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

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

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

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.

Corrigé

1. (a) On a $PQ = \sum_{i=0}^{n+m} c_i X^i$ où $c_i = \sum_{j=0}^{\min i,m} a_{i-j} b_j$ donc $|c_i| \leq (m+1)2^{\tau+\tau'}$.
   (b) On calcule chaque c_i en effectuant au plus $m+1$ multiplications $a_{i-j}b_j$ qui coûtent chacune $O(\tau\tau')$ opérations binaires et m additions qui coûtent $O(\tau + \tau') = O(\tau\tau')$ opérations binaires. Au final on obtient $O((m+1)(n+m+1)\tau\tau') = O(nm\tau\tau')$ opérations binaires.
2. (a) Soit $P = a_n + a_{n-1}X + \cdots + a_0 X^n$.
   On a $|P(a)| \leq \sum_{i=0}^{n} |a_{n-i}||a^i| \leq \sum_{i=0}^{n} 2^\tau 2^{i\tau'} = 2^\tau(2^{(n+1)\tau'} - 1)/(2^{\tau'} - 1) \leq 2^{\tau+(n+1)\tau'}$.
   (b) On utilise le procédé de Horner. Définissons $r_0 = a_0$ et $r_i = ar_{i-1} + a_i$. On a alors, par récurrence, $r_i = H_i(a)$ où $H_i = \sum_{j=0}^{i} a_j X^{i-j}$. D'après la question précédente $\tau(H_i(a)) \leq \tau + (i+1)\tau'$. On calcule donc r_i en $O((\tau + (i+1)\tau')\tau')$ opérations binaires à partir de r_{i-1}. Au final on obtient $r_n = H_n(a) = P(a)$ 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 $\cos r\pi \in \{0, \pm 1/2, \pm 1\}$.

Corrigé

1. (a) En utilisant que XT_n est unitaire de degré $n+1$ et même parité que T_{n-1}, on déduit que T_{n+1} est de degré $n+1$ et de parité $n+1$.

(b) On vérifie que $\cos(n+1)t = 2\cos t \cos nt - \cos(n-1)t$.

(c) On obtient $T_0 = 1, T_1 = X, T_2 = X^2 - 1, T_3 = X^3 - 3X, T_4 = X^4 - 4X^2 + 1, T_5 = X^5 - 5X^3 + 4X$.

(d) En déduire que $X^n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor - 1} \binom{n}{k} T_{n-2k} + \frac{1+(-1)^n}{2}$.

2. (a) Idem que la même question avec T_n.

(b) On vérifie que $\sin(n+1)t = 2\cos t \sin nt - \sin(n-1)t$.

(c) $U_n(2\cos t) = 0$ si et seulement si $\sin nt = 0$ et $\sin t \neq 0$, soit $t = t_k = k\pi/n$ et $\sin t_k \neq 0$. Les racines de U_n sont les $2\cos k\pi/n$, $k = 1, \ldots, n-1$, tous distincts, car $t \mapsto \cos t$ est strictement décroissant sur $[-\pi, \pi]$.

(d) On a $U_1 = 1, U_2 = X, U_3 = X^2 - 1, U_4 = X^3 - 2X, U_5 = X^4 - 3X^2 + 1, U_6 = X^5 - 4X^3 + 3X$.

(e) Si $r = m/n = q + k/n$, où $0 \leq k < n$, alors $\cos r\pi = (-1)^q \cos k\pi/n$. Comme U_n est pair ou impair, alors $2\cos k\pi/n$ et $-2\cos k\pi/n$ sont racines de U_n unitaire. Ils sont donc entiers. On a donc $2\cos r\pi \in \mathbf{Z} \cap [-2, 2]$.

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.

Corrigé

1. (a) Soit $f(t) = 2\cos nt$. Alors $f'(t) = -2n\sin nt = -2\sin t T_n'(2\cos nt)$. Donc $T_n'(2\cos t) = nU_n(2\cos t)$. $T_n' - nU_n$ s'annule sur $[-1, 1]$, il est donc nul.

(b) On a $f'(t) = -2\sin t T_n'(2\cos nt)$ donc $f''(t) = -2\cos t T' n(2\cos nt) + 4\sin^2 t T_n''(2\cos t)$ d'une part et $f'(t) = -2n\sin nt$ donc $f''(t) = -2n^2\cos nt = -n^2 T_n(2\cos t) = -n^2 f(t)$, d'autre part.
En posant $x = 2\cos t$ on obtient $0 = n^2 f(t) + f''(t) = n^2 T_n(x) - xT_n'(x) + (4 - x^2)T_n''(x)$.

