UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille de TD 1

Exercice 1

On propose une preuve analytique du théorème d'Euclide. Supposons que l'ensemble des nombres premiers est fini,

$$\mathcal{P} = \{p_1, ..., p_k\},$$

et posons

$$X = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)^{-1}.$$

1 Pour p premier, et $m \geq 1$, montrez que

$$\left(1 - \frac{1}{p}\right)^{-1} \geq 1 + \frac{1}{p} + \frac{1}{p^2} + .. + \frac{1}{p^m}.$$

2 En déduire que

$$X \geq \sum_{n \in N(m)} \frac{1}{n},$$

où $N(m)$ désigne les entiers dont la décomposition en facteurs premiers $n = p_1^{e_1}...p_k^{e_k}$ vérifie $e_i \leq m$ pour tout i.

3 En conclure une absurdité.

Exercice 2

Le but de cet exercice est de montrer qu'il y a une infinité de nombres premiers congrus à -1 modulo 4. On procède par l'absurde et supposons le contraire, en notant $\{p_1, ..., p_m\}$ les premiers congrus à -1 modulo 4. On pose

$$n = 4p_1...p_m - 1,$$

1 Montrez que tout facteur premier p de n est congru à 1 modulo 4.

2 Obtenir une contradiction.

Exercice 3

Montrez qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

Exercice 4

Soit A un anneau intègre. Rappelons que A est dit euclidien si il existe une fonction $\nu : A - \{0\} \to \mathbb{N}$ (appelée *stathme euclidien*) telle que pour tout $(a, b) \in A \times (A - \{0\})$, il existe $(q, r) \in A^2$ avec

$$a = bq + r,$$

et $r = 0$ ou $\nu(r) < \nu(b)$.
Redémontrez le résultat de cours suivant : un anneau euclidien est principal.

Exercice 5

On se propose de refaire la démonstration du théorème d'Euler : si $n > 1$ et $(a, n) = 1$, alors

$$a^{\varphi(n)} \equiv 1 \, (mod\, n).$$

1 Montrez que a est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ ssi $(a, n) = 1$.
2 Rappelez la définition de la fonction indicatrice d'Euler $\varphi(n)$.
3 Conclure, et déduire comme corollaire le théorème de Fermat.

Exercice 6

Critère de Fermat, nombres de Carmichael.
1 Si $a \in [1, n-1]$ et $(a, n) \neq 1$, montrez que a est témoin de Fermat pour la non-primalité de n.
2 Soit n un nombre sans facteurs carrés, tel que pour tout diviseur premier p de n, $p - 1$ divise $n - 1$. Montrez que n est soit premier, soit de Carmichael.
3 Montrez que 561 et 1105 sont de Carmichael.
4 Soit p un nombre premier tel que p^2 divise n. Montrez que $a = 1 + \frac{n}{p}$ est d'ordre p dans $(\mathbb{Z}/n\mathbb{Z})^\times$, et que a est témoin de Fermat pour la non-primalité de n.
5 En déduire qu'un nombre de Carmichael est sans facteur carré.
6 Montrez qu'un nombre sans facteur carré est de Carmichael si et seulement si pour tout diviseur premier p de n, on a $(p-1)|(n-1)$.

Exercice 7

Démontrez le théorème de Wilson : $n > 1$ est premier si et seulement si

$$(n-1)! \equiv -1 \, (mod\, n).$$

Discutez de la pertinence d'un "test de Wilson" de primalité.

Exercice 8

Soit Q un polynôme non constant à coefficients entiers.
1 On supppose que $Q(0) = 1$. Montrez, en s'inspirant de la preuve du théorème d'Euclide, que l'ensemble des diviseurs premiers des nombres de $Q(\mathbb{Z})$ est infini.
2 Montrez que ce résultat est vrai en général même si $Q(0) \neq 1$, en se ramenant au cas précédent.