CS 70 Discrete Mathematics and Probability Theory
Spring 2020

HW 5

Due: Friday, February 28th, 2020 at 11:59 PM
Grace period until Sunday, March 1st, 2020 at 11:59 PM

1 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

2 Breaking RSA

Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find d as the inverse of e mod $(p-1)(q-1)$. This should be easier than factoring N." Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor N (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring N).

3 Quantum Factoring

We're pretty sure that classical computers can't break RSA (because it is hard to factor large numbers on them), but we know that quantum computers theoretically could. In this question, we will prove a fact that is a key part of Shor's Algorithm, a quantum algorithm for factoring large numbers quickly[1].

Let $N = pq$ where p, q are primes throughout this question.

(a) Prove that, for all $a \in \mathbb{N}$, there are only four possible values for $gcd(a, N)$.

(b) Using part (a), prove that, if $r^2 \equiv 1 \mod N$ and $r \not\equiv \pm 1 \pmod{N}$ (i.e. r is a "nontrivial square root of 1" mod N), then $gcd(r-1, N)$ is one of the prime factors of N.
Hint: $r^2 = 1 \mod N$ can be rewritten as $r^2 - 1 = 0 \mod N$ or $(r+1)(r-1) = 0 \mod N$.

4 Recursively Defined Polynomials

Let's define two polynomials $f_1(x) = x - 2$, $f_2(x) = x^2 + 3$, and for each natural number $n \geq 2$, recursively define $f_n(x) = xf_{n-1}(x) - f_{n-2}(x)$.

[1] Read more at `https://en.wikipedia.org/wiki/Shors_algorithm`.

(a) Compute $f_3(x)$ and $f_4(x)$.

(b) First, show that $f_n(x)$ has degree n. Based on this fact, what is the largest number of roots that $f_n(x)$ can have over $\mathbb{R}$? What is the smallest number of roots it can have?

(c) Prove that $f_n(2) = 0 \mod 7$ for every n.

5 Equivalent Polynomials

This problem is about polynomials with coefficients in $\mathrm{GF}(q)$ for some prime $q \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) = g(x)$ for every $x \in \mathrm{GF}(q)$.

(a) Use Fermat's Little Theorem to find a polynomial equivalent to $f(x) = x^5$ over $\mathrm{GF}(5)$; then find one equivalent to $g(x) = 1 + 3x^{11} + 7x^{13}$ over $\mathrm{GF}(11)$.

(b) Prove that whenever $f(x)$ has degree $\geq q$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< q$.

6 Repeated Roots

Let $p(x) = a_k x^k + \cdots + a_0$ be a polynomial in the variable x, where k is a positive integer and the coefficients $a_0, \ldots, a_k$ are from some field F (here, F can be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathrm{GF}(p)$ for some prime p). Let's define this polynomial's **derivative** to be the polynomial $p'(x) := k a_k x^{k-1} + \cdots + a_1 = \sum_{j=1}^{k} j a_j x^{j-1}$. We say that α is a **repeated root of** p if $p(x)$ can be factored as $(x-\alpha)^2 q(x)$ for some polynomial q. Show that α is a repeated root of p if and only if $p(\alpha) = p'(\alpha) = 0$.

[Note: You may be familiar with the derivatives of polynomials from studying calculus, but we are not using any calculus here, because it does not really make sense to perform calculus on finite fields! Think of the polynomial's derivative as a formal definition, i.e., in this context, it has nothing to do with rate of change, etc. In particular, you should not use any calculus rules such as the product rule without proof.]

7 The CRT and Lagrange Interpolation

Let $n_1, \ldots n_k$ be pairwise coprime, i.e. n_i and n_j are coprime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} && (1) \\ x &\equiv a_2 \pmod{n_2} && (2) \\ &\vdots && (\vdots) \\ x &\equiv a_k \pmod{n_k} && (k) \end{aligned}$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

(a) We start by proving the $k=2$ case: Prove that we can always find an integer x_1 that solves (1) and (2) with $a_1=1, a_2=0$. Similarly, prove that we can always find an integer x_2 that solves (1) and (2) with $a_1=0, a_2=1$.

