CS 70 Discrete Mathematics and Probability Theory
Spring 2025 Rao

HW 04

Due: Saturday, 2/22, 4:00 PM
Grace period until Saturday, 2/22, 6:00 PM

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 Celebrate and Remember Textiles

Note 6

You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements on the row lengths of each of the stitch patterns:

- Alternating Link: Multiple of 7, plus 4
- Double Broken Rib: Multiple of 4, plus 2
- Swag: Multiple of 5, plus 2

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns.

Find the *smallest number of stitches* you need to cast on in order to incorporate all three patterns in your baby blanket.

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) We want to show that if $\gcd(a,b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. Let us proceed by direct proof, and assume that $\gcd(a,b) = 1$ for the subparts of this problem.

  (i) Show that for $z \equiv x \pmod{a}$, if $\gcd(x,a) = 1$, then $\gcd(z,a) = 1$.

  (ii) Let X be the set of positive integers $1 \leq i \leq a$ such that $\gcd(i,a) = 1$ (i.e. all numbers in mod a that are coprime to a), and let Y, Z be defined analogously for mod b, ab respectively. Use the Chinese Remainder Theorem to show that there is a bijection between $X \times Y$ and Z.

  (iii) Use the above parts to show that $\phi(ab) = \phi(a)\phi(b)$.

(d) Show 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 Euler's Totient Theorem

Note 6
Note 7

Euler's Totient Theorem states that, if n and a are coprime,

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

where $\phi(n)$ (known as Euler's Totient Function) is the number of positive integers less than or equal to n which are coprime to n (including 1). Note that this theorem generalizes Fermat's Little Theorem, since if n is prime, then $\phi(n) = n - 1$.

(a) Let the numbers less than n which are coprime to n be $S = \{m_1, m_2, \ldots, m_{\phi(n)}\}$. Show that the set

$$S' = \{am_1 \pmod{n}, am_2 \pmod{n}, \ldots, am_{\phi(n)} \pmod{n}\}$$

is a permutation of S. (Hint: Recall the FLT proof.)

(b) Prove Euler's Totient Theorem. (Hint: Continue to recall the FLT proof.)

(c) Note 7 gave two proofs for Theorem 7.1:

$$x^{ed} \equiv x \pmod{N}$$

Use Euler's Totient Theorem to give a third proof of this theorem, for the case that $\gcd(x,N) = 1$.

4 Sparsity of Primes

Note 6

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. We want to find n such that $(n+1)$, $(n+2)$, $\ldots$, and $(n+k)$ are all not powers of primes. We can enforce this by saying that $n+1$ through $n+k$ each must have two distinct prime divisors. In your proof, you can choose these prime divisors arbitrarily.

5 RSA Practice

Note 7

Consider the following RSA scheme and answer the specified questions.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encrypt your answer from part (b) to check its correctness.

6 Tweaking RSA

Note 7

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose $e, d > 1$ in the encryption and decryption function, respectively. Prove the correctness property: the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.