

DISCRETE MATHEMATICS PROBLEMS. JUNE 19, 2002

INSTRUCTOR: LÁSZLÓ BABAI

Exercise 1. Every subgroup of a cyclic group is cyclic. (This exercise is used in many of the following problems)

Exercise 2. \mathbb{Z}_m is a field if and only if m is prime.

Notation 3. For $a \in \mathbb{Z}$, we denote by $\text{Div}(a)$ the set of all divisors of a .

Theorem 4 (Division Theorem).

$$(\forall a \in \mathbb{Z}) (\forall b \in \mathbb{Z} \setminus \{0\}) (\exists! q, r \in \mathbb{Z}) (a = qb + r \text{ and } 0 \leq r < |b|).$$

These properties uniquely define q and r .

Exercise 5. Prove:

$$(\forall a, b \in \mathbb{Z}) (\exists! d > 0) (\text{Div}(a) \cap \text{Div}(b) = \text{Div}(d)).$$

Show that this uniquely defines d . *Hint:* Use the Division Theorem.

Definition 6. $\text{gcd}(a, b) = d$, where d is the same as in Exercise 5. Define $\text{gcd}(a_1, \dots, a_k)$ analogously.

Exercise 7. Prove: $(\forall a, b \in \mathbb{Z}) (\exists x, y \in \mathbb{Z}) (\text{gcd}(a, b) = ax + by)$.

(i. e., $\text{gcd}(a, b)$ is an *integer linear combination* (a linear combination with integer coefficients) of a and b .)

Exercise 8. \mathbb{Z} is generated (as an additive group) by a_1, \dots, a_k if and only if $\text{gcd}(a_1, \dots, a_k) = 1$.

Now we extend the notion of gcd to polynomials in one variable.

Exercise 9. Define $\text{gcd}(f, g)$ for $f, g \in \mathbb{F}[x]$ analogously to Exercise 5. Prove:

1. such a polynomial exists
2. it is unique up to a constant factor

Notation 10. Let R be a ring, and let $f \in R$. Then $fR := \{f \cdot r \mid r \in R\}$.

Let $A, B \subseteq R$. Then $A + B := \{a + b \mid a \in A, b \in B\}$.

Exercise 11. Let \mathbb{F} be a field, and let $f, g \in R = \mathbb{F}[x]$. Show that $fR + gR = dR$, where $d = \text{gcd}(f, g)$

Exercise 12. If $f \in \mathbb{F}[x]$ and $\deg(f) = k$ then f has at most k roots in F .

Hint: Use the fact that $f(a) = 0$ if and only if $f = (x - a)g$.

Exercise 13. Re-prove $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, for p an odd prime.

Hint: $x^{\frac{p-1}{2}} - 1$ has at most $\frac{p-1}{2}$ roots in \mathbb{F}_p .

Definition 14. Let N be an odd number. Let $N = \prod p_i$, where the p_i are (not necessarily distinct) primes. Let $a \in \mathbb{Z}$. The *Jacobi symbol*, $\left(\frac{a}{N}\right)$ is defined by

$$\left(\frac{a}{N}\right) = \prod \left(\frac{a}{p_i}\right).$$

(Note that if N is prime then both the notation and the definition are the same as the Legendre symbol.) For example,

$$\left(\frac{a}{75}\right) = \left(\frac{a}{3}\right) \left(\frac{a}{5}\right)^2.$$

Exercise 15. Extended QR theorem: if a, b are odd integers, then

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}},$$

where $\left(\frac{*}{*}\right)$ is the Jacobi symbol. *Hint:* Try a prime, $b = pq$.

Exercise 16. If x is an odd integer, then $x^2 \equiv 1 \pmod{8}$

Exercise 17. $\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$ if a is an odd integer.

Hint: Use the fact that the same is true if a is an odd prime.

Exercise 18. $\text{Div}(a) \cap \text{Div}(b) = \text{Div}(a-b) \cap \text{Div}(b)$

Exercise 19. Prove that the Euclidean algorithm takes at most $2n$ rounds on n -bit integers. *Hint:* 2-line proof.

