

Discrete Math, Problem Set (June 21)

REU 2002

Instructor: László Babai

Exercise 1. Let $\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ (where $i = \sqrt{-1}$). This is a complex n^{th} root of unity. Prove that $\omega^k = \omega^\ell$ if and only if $k \equiv \ell \pmod{n}$.

Exercise 2. Prove that $1, \omega, \omega^2, \dots, \omega^{n-1}$ are *all* complex n^{th} roots of unity (i. e., all roots of the polynomial $x^n - 1$).

Exercise 3. Let $\omega_j = \omega^j$. Prove that the order of ω_j is n if and only if $\gcd(j, n) = 1$.

Exercise 4. Prove that the order of ω_j is $\frac{n}{\gcd(j, n)}$.

Exercise 5. Let A_0, \dots, A_{n-1} be a regular n -gon inscribed in a unit circle. Prove $A_0A_1 \cdot A_0A_2 \cdot \dots \cdot A_0A_{n-1} = n$.

Definition 6. The *elementary symmetric polynomials* of x_1, \dots, x_n are

$$\begin{aligned}\sigma_0(x_1, \dots, x_n) &= 1 \\ \sigma_1(x_1, \dots, x_n) &= x_1 + \dots + x_n \\ \sigma_2(x_1, \dots, x_n) &= \sum_{1 \leq i < j \leq n} x_i x_j \quad \left(\binom{n}{2} \text{ terms} \right). \\ \sigma_3(x_1, \dots, x_n) &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k \quad \left(\binom{n}{3} \text{ terms} \right). \\ &\dots \\ \sigma_n(x_1, \dots, x_n) &= x_1 \cdots x_n\end{aligned}$$

Exercise 7. Express $\sum_{i=1}^n x_i^2$ in terms of the first and second elementary symmetric polynomials, $\sigma_1(x_1, \dots, x_n)$ and $\sigma_2(x_1, \dots, x_n)$.

Exercise 8. If f is a polynomial over a field then α is a multiple root of f if and only if $f(\alpha) = f'(\alpha) = 0$.

Exercise 9. Let $f \in \mathbb{R}[x]$ be of the form $f(x) = x^{100} + 5x^{99} + 33x^{98} + \dots$. Prove that not all roots of f are real.

Exercise 10. Prove that $f(x) = x^q - x$ factors into q linear factors (with distinct roots) over \mathbb{F}_q (q a prime power), i. e., $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$.

Exercise 11. For which primes p is the ring $\mathbb{F}_p[\sqrt{-1}]$ a field ?

Exercise 12. Let $f(x) = \prod(x - \alpha_i) = \sum_{i=0}^n a_i x^i$. (Note that $a_n = 1$.) Suppose $\forall i, a_i \in \mathbb{Z}$. (The α_i are complex numbers.) Show that if $g_k(x) = \prod(x - \alpha_i^k)$, then $g_k(x)$ is also a polynomial with integer coefficients.

Exercise 13. Suppose $f \in \mathbb{Z}[x]$ is monic, and $\alpha_1, \dots, \alpha_n$ are the roots of f over \mathbb{C} . Let $s_k = \sum \alpha_i^k$. Show that $s_k \in \mathbb{Z}$.

Exercise 14. (Hermite)

Let $f(x) = \sum_{i=0}^n a_i x^i$ be a monic polynomial of degree n (i.e., $a_n = 1$) with integer coefficients. Suppose all roots of f have unit absolute value. Prove that all roots of f are roots of unity. (In other words, if all algebraic conjugates of a complex algebraic number z have unit absolute value then z is a root of unity.)

Definition 15. ω is a *primitive n^{th} root of unity* if the order of ω is n . (Refer to exercise 2).

Definition 16. The n^{th} *cyclotomic polynomial* is defined as

$$\Phi_n(x) = \prod_{\omega} (x - \omega) \in \mathbb{C}[x]$$

where the product extends over all complex primitive n^{th} roots of unity.

Exercise 17. $\deg(\Phi_n) = \varphi(n)$ (Euler's phi function). *Hint:* Exercise 2

Exercise 18. Prove that n^{th} cyclotomic polynomial has integer coefficients.

Note 19.

$$\begin{aligned}\Phi_1(x) &= x - 1 \\ \Phi_2(x) &= x + 1 = (x^2 - 1)/(x - 1) \\ \Phi_3(x) &= x^2 + x + 1 = (x^3 - 1)/(x - 1) \\ \Phi_4(x) &= x^2 + 1 \\ \Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x - 1) \\ \Phi_6(x) &= x^2 - x + 1 \\ \Phi_7(x) &= (x^7 - 1)/(x - 1) \\ \Phi_8(x) &= x^4 + 1 \\ \Phi_9(x) &= x^6 + x^3 + 1\end{aligned}$$

Exercise 20. Calculate $\Phi_p(x), \Phi_{p^2}(x), \Phi_{p^k}(x), \Phi_{pq}(x), \Phi_{105}(x)$.

Exercise 21. Prove that if $f(x) \in \mathbb{R}[x]$ and $\alpha \in \mathbb{C}$ is a root of $f(x)$, then $\bar{\alpha}$ (conjugate of α) is also a root of f . Moreover, α and $\bar{\alpha}$ have the same multiplicity.

Exercise 22. f is irreducible over \mathbb{R} if and only if $\deg(f) = 1$ or ($\deg(f) = 2$ and discriminant < 0).

Exercise 23. (Gauss Lemma)

If $f \in \mathbb{Z}[x]$ and $f = g \cdot h$ where $g, h \in \mathbb{Q}[x]$ then $f = g_1 \cdot h_1$ with $g_1, h_1 \in \mathbb{Z}[x]$ and $g_1 = cg, h_1 = \frac{1}{c}h$ for some $c \in \mathbb{Q}$. *Hint:* See “Algebra Review,” last section.

