CS 70 Discrete Mathematics and Probability Theory
Summer 2023 Huang, Suzani, and Tausik

HW 3

Due: Jul 13, 2023 11:59pm
Grace period until Jul 14, 2023 11:59pm

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y.

(a) $9x+5 \equiv 7 \pmod{13}$.

(b) Show that $3x+12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x+4y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2023} \equiv x \pmod{12}$.

(e) $7^{62} \equiv x \pmod{11}$.

2 Euler's Totient Function

Note 6

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. We develop a general formula to compute $\phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

(c) Show that if $\gcd(a,b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. (Hint: Use the Chinese Remainder Theorem.)

(d) Argue that if the prime factorization of $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.$$

3 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

4 RSA with CRT

Note 7

Inspired by the efficiency of solving systems of modular equations with CRT, Alice decides to use CRT to speed up RSA!

She first generates the public key (e, N) and private key d as normal, keeping track of the primes $pq = N$. Recall that e is chosen to be coprime to $(p-1)(q-1)$, and d is then defined as $e^{-1} \pmod{(p-1)(q-1)}$. Next, she stores the following values:

$$\begin{aligned} d_p &\equiv d \pmod{p-1} \\ d_q &\equiv d \pmod{q-1} \end{aligned}$$

After receiving an encrypted message $c = m^e \pmod{N}$ from Bob, Alice computes the following expressions:

$$\begin{aligned} x &\equiv c^{d_p} \pmod{p} \\ x &\equiv c^{d_q} \pmod{q} \end{aligned}$$

The message m then calculated as the solution to the above modular system.

(a) Show that this algorithm is correct, i.e. that $x \equiv m$ is the only solution $\pmod{N}$ to the above modular system.

(b) Emboldened by her success in using CRT for RSA, Alice decides to invent a new cryptosystem. To generate her keypair, she first generates $N = pq$. Then, she chooses three numbers g, r_1, r_2 and publishes the public key $(N, g_1 = g^{r_1(p-1)} \pmod N, g_2 = g^{r_2(q-1)} \pmod N)$. Her private key is (p, q).

To encrypt a message, Bob chooses two numbers s_1, s_2 and sends $c_1 = mg_1^{s_1}, c_2 = mg_2^{s_2}$.

Alice decrypts this message by solving the modular system

$$\begin{aligned} x &\equiv c_1 \pmod p \\ x &\equiv c_2 \pmod q \end{aligned}$$

Show that this algorithm is correct, i.e. show that $x \equiv m$ is the only solution $\pmod N$ to the above modular system.

(c) This system is woefully insecure. Show how anyone with access to the public key can recover p, q, given that $g_1 \not\equiv 1 \pmod q$.

5 Equivalent Polynomials

Note 7
Note 8

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

(a) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over $\mathrm{GF}(5)$; then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 70$ over $\mathrm{GF}(11)$.

(b) In $\mathrm{GF}(p)$, prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

6 The CRT and Lagrange Interpolation

Note 6
Note 8

Let $n_1, \ldots n_k$ be pairwise co-prime, i.e. n_i and n_j are co-prime 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 polynomials $p_1(x)$, $p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \bmod q(x)$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.

Define the polynomials $x - a$ and $x - b$ to be co-prime 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 co-prime polynomials just given), show that the system of congruences

$$p(x) \equiv y_1 \pmod{(x - x_1)} \tag{1'}$$
$$p(x) \equiv y_2 \pmod{(x - x_2)} \tag{2'}$$
$$\vdots \tag{\vdots}$$
$$p(x) \equiv y_k \pmod{(x - x_k)} \tag{k'}$$

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 properties are satisfied.

7 Trust No One

Note 8

Gandalf has assembled a fellowship of nine peoples to transport the One Ring to the fires of Mount Doom: five humans, two hobbits, 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.

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 five humans, two hobbits, an elf, and a dwarf, and a secret message that must remain unknown to everyone if not enough members of the party agree.

- A group of people consisting of at least two people from different people classes and at least one people class that is fully represented (i.e., has all members present) can unlock the secret of the ring.

A few examples: only five humans agreeing to use the ring is not enough to know the instructions. One hobbit and four humans is not enough. However, all five humans and one hobbit agreeing is enough. Both hobbits and the dwarf agreeing is enough.