Devoir 1

Devoir à rendre au plus tard dimanche 21 février à 23h59.
Les cinq parties ne sont pas indépendantes.

Rappels
Si a est un entier, on note $\tau(a) = \min\{k \in \mathbf{N}, |a| < 2^k\}$. On convient que $\tau(0) = 0$.
Si $P = \sum_{i=0}^{d} a_i X^i \in \mathbf{Z}[X]$, on note $\tau(P) = \max\{\tau(a_i), i = 0, \ldots, d\}$, la taille $\tau(P)$.
On peut multiplier deux entiers de taille τ et τ' en $O(\tau\tau')$ opérations binaires.

Le polynôme cyclotomique Φ_n est le polynôme unitaire dont les racines sont les $\varphi(n)$ racines primitives n-ème de 1 (dans $\mathbf{C}^*$). Φ_n est de degré $\varphi(n)$ et on a

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Le polynôme $\Phi_p = X^{p-1} + \cdots + X + 1$ est irréductible.

Soit p un nombre premier. On définit le symbole de Legendre associé à l'entier a

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \pmod p \text{ est un carré de } (\mathbf{Z}/p\mathbf{Z})^* \\ -1 & \text{si } a \pmod p \text{ n'est pas un carré de } (\mathbf{Z}/p\mathbf{Z})^* \\ 0 & \text{si } a \equiv 0 \pmod p \end{cases}.$$

On rappelle que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ et que $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$.

I. Première partie.

1. Soit P et Q deux polynômes de taille τ et τ' et de degré n et $m \leq n$.
   (a) Montrer que $\tau(PQ) \leq \log_2(m+1)(\tau + \tau')$.
   (b) Montrer qu'on peut calculer $P \cdot Q$ en $O(mn\tau\tau')$ opérations binaires.
2. Soit $a \in \mathbf{Z}$ de taille τ' et $P \in \mathbf{Z}[X]$ de degré n et de taille τ.
   (a) Montrer que $\tau(P(a)) \leq \tau + (n+1)\tau'$.
   (b) Montrer qu'on peut calculer $P(a)$ en $O(n\tau\tau' + n^2\tau'^2)$ opérations binaires.

II. Identités polynomiales

1. On considère la suite de polynômes $(T_n)_{n\geq 0}$ de $\mathbf{Z}[X]$ définie par

$$T_0 = 2, T_1 = X, T_{n+1} = XT_n - T_{n-1}.$$

   (a) Montrer que pour tout $n \geq 1$, T_n est un polynôme unitaire de $\mathbf{Z}[X]$, de degré n, de même parité que n.
   (b) Montrer que pour tout $n \in \mathbf{N}$, on a $T_n(2\cos t) = 2\cos nt$.
   (c) Calculer T_i, pour $0 \leq i \leq 5$.
2. On considère la suite de polynômes $(U_n)_{n\geq 0}$ de $\mathbf{Z}[X]$ définie par

$$U_0 = 0, U_1 = 1, U_{n+1} = XU_n - U_{n-1}.$$

   (a) Montrer que pour tout $n \geq 1$, U_{n+1} est un polynôme unitaire de $\mathbf{Z}[X]$, de degré n, de même parité que n.
   (b) Montrer que pour tout $n \in \mathbf{N}$, on a $U_n(2\cos t) = \dfrac{\sin nt}{\sin t}$.
   (c) Montrer que les racines de U_n sont les $2\cos k\pi/n$, $k = 1, \ldots, n-1$.
   (d) Calculer U_i pour $1 \leq i \leq 6$.
   (e) Soit $r \in \mathbf{Q}$. En déduire que $\cos r\pi \in \mathbf{Q}$ si et seulement si $\cos r\pi \in \{0, \pm 1/2, \pm 1\}$.

III. Calcul des polynômes

1. (a) Montrer que $T_n' = nU_n$.
   (b) Montrer que T_n vérifie l'équation différentielle $(4-x^2)T_n''(x) - xT_n'(x) + n^2 T_n(x) = 0$.
   (c) En déduire que $T_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} X^{n-2k}$
   (d) En déduire que $U_{n+1} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \binom{n-k}{k} X^{n-2k}$.
2. (a) Montrer que $\tau(T_n) \leq n$ et $\tau(U_n) \leq n-1$.
   (b) En utilisant la formule de récurrence $P_{n+1} = XP_n - P_{n-1}$ pour $(T_n)_{n\geq 1}$ et $(U_n)_{n\geq 1}$, montrer qu'on peut calculer T_n et U_n en $O(n^2)$ opérations binaires.

IV. Polynôme minimal de $\cos 2\pi/p$

1. (a) Montrer que $X^{\varphi(n)}\Phi_n(1/X) = \Phi_n$, pour $n \geq 2$.
   (b) Montrer que pour tout $n \in \mathbf{N}$, on a $T_n(X + \frac{1}{X}) = X^n + \frac{1}{X^n}$.
   (c) En déduire que pour $n \geq 3$, il existe un unique polynôme unitaire $M_n \in \mathbf{Z}[T]$, tel que
   $$\Phi_n = X^{\varphi(n)/2} M_n(X + 1/X).$$
   (d) Montrer que pour tout $n \geq 2$, les racines de M_n sont les $2\cos 2k\pi/n$, $(k,n) = 1$.
   (e) Montrer que M_n divise U_n dans $\mathbf{Z}[X]$, pour $n \geq 3$.
2. On pose également $M_2 = T + 2$.
   (a) Calculer M_3, M_4, M_5.
   (b) En déduire une expression de $\cos 2\pi/5$.
   (c) Montrer que si p est un nombre premier, M_p est est le polynôme minimal de $2\cos 2\pi/p$.

V. Loi de réciprocité quadratique

1. (a) Montrer que $\mathrm{Res}\,(U_n, U_m) = \prod_{k=1}^{n-1} U_m(2\cos k\pi/n) = \prod_{k=1}^{n-1} \frac{\sin km\pi/n}{\sin k\pi/n}$.
   (b) En déduire que si $(n,m) = 1$, alors $\mathrm{Res}\,(U_n, U_m) \in \{-1, 1\}$.
   (c) En déduire que si $(n,m) = 1$, alors $\mathrm{Res}\,(M_n, M_m) \in \{-1, 1\}$.
2. Soit p un nombre premier impair.
   (a) Montrer que $\Phi_p \equiv (X-1)^{p-1} \pmod p$.
   (b) En déduire que $M_p(T) \equiv (T-2)^{(p-1)/2} \pmod p$.
   (c) En déduire que $\mathrm{Res}\,(M_p \pmod p, M_q \pmod p) \equiv q^{(p-1)/2} \pmod p$.
   (d) En déduire que $\mathrm{Res}\,(M_p, M_q) = \left(\frac{q}{p}\right)$
   (e) En déduire la loi de réciprocité quadratique $\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)}{2}\frac{(p-1)}{2}} \left(\frac{p}{q}\right)$ pour p et q premiers impairs.