Exercise 24.* Prove that the n^{th} cyclotomic polynomial Φ_n is irreducible over \mathbb{Q} . *Hint:* See “Algebra Review,” last section, for hints and related exercises.

Definition 25. 1. Euler’s Phi Function

$$\begin{aligned}\varphi(n) &= \left| \{k \in [n] : \gcd(k, n) = 1\} \right| \\ &= \text{number of positive integers } \leq n \text{ which are relatively prime to } n.\end{aligned}$$

2. Number of positive divisors

$$d(n) = |\{d \in \mathbb{N} : d | n\}|$$

3. Möbius Function

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdots p_k \text{ where the } p_i \text{ are distinct primes (} n \text{ is square-free)} \\ 0 & \text{if } (\exists p)(p^2 | n) \end{cases}$$

4. $\nu(n)$ = number of distinct prime factors. (*Note* change in notation from class.)

5. $\nu^*(n)$ = total number of prime factors (not necessarily distinct)

Exercise 26. Prove $d(n) = \prod_{i=1}^s (k_i + 1)$ for $n = \prod_{i=1}^s p_i^{k_i}$.

Exercise 27. Prove that the arithmetic functions $\varphi(n), \mu(n), d(n), 2^{\nu(n)}, 2^{\nu^*(n)}$ are multiplicative and only $2^{\nu^*(n)}$ is fully multiplicative.

Exercise 28. Let $m(n) = \sum \omega$ where the sum is over the primitive n^{th} roots of unity. Check that $m(n)$ is multiplicative. Find $m(n)$ on the list $\varphi, \mu, d, 2^{\nu}, 2^{\nu^*}$.

Exercise 29. (Van der Waerden)

Prove: the probability that a random polynomial of degree n with integer coefficients is irreducible is 1. (Choose the coefficients a_0, \dots, a_n from $[-k, k]$ at random and prove $\lim_{k \rightarrow \infty} P(a_0 + a_1x + \dots + a_nx^n \text{ is irreducible}) = 1$.)

OPEN QUESTION. *Conjecture:* Almost all polynomials of the form $f(x) = \sum_{i=0}^n a_i x^i$, $a_i = \pm 1$ are irreducible.

Exercise 30. If $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ and $f(\frac{r}{s}) = 0$ for $r, s \in \mathbb{Z}$, $\gcd(r, s) = 1$ then $r | a_0$ and $s | a_n$.

Corollary: Any rational root of a monic polynomial in $\mathbb{Z}[x]$ is an integer dividing the constant term.

Exercise 31. (Cayley-Hamilton Theorem) If $f_A(x)$ is the characteristic polynomial of a matrix A , then $f(A) = 0$. (Hints in Linear Algebra Handout)

Exercise 32. Verify the following formulas (elementary symmetric polynomials of eigenvalues of a matrix expressed as sums of determinants of symmetric matrices)

$$\sigma_k(\lambda_1, \dots, \lambda_n) = \sum \det(M_i)$$

where the summation is over the $k \times k$ symmetric minors of M . ($\binom{n}{k}$ terms)

Definition 33. Two $n \times n$ symmetric matrices A, B are said to be similar (denoted $A \sim B$) if \exists an invertible $n \times n$ matrix S such that $B = S^{-1}AS$.

Exercise 34. If $A \sim B$, then $f_A(x) = f_B(x)$. In particular, $\text{trace}(A) = \text{trace}(B)$ and $\det(A) = \det(B)$.

Exercise 35. Prove : $\text{trace}(AB) = \text{trace}(BA)$. This is true even if A and B are not square matrices: A is $n \times k$ and B is $k \times n$.

Exercise 36. Prove that the eigenvalues of a symmetric real matrix are real.

Theorem 37. (Spectral Theorem) If A is a real symmetric matrix, then there exists an orthogonal matrix S such that $S^{-1}AS$ is diagonal:

$$S^{-1}AS = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

where λ_i are the eigenvalues of A .

Exercise 38. Prove: Spectral Theorem \Leftrightarrow Real symmetric matrix has an Orthonormal basis of eigenvectors (called orthonormal eigenbasis).

Exercise 39. If G is a r -regular graph, prove that r is an eigenvalue of the adjacency matrix of G . Moreover, for all eigenvalues λ_i , $|\lambda_i| \leq r$.

Exercise 40. If G is a *connected* r -regular graph, then $\lambda_1 = r$ has multiplicity one (i. e., for $i \geq 2$, $\lambda_i < r$). Moreover, $\lambda_n = -r$ if and only if G is bipartite.

Definition 41. An **automorphism** of a graph, G , is an isomorphism of G to itself. $\text{Aut}(G)$ denotes the set of automorphisms. Note that this is a subgroup of the symmetric group acting on $V(G)$: $\text{Aut}(G) \leq S_n$.

Exercise 42. Prove: $|\text{Aut}(K_n)| = n!$, $|\text{Aut}(C_n)| = 2n$, $|\text{Aut}(\text{Cube})| = 48$, $|\text{Aut}(\text{Dodecahedron})| = 120$, $|\text{Aut}(\text{Petersen Graph})| = 120$.

Exercise 43. $\text{Aut}(\text{Cube}) \cong S_4 \times \mathbb{Z}_2$. $\text{Aut}(\text{Dodecahedron}) \cong A_5 \times \mathbb{Z}_2$. $\text{Aut}(\text{Petersen Graph}) \cong S_5$.

Exercise 44. Let A be the adjacency matrix of the graph G . Let f_A be the characteristic polynomial of A . Prove that if $f_A(x)$ is irreducible over \mathbb{Q} , then $|\text{Aut}(G)| = 1$.