CMSC 250H - Basic Proofs

February 25, 2026

CMSC250H

Review

Diffie Hellman Protocol

Alice and Bob want to communicate a message. They decide on a generator g and a prime p. Secretly, they each pick a "key": Alice picks a and Bob b. They each compute their

$$g^{key} \mod p$$

and send that value to each other. Now, they can raise this value to their own key value to obtain

$$g^{ab} \mod p$$

which is the secret. It is difficult for an eavesdropper, Eve, to find this value, because they can only know $g^a \mod p$ $g^b \mod p$ and it is hard to find the exponent x such that

$$g^x \equiv k \mod p$$

Key Terms

Definition

A generator, g, of a group G (set with a particular operation) is an element in the group such that all other elements can be written as a finite product of g; that is,

$$\forall a \in G, a = g^k$$

for $k \in \mathbb{Z}$

For example, for mod 7, the set we want to consider is $\{1, 2, 3, 4, 5, 6\}$ (this is known as the multiplicative group. 3 is a generator for this group (take its powers and compute mod 7!)

Key Terms

Definition

A generator, g, of a group G (set with a particular operation) is an element in the group such that all other elements can be written as a finite product of g; that is,

$$\forall a \in G, a = g^k$$

for $k \in \mathbb{Z}$

For example, for mod 7, the set we want to consider is $\{1, 2, 3, 4, 5, 6\}$ (this is known as the multiplicative group. 3 is a generator for this group (take its powers and compute mod 7!)

Key Terms

The Discrete Log Problem

An integer k solves the Discrete Log Problem if, for group elements a and b,

$$k = \log_b a \implies b^k = a$$

This is why Diffie Hellman is safe! It is believed Discrete Log is neither in NP or P, in class known as NP-Intermediate.

Key Terms

The Discrete Log Problem

An integer k solves the Discrete Log Problem if, for group elements a and b,

$$k = \log_b a \implies b^k = a$$

This is why Diffie Hellman is safe! It is believed Discrete Log is neither in NP or P, in class known as NP-Intermediate.

Last Lecture

Definition

The **contrapositive** of a statement $p \implies q$ is

$$\neg q \implies \neg p$$

A statement and its contrapositive are logically equivalent, so if we can prove one, we consequently obtain the other.

Last Lecture

Definition

A **proof by contradiction** for statement $p \implies q$ assumes that the statement p is true, with q false. You then logically arrive at a contradiction with your original/natural assumptions (reductio ad absurdum).

Proof that $9^{1/4}$ is Irrational

Work in your tables to prove that $9^{1/4}$ is irrational

Proof that $9^{1/4}$ is Irrational

Proof.

Assume to the contrary that $9^{1/4}$ is rational. Then we can write

$$9^{1/4} = \frac{a}{b} \implies 9 \cdot b^4 = a^4$$

for integers a, b with $\gcd(a, b) = 1$. □

Proof that $9^{1/4}$ is Irrational

Lemma

If 9 *divides* a^4 *then* 3 *divides* a.

Proof.

Since 9 divides a^4, 3 divides a^4. We have 3 cases:

1. $a \equiv 0 \mod 3 \implies a^4 \equiv 0 \mod 3$
2. $a \equiv 1 \mod 3 \implies a^4 \equiv 1 \mod 3$
3. $a \equiv 2 \mod 3 \implies a^4 \equiv 2 \mod 1$

So the only possible way 3 divides a^4 is if 3 divides a. □

Proof that $9^{1/4}$ is Irrational

Proof.

By the lemma we know that 3 divides a, so $a = 3k$ for some integer k. Substituting

$$9 \cdot b^4 = (3k)^4 \implies 3^2 \cdot b^4 = 3^4 k$$

Hence we see that

$$b^4 = 3^2 \cdot k^4 = 9 \cdot k^4$$

So 9 and 3 divides both a and b. But we assumed that $\gcd(a, b) = 1$, a contradiction. □

Unique Factorization

Theorem

Every positive integer can be written as a finite product of prime powers, that is

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

for distinct primes p_i and integers $k_i \geq 0$

Notice that in the previous proof, we used a common factors of a and b to prove the irrationality of $9^{1/4}$. The Unique Factorization Theorem may help us speed that up!

Homework 3

Problem 1:

- This is known as Waring's problem
- It is known that every natural number is the sum of at most 9 cubes. This is known as $g(3) = 9$
- It is known that for sufficiently large n, n can be written as a sum of at most 7 cubes. this is known as $G(3) \leq 7$
- $G(3)$ is conjectured to be smaller, i.e $4 \leq G(4) \leq 7$

Homework 3

Problem 2:

b_3	b_2	b_1	Prime
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Table: Primes ≤ 8

Formula:

$$(\neg b_1 \wedge b_2 \wedge \neg b_3) \vee (b_1 \wedge b_2 \wedge \neg b_3) \vee (b_1 \wedge \neg b_2 \wedge b_3) \vee (b_1 \wedge b_2 \wedge b_3)$$

Homework 3

Showed $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$. Using this we see:

$$\begin{aligned} N(\alpha\beta) &= \alpha\beta \cdot \overline{\alpha\beta} \\ &= \alpha\beta \cdot \overline{\alpha}\overline{\beta} \\ &= \alpha\overline{\alpha} \cdot \beta\overline{\beta} \\ &= N(\alpha) \cdot N(\beta) \end{aligned}$$

Homework 3

Want $N(k) = 1$ for $k \in \mathbb{D}_d = \{a + b\sqrt{d} : a, b \in\}$

a. $\mathbb{D}_3$

$$N(a + b\sqrt{3}) = \pm 1$$
$$(a + b\sqrt{3})(a - b\sqrt{3}) = \pm 1$$
$$a^2 - 3b^2 = \pm 1$$

$a = 7$ and $b = 4$ works so our set is $\{(7 + 4\sqrt{3})^n \quad \text{for all } n \in \mathbb{N}\}$

b. $\mathbb{D}_5$

$$a^2 - 5b^2 = \pm 1$$

$a = 9$ and $b = 4$ works