# Exercise sheet 3

## Prime numbers

**Exercice 1.** Let $P(X_1, \dots, X_r) \in \mathbb{C}[X_1, \dots, X_r]$ be a polynomial in $r$ variables that takes only prime values on $\mathbb{N}^r$.

(1) Using Lagrange's interpolation polynomials with respect to the points $\{0, 1, \dots, n\}$, show that $P$ has rational coefficients.

(2) Let $p = P(1, \dots, 1)$. Show that there exists infinitely many $r$-tuples of integers $(m_1, \dots, m_r)$ such that $P(m_1, \dots, m_r) = p$.

(3) Deduce that $P$ is constant.

**Exercice 2 (Wilson's theorem).** Let $n \geqslant 2$ be an integer. Show that $n$ is prime if and only if $n$ divides $(n-1)! + 1$.

## Probabilistic primality tests

Let $n$ be an odd natural number. Write $n - 1 = q2^s$ with $q$ odd and define the sets

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

**Exercice 3.** (1) Show that if $n$ is prime, then $A_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

(2) Show that if $n$ is composite and $A_n \neq (\mathbb{Z}/n\mathbb{Z})^\times$, then $|A_n| \leqslant \frac{n-1}{2}$.

**Exercice 4.** A *Carmichael number* is an odd natural number $n$ that is composite and verifies that $A_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

Show that every Carmichael number is of the form $n = p_1 \dots p_r$ for some distinct primes $p_1, \dots, p_r$, with $r \geqslant 3$ and such that $(p_i - 1)$ divides $(n-1)$ for all $i$.

**Exercice 5.** Show that $n$ is prime if and only if $C_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

**Exercice 6.** (1) Show that if $n$ is prime, then $B_n = (\mathbb{Z}/n\mathbb{Z})^\times$.

(2) $(*)$ Show that if $n$ is composite, then $|B_n| \leqslant \frac{n-1}{4}$.

**Exercice 7.** Implement the Rabin–Miller and Solovay–Strassen primality tests, which are respectively based on the sets $B_n$ and $C_n$. Compare them in terms of probability of error and complexity. Can we use the set $A_n$ to give a primality test ?