Discrete Mathematics: Homework #4

Due on February 22, 2025 at 4:00pm

Professor Satish Rao

Zachary Brandt
zbrandt@berkeley.edu

Problem 1: Celebrate and Remember Textiles

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.

Solution

Since the numbers 7, 4, and 5 are coprime, we can apply Chinese Remainder Theorem to determine the smallest number of stitches needed. The product of all these multiples is $N = 7 \cdot 4 \cdot 5 = 140$.

$$\begin{aligned}
a_0 b_0 &= \frac{N}{n_0}\left(\frac{N}{n_0}\right)^{-1}_{n_0} = \frac{140}{7}\left(\frac{140}{7}\right)^{-1}_{7} = 20\,(20)^{-1}_7 = 20 \cdot (6) = 120 \\
a_1 b_1 &= \frac{N}{n_1}\left(\frac{N}{n_1}\right)^{-1}_{n_1} = \frac{140}{4}\left(\frac{140}{4}\right)^{-1}_{4} = 35\,(35)^{-1}_4 = 35 \cdot (3) = 70 \\
a_2 b_2 &= \frac{N}{n_2}\left(\frac{N}{n_2}\right)^{-1}_{n_2} = \frac{140}{5}\left(\frac{140}{5}\right)^{-1}_{5} = 28\,(28)^{-1}_5 = 28 \cdot (2) = 56
\end{aligned}$$

Then, our x, or the smallest number of stitches needed, is

$$x = \left(\sum_{i=0}^{k} a_i b_i\right) = (4 \cdot 120 + 2 \cdot 70 + 2 \cdot 56) \equiv 102 \pmod{140}$$

Problem 2: Euler's Totient Function

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 $\phi(ab) = \phi(a)\phi(b)$.

   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

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

Part A

If p is a prime number, $\phi(p)$ will then be $p - 2$ since by definition p will only be divisible by itself and 1, so every other number less than or equal to it will be $\gcd(n,i)$.

Part B

For any p^k, the numbers less than or equal to it that have a greatest common divisor greater than one will be all $p^{k-1}, p^{k-2}, \ldots p$ and their multiples. For example, for 81 (or 3^4), the divisors are 27, 9, 3, and 1, i.e., $3^3, 3^2, 3^1$, and 3^0. So, $\phi(p^k) = p^{k-1}$.

Part C

For part i), assume the contrary. If z is equivalent to x modulos a, and if $\gcd(x,a) = 1$, then z can be expressed as $z = ka + x$. Then, $\gcd(z,a) = \gcd(ka + x, a) = \gcd(a,x) = 1$, using Euclid's algorithm.

For part ii), with the Chinese Remainder Theorem, we can show that there is an x

$$x \equiv i \pmod a$$
$$x \equiv j \pmod b$$

for every (i,j) defined by $X \times Y$, and such there exists a bijection between $X \times Y$ and Z.

For part iii), we know the above and everything from i). $\phi(a)$ is the size of the set of all $1 \leq i \leq a$ where $\gcd(a,i) = 1$. So what is the size of $X \times Y$, well from before we know it's all the possible combos so $|X \times Y| = |X||Y|$. So, since $|X| = \phi(a)$ and $|Y| = \phi(b)$, $|X||Y| = \phi(a)\phi(b) = |X \times Y| = \phi(ab)$.

Part D

The numbers that have a greatest common divisor greater than 1 with p

$$p^k - p^{k-1} = p^k(1 - p^{-1}) = p^k(1 - \frac{1}{p^k})$$

Problem 2 continued on next page...

and then,

$$\phi(n) = \phi(p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}) = \phi(p_1^{e_1})\phi(p_1^{e_1})\dots\phi(p_k^{e_k}) = n\prod_i^k(1-\frac{1}{p^i}) = n\prod_i^k(\frac{p_i-1}{p_i})$$

Problem 3: Euler's Totient Theorem

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 $\gcd(x, N) = 1$.

