

Discrete Mathematics Problems. June 18, 2002

Instructor: Laszlo Babai

Exercise 1 Let $G(n)$ denote the number of non-isomorphic graphs on n vertices. Show

$$2^{\binom{n}{2}} > G(n) > \frac{2^{\binom{n}{2}}}{n!}$$

Corollary 2 $\log_2(G(n)) \sim n^2/2$

Definition 3 A k -universal graph is a graph which contains every graph on k vertices as an induced subgraph.

An earlier exercise was to prove there exists a k -universal graph with $n = O(k^2 2^k)$ vertices. The next exercise is to find a nearly matching *lower bound*.

Exercise 4 Let U_k be a k -universal graph. Prove:

$$(\forall \epsilon > 0)(\exists k_0)(\forall k \geq k_0) (U_k \text{ must have } \geq (2 - \epsilon)^k \text{ vertices.})$$

Exercise 5 If $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

Definition 6 For $a \in \mathbb{Z}$, the set

$$\bar{a} = a + m\mathbb{Z} = \{a + mk \mid k \in \mathbb{Z}\}$$

is the *residue class of a modulo m*.

Definition 7 A *semigroup* is a set with an *associative* operation.

Definition 8 Let m be a positive integer. The set of mod m residue classes \bar{a} such that $\gcd(a, m) = 1$, is denoted \mathbb{Z}_m^\times . Note that $(\mathbb{Z}_m^\times, \cdot)$ is a semigroup, i. e., \mathbb{Z}_m^\times is *closed* under multiplication. *Euler's φ function* is defined by $\varphi(m) = |\mathbb{Z}_m^\times|$.

Exercise 9 If $m = p_1^{k_1} \cdots p_s^{k_s}$, then

$$\varphi(m)/m = (1 - 1/p_1) \cdots (1 - 1/p_s)$$

Exercise 10 Prove that \mathbb{Z}_m^\times satisfies the *cancellation law* : for a relatively prime to m ,

$$\bar{a}\bar{b} = \bar{a}\bar{c} \Rightarrow \bar{b} = \bar{c},$$

where \bar{x} denotes the residue class of x modulo m . In other words, if $ab \equiv ac \pmod{m}$, and $\gcd(a, m) = 1$ then $b \equiv c \pmod{m}$.

Exercise 11 If a finite semigroup satisfies the cancellation law, then it is a group.

Corollary 12 \mathbb{Z}_m^\times is a group under multiplication.

Exercise 13 If p is a prime, then \mathbb{Z}_p^\times is a cyclic group.

Hint 1: If G and H are finite cyclic groups, then $G \times H$ is cyclic iff $\gcd(|G|, |H|) = 1$ (see Exercise 17 below).

Hint 2: Use Sylow's Theorem, the first part of which is: If p^k is the maximal power of p dividing $|G|$ (i. e., $p^k \mid |G|$ but $p^{k+1} \nmid |G|$), then there is a subgroup of G of order p^k .

Definition 14 A *generator* of \mathbb{Z}_p^\times is called a *primitive root mod p* .

Exercise 15 If p is prime, then

$$x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}.$$

Exercise 16 If p and q are distinct odd primes, then

$$x^2 \equiv 1 \pmod{pq} \not\Rightarrow x \equiv \pm 1 \pmod{pq}.$$

(For every p and q , prove that a counterexample exists.)

Hint: Chinese Remainder Theorem.

Exercise 17 Prove: if p and q are relatively prime, then $\mathbb{Z}_p \times \mathbb{Z}_q$ and \mathbb{Z}_{pq} are isomorphic groups (and even isomorphic rings).

Exercise 18 Suppose p is an odd prime and $a \not\equiv 0 \pmod{p}$. Then $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. *Hint:* Fermat's Little Theorem.

Exercise 19 For p an odd prime, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Hint for first solution: Use a primitive root.

Hint for second solution: Use that the polynomial $x^{(p-1)/2} - 1$ has at most $(p-1)/2$ roots in the field \mathbb{Z}_p .

Exercise 20 Give an algorithm to compute $a^k \pmod{m}$ using $O(\log k)$ arithmetic operations on numbers never exceeding m^2 .

Exercise 21⁺ Prove that $\mathbb{Z}_{p^k}^\times$ is cyclic if p is odd. Check: \mathbb{Z}_8^\times is not cyclic.

Definition 22 Recall the Indian poker game discussed in class. In this game, k players each have an n -bit input written on their foreheads, so that each knows every number except one. The players have a target function f which they are trying to evaluate for the given inputs (f is a function which takes kn $\{0, 1\}$ -valued inputs and returns either 0 or 1). Each player has unlimited *local* computational power, but the players are charged \$1 for every bit they communicate. A *strategy* in this game is a *communication protocol*, which the players arrange before receiving their inputs. Note that the players all know f and may use this when selecting their strategy. The *cost* of a strategy is the maximum over the input space $\{0, 1\}^{kn}$ of the cost (in dollars) to evaluate the function using the strategy (i.e., the cost of a strategy equals the cost of its *worst* input). The *communication complexity* $C_k(f)$ is the cost of the best strategy, i.e.,

$$C_k(f) := \min_{\text{protocols}} \max_{\text{inputs}} \text{cost of computing } f(\text{inputs}) \text{ using the protocol.}$$

Exercise 23⁺ Prove by the probabilistic method that almost all functions $f : \{0, 1\}^{kn} \rightarrow \{0, 1\}$ have $C_k(f) \approx n$. *Hint:* The number of functions available is $2^{2^{kn}}$. Bound the number of communication protocols from above.

OPEN QUESTION Find an *explicit* function $f: \{0, 1\}^{kn} \rightarrow \{0, 1\}$, for $k \geq \log n$, such that $C_k(f) > \log^2 n$.

Exercise 24 Let GIP_3 denote the generalized inner product on triples of n -vectors over \mathbb{Z}_2 :

$$\text{GIP}_3(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{i=1}^n x_i y_i z_i \pmod{2}$$

GIP_k is defined analogously on k -tuples. For $k = \log_2 n + 1$, show that $C_k(\text{GIP}_k) = O(\log n)$.

Definition 25 Let N be an odd number. Let $N = \prod p_i$, where the p_i are (not necessarily distinct) primes. 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 26⁺ (Solovay-Strassen) Suppose N is an odd composite and not a power, i. e., N cannot be written as b^k for any $b \in \mathbb{Z}$ and $k \geq 2$. Show that there exists a such that $\gcd(a, N) = 1$ and $a^{(N-1)/2} \not\equiv \left(\frac{a}{N}\right) \pmod{N}$. (a is a *witness of compositeness* of N .)