Exercise 20 (Schwartz-Zippel Lemma). Suppose $f(x_1, \dots, x_k)$ has degree at most d . Then either $f = 0$ (identically) or $\Pr(f(\alpha_1, \dots, \alpha_k) = 0 \mid \alpha_i \in \{1, \dots, N\}) \leq \frac{d}{N}$.

Notation 21. Let G be a marriage graph (i. e., an $n+n$ bipartite graph with edges between compatible pairs). The matrix $A(x_{i,j})$ is the $n \times n$ square matrix which has a variable $x_{i,j}$ in the i -th row and j -th column if there is an edge between a_i and b_j in G , and a 0 if there is no edge. The n^2 variables $x_{i,j}$ are all distinct.

Exercise 22. Let $A(x_{i,j})$ be the matrix of a marriage graph. Note that $\det(A(x_{i,j}))$ is a polynomial in $\leq n^2$ variables. Show that $\det(A(x_{i,j})) = 0$ (identically zero) if and only if there is no perfect matching.

Exercise 23. Given a vector $\mathbf{x} = (x_1, \dots, x_n)$, recall that $\|\mathbf{x}\| = \sqrt{x_1^2 + \dots + x_n^2}$. Suppose that H is a Hadamard matrix. Show that $\|H\mathbf{x}\| = \sqrt{n} \|\mathbf{x}\|$

Exercise⁺ 24. Let $H = (h_{ij})$ be a Hadamard matrix; then $|\sum h_{ij}| \leq n^{3/2}$.

Exercise⁺ 25. Recall the Gale-Berlekamp switching game: P1 picks a (± 1) -matrix, and P2 flips some rows and columns (multiplies them by -1), seeking to maximize $|\sum a_{ij}|$.

Show that if P1 and P2 play optimally, then payoff is $\Theta(n^{3/2})$.

Hint: Player 1 needs to pick a good matrix; a Hadamard matrix would work (by the previous exercise) if there exists one of size $n \times n$: what does one do for other n ?

Player 2 needs a clever strategy; perhaps a probabilistic one?

Exercise 26. Recall the divisor game: given n , P1 and P2 take turns picking divisors of n ; divisors of numbers that have already been selected are disallowed. The player forced to pick n loses.

Prove that P1 has a winning strategy.

Hint: Don't try to construct a winning strategy.

Exercise 27. Players take turns placing dimes (nah, pennies – it's cheaper) on a table; once placed, a penny cannot be moved, and pennies cannot overlap. Whoever places the last penny wins.

Display a winning strategy for the first player.

Definition 28. Let $G = (V, E)$ be a graph, let \mathbb{F} be a field, and let d be a positive integer. Let S denote the set of all subspaces of the vector space \mathbb{F}^d . A *projective representation of G over \mathbb{F} of dimension d* is a function $f: V \rightarrow S$ such that any two vertices $u \neq v$ are adjacent if and only if $f(u) \cap f(v) \neq \{0\}$. The *projective dimension of G over \mathbb{F}* is the smallest d for which such a representation exists.

Exercise 29. If the projective dimension of a graph G is d and $|\mathbb{F}|$ is sufficiently large (or infinite) then there exists a projective representation of G in dimension $2d$ such that all subspaces have dimension d .

Exercise 30. If $|\mathbb{F}|$ is sufficiently large (or infinite) then the projective dimension of G is at most twice the maximum degree of G .

OPEN QUESTION. Construct an explicit family of graphs with projective dimension greater than $(\log n)^2$; or better yet, for n^ϵ (where n is the number of vertices). A candidate is the Paley graph.

Exercise 31. If $A_1, \dots, A_m \subset \Omega$, a finite probability space, then $\Pr(\bigcup_{i=1}^m A_i) \leq \sum_{i=1}^m \Pr(A_i)$. Equality holds exactly when the A_i are pairwise disjoint.

Exercise 32. Prove linearity of expectation, i.e., given random variables $\xi, \eta: \Omega \rightarrow \mathbb{R}$, $E(c\xi + \eta) = cE(\xi) + E(\eta)$.