(c) Posons $T_n(x) = \sum_{k=0}^n a_k x^k$. On a $xT_n'x = \sum_k k a_k x^k$ et $(4-x^2)T_n'' = \sum_k (4(k+2)(k+1)a_{k+2} - k(k-1)a_k)x^k$. Alors, à partir de l'équation différentielle on obtient $n^2 a_k - k a_k + 4(k+2)(k+1)a_{k+2} - k(k-1)a_k = 0$, soit $a_k(n^2 - k - k(k-1)) + 4(k+2)(k+1)a_{k+2} = 0$. On obtient finalement

$$a_{k-2}(n-k+2)(n+k-2) = -4k(k-1)a_k.$$

Comme $a_n = 1$, on obtient
$a_{n-2k} = (-1)^k 4^k \dfrac{n(n-1)\cdots(n-2k)}{(2\cdot 4\cdots 2k)((2n-2)\cdots(2n-2k))} = (-1)^k \dfrac{n(n-1)\cdots(n-2k)}{k!(n-1)\cdots(n-k)} = (-1)^k \dfrac{n}{n-k}\binom{n-k}{k}.T_n$
est une fonction hypergéométrique.

(d) En dérivant, on obtient

$$\begin{aligned}
(n+1)U_{n+1} &= \sum_{k=0}^{\lfloor \frac{n+1}{2} \rfloor} (-1)^k \tfrac{n+1}{n+1-k}\binom{n+1-k}{k}(n+1-2k)X^{n-2k} \\
&= (n+1)\sum_{k=0}^{\lfloor \frac{n+1}{2} \rfloor} (-1)^k \tfrac{n+1-2k}{n+1-k}\binom{n+1-k}{n+1-2k}X^{n-2k} \\
&= (n+1)\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \binom{n-k}{k}X^{n-2k}
\end{aligned}$$

2. (a) On a $T_n = \sum_{k=0}^n (-1)^k |a_k| X^{n-2k}$, et donc $u_n = (-i)^n T_n(i) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} |a_k|$. Mais $T_{n+1}(i) = iT_n(i) - T_{n-1}(i)$ d'où $u_{n+1} = u_n + u_{n-1}$ avec $u_0 = 2$, $u_1 = 1$, $u_2 = 2$, d'où l'on vérifie que $0 < u_n < 2^n$, pour $n \geq 1$. Au final $\tau(a_k) \leq n$ et $\tau(T_n) \leq n$.
De $\binom{n-k}{k} \leq \frac{n}{n-k}\binom{n}{n-k}$, on tire que $\tau(U_{n+1}) \leq n$.

(b) T_n et U_n en $O(n^3)$ opérations binaires. Si $\tau(P_i) \leq i$ alors on calcule XP_i en $O(i)$ opérations binaires et $XP_i - P_{i-1}$ en $O(i)$ additions, à partir de P_i et P_{i-1}. Au final on obtient $O(n^2)$ 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 $T_n(X + \dfrac{1}{X}) = X^n + \dfrac{1}{X^n}$.

(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 $2\cos 2\pi/p$.

Corrigé

1. (a) Si x est racine de Φ_n alors x est d'ordre n et $1/x$ également. Donc $1/x$ est racine de Φ_n donc x est racine de $\Phi_n(1/X)X^{\deg \Phi_n}$. Par conséquent Φ_n et $X^{\varphi(n)}\Phi_n$ sont unitaires et ont les mêmes racines, sont égaux.

(b) Pour $x = \exp it$, on obtient $T_n(x + 1/x) = T_n(2\cos t) = x^n + 1/x^n$. La fraction $T_n(X + \dfrac{1}{X}) - (X^n + \dfrac{1}{X^n})$ s'annule pour une infinité de valeurs sur $\mathbf{C}$. Elle est nulle.

(c) On écrit $\Phi_n = a_0 + a_1 X + \cdots + a_n X^{\varphi(n)}$. Remarquons que $\varphi(n)$ est pair, si $n \geq 3$. Le fait que $\Phi_n = X^{\varphi(n)}\Phi_n$ indique que $a_k = a_{\varphi(n)-k}$, pour tout k, donc $\Phi_n = \sum_{k=0}^{\varphi(n)/2-1} a_k(X^k + X^{\varphi(n)-k}) + a_{\varphi(n)/2}X^{\varphi(n)/2}$. En factorisant par $X^{\varphi(n)/2}$, on obtient $M_n = \sum_{k=0}^{\varphi(n)/2} a_k T_k + a_{\varphi(n)/2}$. Un tel polynôme est unitaire et de degré $\varphi(n)/2$, ses racines sont connues (voir question suivante).

(d) On a $M_n(2\cos 2k\pi/n)\exp(i\varphi(n)k\pi/n) = \Phi_n(\exp(2ik\pi/n) = 0$ si $(k,n) = 1$.

(e) M_n est scindé et ses racines sont parmi celles de U_n, donc M_n divise U_n dans $\mathbf{C}[X]$. Par unicité de la division euclidienne dans $\mathbf{C}[X]$, M_n divise U_n dans $\mathbf{Q}[X]$. Mais comme M_n est également unitaire, donc primitif, alors M_n divise U_n dans $\mathbf{Z}[X]$.

2. (a) En posant $T = X + 1/X$. On a $\varphi_3 = X^2 + X + 1 = X(T+1)$, d'où $M_3 = T + 1$. $\Phi_4 = X^2 + 1 = X \cdot T$, d'où $M_4 = T$. $\varphi_5 = X^4 + X^3 + X^2 + X + 1 = X^2((T^2-2) + T + 1)$, d'où $M_5 = T^2 + T - 1$.

