{Z}$ vérifient $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

(d) Plus généralement, montrer que si p divise un produit $a_1 \cdots a_k$, alors p divise l'un des a_i.

Exercice 2.

(a) Soit $n \geq 2$ un entier. Montrer que n est premier si et seulement si n n'admet aucun diviseur premier inférieur ou égal à $\sqrt{n}$.

(b) (*Teste de primalité*) En utilisant (a), écrire un algorithme qui teste si un entier $n \geq 2$ est premier. Combien de divisions effectue-t-il dans le pire des cas ? Exprimer ce nombre en fonction de la taille k de n. L'algorithme est-il polynomial ?

Exercice 3. Démontrer le théorème d'Euclide :

Il existe une infinité de nombres premiers.

Indice : Supposer par l'absurde qu'il existe un nombre fini de nombres premiers, $p_1, \ldots, p_k$, et considérer l'entier $p_1 \cdots p_k + 1$.

Exercice 4. Montrer que, pour tout nombre premier p, le nombre $\sqrt{p}$ n'est pas rationnel.

Exercice 5. Soit p un nombre premier. On définit la fonction $\nu_p : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ de la manière suivante : pour tout entier $n \neq 0$, si $n = p^e m$ avec $p \nmid m$, alors $\nu_p(n) := e$.

(a) Montrer que tout entier $n \neq 0$ admet une factorisation en nombres premiers de la forme

$$n = \pm \prod_p p^{\nu_p(n)},$$

où le produit est pris sur l'ensemble des nombres premiers.

(b) Montrer que, pour $a, b \neq 0$,

$$a \mid b \quad \Longleftrightarrow \quad \nu_p(a) \leq \nu_p(b) \quad \text{pour tout nombre premier } p.$$

(c) En déduire que le plus grand commun diviseur de a et b peut s'écrire

$$\operatorname{pgcd}(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}.$$

(d) On prolonge la définition de ν_p à $\mathbb{Z}$ en posant

$$\nu_p(0) := \infty.$$

où ∞ satisfait les règles suivantes :

- $\infty \geq a \quad$ pour tout $a \in \mathbb{Z}$,
- $\infty + a = a + \infty = \infty + \infty = \infty \quad$ pour tout $a \in \mathbb{Z}$.

Montrer que pour tout $a, b \in \mathbb{Z}$, on a

$$\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b). \qquad \text{et} \qquad \nu_p(a + b) \geq \min\{\nu_p(a), \nu_p(b)\}.$$

et que l'égalité $\nu_p(a+b) = \min\{\nu_p(a), \nu_p(b)\}$ est vraie si $\nu_p(a) \neq \nu_p(b)$.

(e) On prolonge encore la définition de ν_p à $\mathbb{Q}$ en posant, pour $a, b \in \mathbb{Z} \setminus \{0\}$,

$$\nu_p\left(\tfrac{a}{b}\right) := \nu_p(a) - \nu_p(b).$$

Vérifier que cette définition est bien posée, c'est-à-dire indépendante de l'écriture de a/b.

(f) Soit K un corps. Une application $v : K \to \mathbb{Z} \cup \{\infty\}$ est une *valuation discrète* si, pour tous $x, y \in K$,

- $v(xy) = v(x) + v(y)$,
- $v(x + y) \geq \min\{v(x), v(y)\}$,
- $v(x) = \infty \Leftrightarrow x = 0$.

Montrer que ν_p est une valuation discrète sur $\mathbb{Q}$, appelée *valuation p-adique*.