CS 409M : Introduction to Cryptography Fall 2024

Assignment 5
The Theory of Numbers

Instructor: Sruthi Sekar *TAs:* Giriraj Singh, Gyara Pragathi, Nilabha Saha

On Number-Crunching

In this section, we shall largely deal with getting our hands wet crunching numbers just to ensure that we are comfortable with the topics.

Problem 1: Wrestling with Naturals

Compute the following:

1. $89 + 74 \pmod{13}$
2. $29 \cdot 5 \pmod{12}$
3. $9 - 78 \pmod{7}$
4. $7^{-1} \pmod{13}$
5. $3 + 4 \cdot 6^{-1} \pmod{5}$

Problem 2: Using Fermat et Euler

Compute the following using Fermat's Little Theorem or Euler's Theorem [Refer to Problem 6]:

1. $3^{845} \pmod{7}$
2. $89^{-672} \pmod{5}$
3. $5^{139^{8934}} \pmod{12}$

Problem 3: Trip to China

Use the Chinese Remainder Theorem to solve the following systems to linear equations:

1. Solve for general $x \in \mathbb{Z}$.

$$\begin{aligned} x &\equiv 7 \pmod{4} \\ x &\equiv 4 \pmod{7} \\ x &\equiv 2 \pmod{13} \end{aligned}$$

2. Solve for general $x \in \mathbb{Z}$.

$$\begin{aligned} 3x + 7 &\equiv 2 \pmod{13} \\ 2x + 6 &\equiv 1 \pmod{7} \end{aligned}$$

Problem 4: Oh, To Be A Residue!

State whether the following are quadratic residues or non-residues:

1. 5 modulo 7
2. -1 modulo 10

On Mathematics

In this section, we will look at number theory from a mathematical perspective to get you comfortable with the mathematical framework and proofs.

Problem 5: Divisibility Preserved under Integer Combinations

If a divides b, we denote it by $a \mid b$. If a does not divide b, we denote that by $a \nmid b$. Show that if $a, b, c \in \mathbb{Z}$ are such that $a \mid b$ and $a \mid c$, then $a \mid xb + yc$ where $x, y \in \mathbb{Z}$.

Problem 6: Proving Fermat et Euler

We prove two famous results in number theory.
Hint: Use Lagrange's Theorem

1. Prove Fermat's Little Theorem:

   Fermat's Little Theorem

   If p is a prime number and a is an integer not divisible by p, then we have

   $$a^{p-1} \equiv 1 \pmod{p}$$

2. Prove Euler's Theorem:

   Euler's Theorem

   If n is any positive integer and a is an integer such that $\gcd(a, n) = 1$, then we have

   $$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Problem 7: Modular Arithmetic Machinery

We now look at a few operations that are permissible in modular arithmetic.
Throughout these questions, assume that n is a positive integer and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

1. Prove that $a + c \equiv b + d \pmod{n}$.
2. Prove that $a - c \equiv b - d \pmod{n}$.
3. Prove that $a \cdot c \equiv b \cdot d \pmod{n}$

4. Prove that $a^{-1} \equiv b^{-1} \pmod{n}$. Use this to prove that $a \cdot c^{-1} \equiv b \cdot d^{-1} \pmod{n}$.

5. Prove that if $\gcd(a, n) = 1$, then for any integers p, q we have that

$$ap \equiv aq \pmod{n} \implies p \equiv q \pmod{n}$$

Give values of a, p, q, n which establishes a counter-example to the above statement if $\gcd(a, n) \neq 1$.

6. Extending the above subproblem, if $\gcd(a, n) = d$, then show that

$$ap \equiv aq \pmod{n} \implies p \equiv q \pmod{\left(\frac{n}{d}\right)}$$

Problem 8: Legendary Legendre

Let p be an odd prime, and let $\gcd(a, p) = 1$. The *Legendre symbol* (a/p) is defined as

$$(a/p) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic non-residue of } p \end{cases}$$

Prove the following properties of the Legendre symbol (assume the symbol is defined everywhere):

1. If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.
2. If $p \nmid a$, then $(a^2/p) = 1$.
3. $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.
4. $(ab/p) = (a/p)(b/p)$.
5. $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$.

Furthermore, argue that:

a) $(a/p) = 1 \iff a$ is a quadratic residue modulo p.

b) $(a/p) = -1 \iff a$ is a quadratic non-residue modulo p.

Problem 9: The Curious Case of Modular Square Roots

In this problem, we investigate the case of taking modular square roots.
If $x \in \mathbb{Z}_n$ such that $x^2 \equiv a \pmod{n}$, then x is called a square root of a modulo n.

1. Consider the congruence relation

$$x^2 \equiv a \pmod{p}$$

What are all possible values of (a, p) (where p is prime) such that the above congruence admits exactly one solution?

2. For a prime p, show that the aforementioned congruence relation can admit at most 2 solutions.

3. Let $p \equiv 3 \pmod{4}$[1] be a prime. Show that for $a \not\equiv 0 \pmod{p}$, the modular square roots of a are given by $\pm a^{(p+1)/4} \pmod{p}$.

