CS 70 Discrete Mathematics and Probability Theory
Summer 2020 Course Notes

HW 3

Due: Sunday, July 12, 2020 at 10:00 PM
Grace period until Sunday, July 12, 2020 at 11:59 PM

1 Modular Exponentiation

Compute the following. You only need repeated squaring in one of these questions!

(a) $8^{11111} \pmod 9$

(b) $3^{160} \pmod{23}$

(c) $218^3 \pmod 9$

(d) $998^{156} \pmod{13}$

2 Sparsity of Primes

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: this is a Chinese Remainder Theorem problem

3 LOTUS but for CRT

Suppose that p and q are distinct odd primes and a is an integer such that $\gcd(a, pq) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$. *Hint: Use both Fermat's Little Theorem and Chinese Remainder Theorem!*

As an aside, perhaps after doing the problem, see the etymology section of the wiki page on Law of the unconscious statistician to see the derivation of this question's title.

4 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is coprime to p, and p is prime. (Hint: Try to mimic the proof of Fermat's Little Theorem from the notes.)

(b) Now consider the RSA scheme: the public key is $(N = p^2q^2, e)$ for primes p and q, with e relatively prime to $p(p-1)q(q-1)$. The private key is $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Prove that the scheme is correct for x relatively prime to both p and q, i.e. $x^{ed} \equiv x \pmod{N}$. (Hint: Try to mimic the proof of RSA correctness from the notes.)

5 Polynomials over Galois Fields

Real numbers, complex numbers, and rational numbers are all examples of *fields*. A field is a set of numbers that has some nice properties over some operations. Galois fields are fields with only a finite number of elements, unlike fields such as the real numbers. Galois fields are denoted by GF(q), where q is the number of elements in the field.

(a) In the field GF(p), where p is a prime, how many roots does $q(x) = x^p - x$ have? Use this fact to express $q(x)$ in terms of degree one polynomials. Justify your answers.

(b) Prove that in GF(p), where p is a prime, whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

(c) Show that if P and Q are polynomials over the reals (or complex numbers, or rationals) and $P(x)Q(x) = 0$ for all x, then either $P(x) = 0$ for all x, $Q(x) = 0$ for all x, or both. (*Hint*: You may want to prove first this lemma, which is true for all fields: The roots of $R(x) = P(x)Q(x)$ are the union of the roots of P and Q.)

(d) Show that the claim in part (c) is false for finite fields GF(p), where p is a prime.

6 Packet Requirements

In class, we learned that $n + 2k$ packets are required to protect against general errors when using polynomial interpolation methods. The Berlekamp-Welch algorithm provides an efficient method to recover the original message using only $n + 2k$ packets.

Alice is sending Bob a message of length n on a channel with k general errors by interpolating a polynomial through n points. Unfortunately, Bob hasn't watched the lecture on Error-Correcting Codes yet! He only knows about polynomial interpolation. Bob realizes that he needs to determine n points that are uncorrupted, which he can then use to interpolate the polynomial and recover Alice's original message.

Bob decides that he will interpolate polynomials through different combinations of n packets. Then he will compare the polynomials on their respective remaining additional packets to determine which polynomial was interpolated on uncorrupted points.

(a) Prove that with Bob's scheme there is not enough information to recover the original message when fewer than $n + 2k$ packets are sent. You may assume that Bob knows the length of the message, n, and the number of general errors, k. (*Hints*: How can Bob compare the polynomials on the leftover points? What would it mean for there not be enough information to recover the original message?)

(b) Prove that with Bob's scheme there is enough information to recover the original message when $n+2k$ packets or more are sent. You may again assume that Bob knows the length of the message, n, and the number of general errors, k.

7 Alice and Bob

(a) Alice decides that instead of encoding her message as the values of a polynomial, she will encode her message as the coefficients of a degree 2 polynomial $P(x)$. For her message $[m_1, m_2, m_3]$, she creates the polynomial $P(x) = m_1x^2 + m_2x + m_3$ and sends the five packets $(0, P(0))$, $(1, P(1))$, $(2, P(2))$, $(3, P(3))$, and $(4, P(4))$ to Bob. However, one of the packet y-values is changed by Eve before it reaches Bob. If Bob receives

$$(0,1), (1,3), (2,0), (3,1), (4,0)$$

and knows Alice's encoding scheme and that Eve changed one of the packets, can he recover the original message? If so, find it as well as the x-value of the packet that Eve changed. If he can't, explain why. Work in mod 7.

(b) Bob gets tired of decoding degree 2 polynomials. He convinces Alice to encode her messages on a degree 1 polynomial. Alice, just to be safe, continues to send 5 points on her polynomial even though it is only degree 1. She makes sure to choose her message so that it can be encoded on a degree 1 polynomial. However, Eve changes two of the packets. Bob receives $(0,5)$, $(1,7)$, $(2,x)$, $(3,5)$, $(4,0)$. If Alice sent $(0,5)$, $(1,7)$, $(2,9)$, $(3,-2)$, $(4,0)$, for what values of x will Bob not uniquely be able to determine Alice's message? Assume that Bob knows Eve changed two packets. Work in mod 13.

(c) Alice wants to send a length 9 message to Bob. There are two communication channels available to her: Channel A and Channel B. When n packets are fed through Channel A, only 6 packets, picked at random, are delivered. Similarly, Channel B will only deliver 6 packets, picked at random, but it will also corrupt (change the value) of one of the delivered packets. Each channel will only work if at least 10 packets are sent through it. Using each of the two channels once, provide a way for Alice to send her message to Bob.

8 Homework Process and Study Group

Citing sources and collaborators are an important part of life, including being a student! We also want to understand what resources you find helpful and how much time homework is taking, so we can change things in the future if possible.

1. **What sources (if any) did you use as you worked through the homework?**
2. **If you worked with someone on this homework, who did you work with?** List names and student ID's. (In case of homework party, you can also just describe the group.)

3. **How did you work on this homework?** (For example, *I first worked by myself for 2 hours, but got stuck on problem 3, so I went to office hours. Then I went to homework party for a few hours, where I finished the homework.*)

4. **Roughly how many total hours did you work on this homework?**