



On rappelle qu'un nombre entier p est dit premier s'il est strictement supérieur à 1 et s'il n'admet aucun autre diviseur positif que 1 et p . Un nombre strictement supérieur à 1 et qui n'est pas premier est dit composé. On note p_1, p_2, \dots la suite des nombres premiers, i.e. 2, 3, 5, 7 \dots et $\pi(x)$ le cardinal de l'ensemble des nombres premiers inférieurs au réel x ($x \geq 1$). Le but de ces questions est d'étudier la répartition des nombres premiers.

Dans la suite n désigne un entier naturel non nul, x un réel supérieur à 1 et p un nombre premier.

1. Second théorème d'Euclide

- (a) On note $q_n = p_1 p_2 \dots p_n$. En considérant $q_n + 1$, déterminer $\lim_{x \rightarrow +\infty} \pi(x)$.
- (b) Montrer qu'il existe des séquences arbitrairement longues de nombres composés consécutifs.
- (c) Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 3$.
- (d) Montrer qu'il existe une infinité de nombres premiers de la forme $6k + 5$.
- (e) Montrer $p_n < 2^{2^n}$ et en déduire $\pi(x) \geq \log \log(x)$ si $x \geq 2$.
- (f) Soit $N_n(x)$ le nombre d'entiers k inférieurs à x et qui ne sont divisibles par aucun nombre premier p strictement supérieur à p_n . Montrer $N_n(x) \leq 2^n \sqrt{x}$. (Considérer les $m \leq x$ avec $m = k^2 p_{i_1} p_{i_2} \dots p_{i_r}$.)
- (g) En déduire que la suite $\left(\sum_{k=1}^n \frac{1}{p_k} \right)$ n'est pas bornée.
- (h) En déduire également $\pi(x) \geq \frac{\log(x)}{2 \log(2)}$.

2. Cas élémentaire du Grand théorème de Dirichlet (Johann Peter Gustav Lejeune-Dirichlet)

- (a) On note $\Phi_n = \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} \left(X - \exp\left(\frac{2ik\pi}{n}\right) \right)$. Montrer $\prod_{d|n} \Phi_d = X^n - 1$, puis $\Phi_n \in \mathbf{Z}[X]$.
- (b) Soit P dans $\mathbf{Z}[X]$, n_1, \dots, n_k des entiers naturels non nuls et a un entier tel que $b = P(a)$ soit non nul. Soit $Q = \frac{1}{b} P(a + n_1 n_2 \dots n_k X)$. Montrer $Q \in \mathbf{Z}[X]$ et $Q(n) \equiv 1 [n_i]$, pour $1 \leq i \leq k$.
- (c) Soit P dans $\mathbf{Z}[X]$. On dit que p est un diviseur de P si p divise $P(n)$ pour un n tel que $P(n) \neq 0$. En utilisant la remarque précédente, montrer que P a une infinité de diviseurs.
- (d) On suppose que n n'est pas un multiple de p et que a dans \mathbf{N} est tel que $p | \Phi_n(a)$. Montrer $a^n \equiv 1 [p]$ et en déduire que p ne divise pas a .
- (e) En considérant $\Phi_n(a)$ et $\Phi_n(a + p)$ montrer que n est le plus petit entier naturel non nul tel que $a^n \equiv 1 [p]$.
- (f) En déduire qu'il existe une infinité de nombres premiers de la forme $km + 1$.

3. Vers le théorème des nombres premiers (Jacques Hadamard - Charles-Jean de la Vallée Poussin)

- (a) On note $\theta(x) = \sum_{p \leq x} \log p$ et $\psi(x) = \sum_p \sum_{\substack{m \\ p^m \leq x}} \log p$, de sorte que $\theta(10) = \log 2 + \log 3 + \log 5 + \log 7$ et $\psi(10) = 3 \log 2 + 2 \log 3 + \log 5 + \log 7$. Montrer $\psi(x) = \theta(x) + O(\sqrt{x}(\log x)^2)$.
- (b) Montrer $\theta(n) < 2n \log 2$ (on pourra considérer les nombres premiers divisant $\binom{2m+1}{m}$ et raisonner par récurrence).
- (c) Montrer $\psi(2n) = \sum_{p \leq 2n} \left[\frac{\log(2n)}{\log(p)} \right] \log(p) > \log \left(\binom{2n}{n} \right)$.
- (d) En déduire $\theta(x) \asymp x$, $\psi(x) \asymp x$, puis $\pi(x) \asymp \frac{x}{\log(x)}$ et $p_n \asymp n \log(n)$ (où $f \asymp g$ si $f = O(g)$ et $g = O(f)$).

4. Questions subsidiaires : Qui fut le premier à être élu président de l'Union mathématique internationale en 1920, avant d'être anobli en 1930 par le roi Albert Ier ? Qui servit de modèle au Savant Cosinus et fut par ailleurs président de la Société mathématique de France en 1906 et le cousin issu de germain de la femme d'Alfred Dreyfus ? Qui fut le premier à énoncer le principe des tiroirs ? Enfin à qui est dû le dernier théorème démontré (indications : des polynômes portent son nom, on lui doit l'étude de la machine à marcher et le patron de la demi-sphère) et quel est son prénom ?