[1] The case of $p \equiv 1 \pmod{4}$ is a little more complicated. Look up the *Tonelli-Shanks* algorithm if you are interested.

Problem 10: Jacobi in the House Tonight

We explore the Jacobi symbol, a generalisation of the Legendre symbol, in this problem.
For any integer a and any positive odd integer $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ (where the p_i's are distinct primes), the Jacobi symbol is defined as the following product of Legendre symbols:

$$(a/n) = (a/p_1)^{\alpha_1} \cdot (a/p_2)^{\alpha_2} \cdot \cdots \cdot (a/p_n)^{\alpha_n}$$

Prove the following properties about the Jacobi symbol:

1. If n is an odd prime, then (a/p) as a Jacobi symbol is same as (a/n) as a Legendre symbol.
2. If $a \equiv b \pmod{n}$, then $(a/n) = (b/n)$.
3. $(a/n) = \begin{cases} 0 & \text{if } \gcd(a,n) \neq 1 \\ +1 \text{ or } -1 & \text{if } \gcd(a,n) = 1 \end{cases}$
4. $(ab/n) = (a/n)(b/n)$.
5. $(a/(mn)) = (a/m)(a/n)$.
6. $(-1/n) = (-1)^{(n-1)/2}$

The Jacobi symbol inherits **some** of the properties of the Legendre symbol when it comes to identifying quadratic residues and non-residues, but **not all** of them.

a) Show that if $(a/n) = -1$, then a is a quadratic non-residue modulo n.

b) Show that if a is a quadratic residue modulo n and $\gcd(a,n) = 1$, then $(a/n) = 1$.

c) Give a counterexample to demonstrate that even if $(a/n) = 1$, a may not be a quadratic residue modulo n. Give a counterexample also in the case when $\gcd(a,n) = 1$.

On Cryptosystems

In this section, we look at applications of number theory to cryptosystems. We only intend to verify the correctness of the cryptosystems here and not look into its security, any formal definitions or background, or any implementational optimisations of the cryptosystem.

Problem 11: Goldwasser-Micali Cryptosystem

The Goldwasser-Micali cryptosystem is a probabilistic public-key cryptosystem for encrypting bits. It works as follows:

- `KeyGen`: Choose secret prime p and q. Choose a such that $(a/p) = (a/q) = -1$. Publish $N = pq$ and a.
- `Enc`: Choose a plaintext $m \in \{0,1\}$. Choose a random $r \in [2, N-1]$. Use the public key (N, a) to compute

  $$c = \begin{cases} r^2 \pmod{N} & \text{if } m = 0 \\ ar^2 \pmod{N} & \text{if } m = 1. \end{cases}$$

  c is the ciphertext.

- `Dec`: Compute (c/p). Decrypt to

$$m = \begin{cases} 0 & \text{if } (c/p) = 1 \\ 1 & \text{if } (c/p) = -1. \end{cases}$$

Prove that this cryptosystem does satisfy perfect correctness, that is, the decryption of an encrypted message always returns the original message with 100% probability.

Advanced Problem: Paillier Cryptosystem

In this problem, we explore the Paillier cryptosystem, which works as follows:

- `KeyGen`:
  1. Choose two large prime numbers p, q randomly and independently of each other such that $\gcd(pq, (p-1)(q-1)) = 1$.
  2. Compute $n = pq$ and $\lambda = \text{lcm}(p-1, q-1)$.
  3. Select a random integer $g \in \mathbb{Z}^*_{n^2}$.
  4. Ensure that n divides the order of g by checking the existence of the following modular multiplicative inverse:

$$\mu = \mathcal{L}([g^\lambda \pmod{n^2}])^{-1} \pmod{n}$$

     where

$$\mathcal{L}(x) = \left\lfloor \frac{x-1}{n} \right\rfloor.$$

  5. The public encryption key is (n, g). The private decryption key is (λ, μ).
- `Enc`:
  1. Let $m \in [0, n)$ be the message to be encrypted.
  2. Select a random $r \in [1, n-1]$ such that $\gcd(r, n) = 1$.
  3. Compute ciphertext as:

$$c = g^m \cdot r^n \pmod{n^2}$$

- `Dec`:
  1. Let $c \in \mathbb{Z}^*_{n^2}$ be the ciphertext to decrypt.
  2. Compute the plaintext as:

$$m = \mathcal{L}([c^\lambda \pmod{n^2}]) \cdot \mu \pmod{n}$$

a) Explain how point 4. of `KeyGen` ensures that n divides the order of g.

b) Show that given the public key parameters, if you could somehow find an r such that $\gcd(r, n) \neq 1$, then you could recover the private key.

c) Prove the perfect correctness of the Pailler cryptosystem.

d) Show that the Paillier cryptosystem is additively homomorphic in the following sense: If m_1 and m_2 are encrypted (under the same key) to obtain ciphertexts c_1 and c_2, respectively, then the decryption of $c_1 c_2 \pmod{n^2}$ would yield $m_1 + m_2 \pmod{n}$.