CS 170 HW 13

Due **2020-12-02, at 10:00 pm**

Please note that the due date for this homework set is on a Wednesday and not a Monday due to the holiday break. Homework 14 is not currently planned to have a similarly delayed due date; please plan accordingly.

1 Study Group

List the names and SIDs of the members in your study group. If you have no collaborators, you must explicitly write none.

In addition, we would like to share correct student solutions that are well-written with the class after each homework. Are you okay with your correct solutions being used for this purpose? Answer “Yes”, “Yes but anonymously”, or “No”

2 Two Primality Tests

This is a solo question.

Suppose we have access to two primality tests, both of which have the same runtime for n-bit numbers:

- Given x, Test A always outputs x is prime if it is prime, but has a $p_A \leq 1/2$ chance of outputting x is prime if it is composite.
- Given x, Test B always outputs x is composite if it is composite, but has a $p_B \leq 1/2$ chance of outputting x is composite if it is prime.

Recall that the prime number theorem says a fraction $\Theta(1/n)$ of all n-bit numbers are prime. We want to use the following algorithm for sampling primes: repeatedly sample an n-bit number x, and then apply a primality test to x. If the primality test says x is prime, return x, otherwise sample a new prime. Suppose it costs T dollars to run one of these primality tests, and if we accidentally output a composite number, it will cost us L dollars.

What is our asymptotic expected cost if we only use Test A? What is our asymptotic expected cost if we only use Test B? Give an informal description of what your answers imply about when each test would be better to use.

3 Reduction from Factoring to Order-Finding

Recall that for a fixed N, the order of a number of a that is relatively prime to N, $ord_N(a)$, is the smallest positive integer such that $a^{ord_N(a)} \equiv 1 \mod N$.

In this problem, we will show a weaker version of the following statement: we can reduce factoring to order-finding.

(a) Let p be an odd prime and let a be chosen uniformly at random from $\{1, 2, \ldots, p-1\}$. Show that $ord_p(a)$ is even with probability at least $1/2$. (Hint: There is some g such that the sequence $g \mod p, g^2 \mod p, \ldots g^{p-1} \mod p$ is a permutation of $1, 2, \ldots, p-1$, and $ord_p(g) = p-1$).

(b) Fix N that is the product of two odd primes p, q.

The Chinese remainder theorem says that for any a, there is a unique pair $a_1 \in \{0, 1, \dots p-1\}, a_2 \in \{0, 1, \dots q-1\}$ such that $a \equiv a_1 \mod p$ and $a \equiv a_2 \mod q$, and similarly for any a_1, a_2, there is a unique $a \in \{0, 1, \dots, N-1\}$ such that $a \equiv a_1 \mod p$ and $a \equiv a_2 \mod q$.

Let a be chosen uniformly at random from $\{1, 2, \dots, N-1\}$. Using the Chinese remainder theorem, show that with probability at least $3/4$, either a and N share a factor or $ord_N(a)$ is even.

(c) One can show that conditioned on $r = ord_N(a)$ being even, we have $a^{ord_N(a)/2} \not\equiv \pm 1 \mod N$ with probability at least $1/2$. So by sampling a at random, we find a such that either a shares a factor with N or $a^{ord_N(a)/2} \not\equiv \pm 1 \mod N$ with probability at least $3/8$.

Complete the reduction by showing that if we know a, $ord_N(a)$, and $a^{ord_N(a)/2} \not\equiv \pm 1 \mod N$, we can efficiently find a factor of N. (Hint: We can efficiently compute GCDs, so it suffices to show we can find a number that shares a factor with N but is not divisible by N).

4 Intro to Hashing

This is a solo question.

Let $\mathcal{H}$ be a family of hash functions in which each $h \in \mathcal{H}$ maps the universe $\mathcal{U}$ of keys to $[m] := \{0, 1, \dots, m-1\}$. $\mathcal{H}$ is *universal* if for any $x \neq y \in \mathcal{U}$, $\Pr_{h \in \mathcal{H}}[h(x) = h(y)] \leq 1/m$. That is, the chance that $h(x) = h(y)$ if we sample h uniformly at random from $\mathcal{H}$ is at most $1/m$.

Consider the following family of hash functions from $[m] \times [m]$ to $[m]$: Let $h_{a,b}(x_1, x_2) = a \cdot x_1 + b \cdot x_2 \mod m$, and let $\mathcal{H} = \{h_{a,b} | a, b \in [m]\}$. Chapter 1 of the textbook shows this family is universal if m is prime. Show that if m is composite, then there exists $(x_1, x_2) \neq (y_1, y_2)$ such that $h(x_1, x_2) = h(y_1, y_2)$ for at least a $1/\sqrt{m}$ fraction of functions in $\mathcal{H}$, i.e. this family is not universal.