Feuille de TD 3

Nombres premiers

Exercice 1. Soit $P(X_1, \ldots, X_r) \in \mathbb{C}[X_1, \ldots, X_r]$ un polynôme à r variables ne prenant que des valeurs premières sur $\mathbb{N}^r$.

(1) En utilisant les polynômes de Lagrange associés aux points $\{0, 1, \ldots, n\}$, montrer que P est à coefficients rationnels.

(2) Soit $p = P(1, \ldots, 1)$. Montrer qu'il existe une infinité de r-uplets d'entiers $(m_1, \ldots, m_r)$ tels que $P(m_1, \ldots, m_r) = p$.

(3) En déduire que P est constant.

Exercice 2 (Théorème de Wilson). Soit $n \geqslant 2$ un entier. Montrer que n est premier si et seulement si n divise $(n-1)! + 1$.

Tests de primalité probabilistes

Soit n un entier naturel impair. On écrit $n-1 = q2^s$ avec q impair et on définit les ensembles

$$\begin{aligned} A_n &= \{a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^{n-1} = 1\}, \\ B_n &= \{a \in A_n \mid a^{q2^{j+1}} = 1 \implies a^{q2^j} = \pm 1 \quad \text{pour} \quad j = 0, \ldots, s-1\}, \\ C_n &= \{a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^{(n-1)/2} = \left(\frac{a}{n}\right)\}. \end{aligned}$$

Exercice 3. (1) Montrer que si n est premier, alors $A_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

(2) Montrer que si n est composé et que $A_n \neq (\mathbb{Z}/n\mathbb{Z})^\times$, alors $|A_n| \leqslant \frac{n-1}{2}$.

Exercice 4. On appelle *nombre de Carmichael* tout entier naturel n impair, composé et tel que $A_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

Montrer que tout nombre de Carmichael n est de la forme $n = p_1 \ldots p_r$ pour des nombres premiers distincts $p_1, \ldots, p_r$, avec $r \geqslant 3$ et tels que $(p_i - 1)$ divise $(n-1)$ pour tout i.

Exercice 5. Montrer que n est premier si et seulement si $C_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 6. (1) Montrer que si n est premier, alors $B_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

(2) $(*)$ Montrer que si n est composé, alors $|B_n| \leqslant \frac{n-1}{4}$.

Exercice 7. Implémenter les tests de primalité de Rabin–Miller et de Solovay–Strassen, respectivement basés sur les tests d'appartenance aux ensembles B_n et C_n. Les comparer en termes de nombres d'erreurs et de temps de calcul. Que se passe-t-il si on implémente l'algorithme analogue en utilisant l'ensemble A_n (test de Fermat) ?