TD 2

Nombres premiers, Relations d'équivalence

Esercizio 1. 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 $\sqrt{n}$.

Esercizio 2. 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 le produit $p_1 \cdots p_k + 1$.

Esercizio 3. Montrer que, pour tout nombre premier p, le nombre $\sqrt{p}$ n'est pas rationnel.

Esercizio 4. 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
$$\mathrm{pgcd}(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}.$$

(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.*

Esercizio 5. On considère sur $\mathbb{Z}$ la relation suivante : soient $a, b \in \mathbb{Z}$

$$a \sim b \Leftrightarrow |a - b| \leq 2.$$

Est-ce que $\sim$ est une relation d'équivalence ? Si oui, décrire pour tout $a \in \mathbb{Z}$ la classe d'équivalence $[a]$ de a et l'ensemble quotient $\mathbb{Z}/\sim$.

Esercizio 6. On considère sur $\mathbb{R}$ la relation suivante : soient $x, y \in \mathbb{R}$

$$x \sim y \Leftrightarrow x^2 = y^2.$$

Est-ce que $\sim$ est une relation d'équivalence ? Si oui, décrire pour tout $x \in \mathbb{R}$ la classe d'équivalence $[x]$ de x et l'ensemble quotient $\mathbb{R}/\sim$.

Esercizio 7. Soit $n \in \mathbb{Z}_{>0}$. On considère sur $\mathbb{Z}$ la relation suivante : soient $a, b \in \mathbb{Z}$

$$a \sim_n b \Leftrightarrow n \mid (a - b).$$

1) Montrer que $\sim_n$ est une relation d'équivalence.
2) Décrire les classes d'équivalences de 0, 1 et n, c'est-à-dire :

$$\begin{aligned}
[0]_n &:= \{a \in \mathbb{Z} : a \sim_n 0\}, \\
[1]_n &:= \{a \in \mathbb{Z} : a \sim_n 1\}, \\
[r]_n &:= \{a \in \mathbb{Z} : a \sim_n r\}, \text{pour } 1 < r < n, \\
[n]_n &:= \{a \in \mathbb{Z} : a \sim_n n\}.
\end{aligned}$$

3) Décrire l'ensemble quotient $\mathbb{Z}/\sim_n$.