(b) Use part (a) to prove that we can always find at least one solution to (1) and (2) for any a_1, a_2. Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.

(c) Now we can tackle the case of arbitrary k: Use part (b) to prove that there exists a solution x to (1)-(k) and that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$.

(d) For two polynomials $p(x)$ and $q(x)$, mimic the definition of $a \bmod b$ for integers to define $p(x) \bmod q(x)$. Use your definition to find $p(x) \bmod (x-1)$.

(e) Define the polynomials $x-a$ and $x-b$ to be coprime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing x, a_i and n_i with polynomials (using the definition of coprime polynomials just given), show that the system of congruences

$$\begin{aligned} p(x) &\equiv y_1 \pmod{(x-x_1)} && \text{(1')} \\ p(x) &\equiv y_2 \pmod{(x-x_2)} && \text{(2')} \\ &\vdots && (\vdots) \\ p(x) &\equiv y_k \pmod{(x-x_k)} && \text{(k')} \end{aligned}$$

has a unique solution $\pmod{(x-x_1)\cdots(x-x_k)}$ whenever the x_i are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properies are satisfied.

8 GCD of Polynomials

Let $A(x)$ and $B(x)$ be polynomials (with coefficients in $\mathbb{R}$). We say that $\gcd(A(x), B(x)) = D(x)$ if $D(x)$ divides $A(x)$ and $B(x)$, and if every polynomial $C(x)$ that divides both $A(x)$ and $B(x)$ also divides $D(x)$. For example, $\gcd((x-1)(x+1), (x-1)(x+2)) = x-1$. Notice this is the exact same as the normal definition of GCD, just extended to polynomials.

Incidentally, $\gcd(A(x), B(x))$ is the highest degree polynomial that divides both $A(x)$ and $B(x)$. In the subproblems below, you may assume you already have a subroutine divide$(P(x), S(x))$ for dividing two polynomials, which returns a tuple $(Q(x), R(x))$ of the quotient and the remainder, respectively, of dividing $P(x)$ by $S(x)$.

(a) Write a recursive program to compute gcd$(A(x), B(x))$.

(b) Write a recursive program to compute extended-gcd$(A(x), B(x))$.

9 Trust No One

Gandalf has assembled a fellowship of eight people to transport the One Ring to the fires of Mount Doom: four hobbits, two men, one elf, and one dwarf. The ring has great power that may be of use to the fellowship during their long and dangerous journey. Unfortunately, the use of its immense power will eventually corrupt the user, so it must not be used except in the most dire of circumstances. To safeguard against this possibility, Gandalf wishes to keep the instructions a secret from members of the fellowship. The secret must only be revealed if enough members of the fellowship are present and agree to use it.

Requiring all eight members to agree is certainly a sufficient condition to know the instructions, but it seems excessive. However, we also know that the separate races (hobbits, men, elf, and dwarf) do not completely trust each other so instead we decide to require members from at least two races in order to use the ring. In particular, we will require a unanimous decision by all members of one race in addition to at least one member of a different race. That is, if only the four hobbits want to use the ring, then they alone should not have sufficient information to figure out the instructions. Same goes for the two men, the elf, and the dwarf.

More explicitly, some examples: only four hobbits agreeing to use the ring is not enough to know the instructions. Only two men agreeing is not enough. Only the elf agreeing is not enough. Only the dwarf agreeing is not enough. All four hobbits and a man agreeing is enough. Both men and a dwarf agreeing is enough. Both the elf and the dwarf agreeing is enough.

Gandalf has hired your services to help him come up with a secret sharing scheme that accomplishes this task, summarized by the following points:

- There is a party of four hobbits, two men, an elf, and a dwarf.
- There is a secret message that needs to be known if enough members of the party agree.
- The message must remain unknown to everyone (except Gandalf) if not enough members of the party agree.
- If only the members of one race agree, the message remains a secret.
- If all the members of one race agree plus at least one additional person, the message can be determined.

10 Make Your Own Question

Make your own question on this week's material and solve it.

11 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?**