Homework 3

CS 70, Summer 2024

Due by Friday, July 12th at 11:59 PM

Instructions. Start each problem on a separate page. The subparts of each problem can be on the same page. Every answer should contain a calculation or reasoning. Your answers should be clear, organized, and legible—your final submission should not include scratch work or failed attempts. You must always commit to a final answer; if multiple answers are provided, the most incorrect one will be graded.

If you are completing the homework using LaTeX, you may use the templates. Homeworks must be submitted through Gradescope. See the end of the homework for submission instructions.

Sundry. Before you start writing your final homework submission, state briefly how you worked on it (e.g., if you went to office hours, how frequently you worked on it, etc.). If you worked on the assignment in a group with other students, list their names and email addresses.

1 Properties of the Greatest Common Divisor

Prove each of the following statements about the greatest common divisor.

(a) For any integers $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

(b) For any integers $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

(c) For any positive integer $n \in \mathbb{Z}^+$ and integers $a_1, \ldots, a_n, b \in \mathbb{Z}$, if $\gcd(a_1, b) = \ldots = \gcd(a_n, b) = 1$, then

$$\gcd(a_1 \cdot \ldots \cdot a_n, b) = 1.$$

2 Existing Uniquely in the Chinese Remainder Theorem

The Chinese remainder theorem states that for $n \in \mathbb{N}^+$, $m_1, \ldots, m_n \in \mathbb{Z}^+$ pairwise coprime, and any $a_1, \ldots, a_n \in \mathbb{Z}$, the system of congruences

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ &\vdots \\ x &= a_n \pmod{m_n} \end{aligned}$$

has a unique solution. When $n = 1$, this result is not very interesting. We will prove the result for when there are at least two congruences.

(a) Prove that a solution to the system of congruences exists for $n \geq 2$.

(b) Prove that the solution is unique modulo $m_1 \cdot \ldots \cdot m_n$ for $n \geq 2$.

(Yes, the proofs are in the lecture notes, but they are incomplete. In this question, you will complete the proofs.)

3 The Totient Function

For each positive integer $j \in \mathbb{Z}^+$, let

$$S_j = \left\{k \in \mathbb{N}^+ : k \leq j \text{ and } \gcd(j, k) = 1\right\}$$

be the set of positive integers up to j which are coprime with j. The *totient function* $\varphi : \mathbb{N}^+ \to \mathbb{N}^+$ is defined as

$$\varphi(n) = |S_n|$$

for each $n \in \mathbb{N}^+$. That is, for any $n \in \mathbb{N}^+$, $\varphi(n)$ is the count of positive integers up to n which are relatively prime to n.

In this question, we will use the Chinese remainder theorem to prove that for any coprime moduli $m, n \in \mathbb{N}^+$,

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Let m and n be coprime and consider the function $f : S_{mn} \to S_m \times S_n$ defined as follows. For any $r \in S_{mn}$, we define $f(r) = (r \bmod m, r \bmod n)$.

(a) Prove that this function is well-defined. That is, prove that for any $r \in S_{mn}$, $f(r) \in S_m \times S_n$.

(b) Prove that f is an injection.

(c) Prove that f is a surjection.

(d) Use parts **(a)** through **(c)** to prove that $\varphi(mn) = \varphi(m)\varphi(n)$.

4 Generalizing the Chinese Remainder Theorem

The Chinese remainder theorem applies in the case where the moduli are pairwise coprime. In this question, we investigate systems of linear congruences where the moduli are not necessarily pairwise coprime, and when solutions to such systems exist.

For any moduli $m, n \in \mathbb{Z}^+$ and any integers $a, b \in \mathbb{Z}$, let $d = \gcd(m, n)$ and consider the following system of linear congruences.

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

(a) Prove that if there is a solution to the system of linear congruences, then $d \mid (a - b)$.

(b) Prove that if $d \mid (a - b)$, then there is a solution to the system of linear congruences.

(c) For any integers $a, b \in \mathbb{Z}$, *least common multiple of a and b*, written $\operatorname{lcm}(a, b)$, is the smallest $\ell \in \mathbb{Z}^+$ such that $a \mid \ell$ and $b \mid \ell$.

Let $a, b, c \in \mathbb{Z}$ be any three integers and let $\ell = \operatorname{lcm}(a, b)$. Prove that if $a \mid c$ and $b \mid c$, then $\ell \mid c$.

(d) Prove that the solution to the system of linear congruences is unique modulo $\operatorname{lcm}(m, n)$.

(e) For any moduli $m_1, \ldots, m_n \in \mathbb{Z}^+$ which are not necessarily pairwise coprime and any integers $a_1, \ldots, a_n \in \mathbb{Z}$, consider the following system of linear congruences.

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ &\vdots \\ x &= a_n \pmod{m_n}. \end{aligned}$$

Use parts **(a)** through **(d)** to develop a method to solve such a system of linear congruences or determine that no solution exists. You just need to explain in plain English which steps your method would take—you don't need to express it as a formal algorithm, nor do you have to prove that it works.

(f) Demonstrate that your method from part **(e)** works by using it to find the smallest positive integer solution to the following system of linear congruences.

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 2 \pmod{13} \\ x &\equiv 4 \pmod{18}. \end{aligned}$$

5 RSA Prime Counts

In this question, we will consider the RSA scheme with different numbers of primes.

Suppose Anahit is trying to communicate with Bemidji through an insecure channel on which Evan is eavesdropping. Anahit wants to send messages to Bemidji, but doesn't want Evan to know what they're saying.

(a) Anahit and Bemidji decide to try using an RSA-type scheme involving one prime. Bemidji generates a prime p and an exponent e which is coprime with $p-1$. Bemidji sets his modulus $N = p$ and releases (N, e) as his public key.

To send a message $x \in \{0, \ldots, N-1\}$ to Bemidji, Anahit computes $E(x) = x^e \bmod N$ and sends it through the channel to Bemidji.

Find the decryption function $D(y)$ for this RSA scheme and prove that the scheme with this encryption and decryption works.

(b) Evan knows that Anahit and Bemidji are only using one prime. Explain how Evan can break their encryption.

(c) After Evan breaks their encryption, Anahit and Bemidji decide that to make their encryption extra secure, they'll use three primes.

Bemidji generates three primes, p, q, and r and an exponent e which is coprime with $(p-1)(q-1)(r-1)$. Bemidji sets his modulus $N = pqr$ and releases (N, e) as his public key.

To send a message $x \in \{0, \ldots, N-1\}$ to Bemidji, Anahit computes $E(x) = x^e \bmod N$ and sends it through the channel to Bemidji.

Find the decryption function $D(y)$ for this RSA scheme and prove that the scheme with this encryption and decryption function works.

(d) Explain why this scheme can't be broken the way the scheme from part **(a)** was able to be broken in part **(b)**, even if Evan knows that Anahit and Bemidji are using three primes.

6 Euler's Theorem

In this question, you will prove Euler's theorem, which says that for any modulus $m \in \mathbb{Z}^+$ and integer $a \in \mathbb{Z}$, if a and m are coprime, then

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

where φ is the totient function.

(a) Prove Euler's theorem in the case where $m = p$, a prime.

(b) Let $S_m = \{x_1, \ldots, x_{\varphi(m)}\}$ be the set of positive integers up to m which are coprime to m. Let the function $f : S_m \to S_m$ be defined as

$$f(x) = ax \bmod m$$

for any $x \in S_m$. Prove that this function is well-defined. That is, prove that for any $x \in S_m$, we have that $f(x) \in S_m$.

(c) Prove that f is a bijection.

(d) Use parts **(b)** and **(c)** to prove Euler's theorem.