(b) Les racines de M_5 sont $2\cos 2\pi/5$ et $2\cos 4\pi/5$. Mais $M_5 = (T+1/2)^2 - 5/4$, d'où $\cos 2\pi/5 = -\frac{1}{4} + \frac{\sqrt{5}}{4}$ et $\cos 4\pi/5 = -\frac{1}{4} - \frac{\sqrt{5}}{4}$

(c) Si $M_p(T) = P(T)Q(T)$, alors $X^{(p-1)/2}M_p(X+1/X) = X^{\deg P}P(X+1/X) \cdot X^{\deg Q}Q(X+1/X) = \widehat{P}\widehat{Q} = \Phi_p$. Mais Φ_p est irréductible donc $\deg \widehat{P} = 0$ ou $\deg \widehat{Q} = 0$ et $\deg P = 0$ ou $\deg Q = 0$. M_p est irréductible.

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.

Corrigé

1. (a) On a $\mathrm{Res}\,(U_n, U_m) = \prod_{k=1}^{n-1} U_m(2\cos k\pi/n)$ car U_n est unitaire et ses racines sont les $2\cos k\pi/n$. $U_m(2\cos k\pi/n) = \frac{\sin km\pi/n}{\sin k\pi/n}$, d'après II.2b.

(b) On a $\mathrm{Res}\,(U_n, U_m) = \prod_{k=1}^{n-1} \frac{\sin km\pi/n}{\sin k\pi/n}$. Comme $(m,n) = 1$, alors $k \mapsto m \cdot k$ est une bijection de $(\mathbf{Z}/n\mathbf{Z})^*$. L'ensemble des $|\sin k\pi/n|$ et des $|\sin km\pi/n|$ coincident. Donc $\mathrm{Res}\,(U_n, U_m) = \pm 1$.

(c) On sait que $\mathrm{Res}\,(A, BC) = \mathrm{Res}\,(A,B)\mathrm{Res}\,(A,C)$. D'autre part, $\mathrm{Res}\,(M_n, M_m) \in \mathbf{Z}$ car M_m et $M_n \in \mathbf{Z}[X]$. Comme M_n divise U_n alors $\mathrm{Res}\,(M_n, U_m)$ divise $\mathrm{Res}\,(U_n, U_m)$. Comme M_m divise U_m, Alors $\mathrm{Res}\,(M_n, M_m)$ divise $\mathrm{Res}\,(M_n, U_m)$. Finalament $\mathrm{Res}\,(U_n, U_m)$ divise 1.

2. (a) On a $(X-1)\Phi_p = X^p - 1 \equiv (X-1)^p \pmod p$, d'où le résultat.

(b) Posons $T = X + 1/X$, alors $T - 2 = (X-1)^2/X$, donc $X^{(p-1)/2}(T-2)^{(p-1)/2} = (X-1)^{p-1}$. On a donc

$$\Phi_p(X) \equiv (X-1)^{p-1} \equiv X^{(p-1)/2}M_p(T) \pmod p \equiv X^{(p-1)/2}(T-2)^{(p-1)/2} \pmod p.$$

Il s'agit d'une égalité dans $\mathbf{Z}/p\mathbf{Z}(X)$, d'où l'on tire, par unicité de la décomposition des fractions rationnelles : $M_p(T) \equiv (T-2)^{(p-1)/2} \pmod p$.

(c) $\mathrm{Res}\,(M_p \bmod p, M_q \bmod p) = \mathrm{Res}\,((T-2)^{(p-1)/2}, M_q \bmod p) = (M_q(2) \pmod p)^{(p-1)/2}$. Mais $M_q(2) = \Phi_q(1) = q$, d'où le résultat.

(d) Tout d'abord, $\mathrm{Res}\,(M_p \pmod p, M_q \pmod p) = \mathrm{Res}\,(M_p, M_q) \pmod p$ car M_p et M_q sont unitaires. Ensuite, $(\mathbf{Z}/p\mathbf{Z})^*$ a exactement $(p-1)/2$ carrés, ce sont les racines de $X^{(p-1)/2} = 1$. Les autres vérifient $X^{(p-1)/2} = -1$ car $X^{p-1} = 1$ et $X^2 = 1$ a exactement deux racines : 1 et -1, distinctes car $p \neq 2$. Par conséquent $q^{(p-1)/2} \pmod p = \left(\frac{q}{p}\right)$. Comme $\mathrm{Res}\,(M_p, M_q) = \pm 1 \equiv \left(\frac{q}{p}\right) \pmod p$, on déduit que $\mathrm{Res}\,(M_p, M_q) = \left(\frac{q}{p}\right)$.

(e) On a $\mathrm{Res}\,(M_q, M_p) = (-1)^{\deg M_p \cdot \deg M_q}\mathrm{Res}\,(M_p, M_q)$, d'après le cours, d'où le résultat.