Part A

Since n and a are coprime, i.e., $\gcd(n, a) = 1$, the numbers in the set S' are all distinct. Since none of the elements in the set S, and the number of elements in the set is $\phi(n) = n - 1$. Therefore, S' is a permutation of S, i.e., it includes all the same elements just in a different order.

Part B

Continuing from the proof of Fermat's Last Theorem, if we take the product of all the numbers in S

$$1 \cdot 2 \cdot \ldots \cdot (n-1) \equiv (n-1)! \pmod{n}$$

But, taking the product of all the numbers in S', the equivalency is

$$a \cdot 2a \cdot \ldots \cdot (n-1)a \equiv a^{n-1}(n-1)! \pmod{n}$$

However, since we know that the numbers in S and S' are the same, the products of both sets' elements must be the same

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

Multiplying both sides of the equivalency by the multiplicative inverse of $(n-1)!$, the equivalency becomes

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

Part C

Problem 4: Sparsity of Primes

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.

Solution

To find an n such that the consecutive sequence of $(n+1), (n+2), \cdots, (n+k)$ of k integers is composed of no prime powers, we need to find a sequence where all the numbers have two distinct prime factors (a prime power, by definition, only has one).

With two times the numbers of consecutive integers for prime number factors we can construct the sequence of equivalencies for Chinese Remainder Theorem

$$\begin{aligned}
n+1 &\equiv 0 \pmod{p_1 p_2} \\
n+2 &\equiv 0 \pmod{p_3 p_4} \\
&\vdots \\
n+k &\equiv 0 \pmod{p_{2k-1} p_{2k}}
\end{aligned}$$

The Chinese Remainder Thereom states that there is such an n for this setup, and we can therefore find a consecutive sequence of non-prime powers.

Problem 5: RSA Practice

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 B) to check its correctness.

Part A

The number d is the multiplicative inverse of e modulos $(p-1)(q-1)$, that is, $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. In our case, d becomes

$$\begin{aligned} d &\equiv e^{-1} \pmod{(p-1)(q-1)} \\ &\equiv 9^{-1} \pmod{(5-1)(11-1)} \\ &\equiv 9 \pmod{40} \end{aligned}$$

Part B

To decrypt the message $y = E(x)$, we must compute $D(y) \equiv y^d \pmod{N}$

$$\begin{aligned} x &\equiv D(y) \pmod{N} \\ &\equiv y^d \pmod{N} \\ &\equiv 4^9 \pmod{55} \\ &\equiv 4^3 \cdot 4^3 \cdot 4^3 \pmod{55} \\ &\equiv 9 \cdot 9 \cdot 9 \pmod{55} \\ &\equiv 26 \cdot 9 \pmod{55} \\ &\equiv 14 \pmod{55} \end{aligned}$$

Part C

From the last part, $x = 14$, to encrypt we need to compute $y = E(x) \equiv x^e \pmod{N}$

$$\begin{aligned} y &\equiv E(x) \pmod{N} \\ &\equiv x^e \pmod{N} \\ &\equiv 14^9 \pmod{55} \\ &\equiv (14^2)^4 \cdot 14 \pmod{55} \\ &\equiv (31^2)^2 \cdot 14 \pmod{55} \\ &\equiv (26)^2 \cdot 14 \pmod{55} \\ &\equiv 16 \cdot 14 \pmod{55} \\ &\equiv 4 \pmod{55} \end{aligned}$$

The encrypted message from part B) decrypted resulted again in 4.

Problem 6: Tweaking RSA

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 $D(E(x)) = x$.

Part A

For correctness, $D(E(x)) \equiv (x^e)^d \pmod{N}$. But in our case, where $N = p$, and not $N = pq$ as usual, $x \equiv x^{ed} \pmod{p}$. d must be such that $ed \equiv 1 \pmod{p-1}$, and can be expressed as $ed = k(p-1)+1$. Fermat's Little Theorem then shows how $x \equiv x^{ed} \pmod{p}$

$$\begin{aligned} x^{ed} &\equiv x^{k(p-1)+1} \pmod{p} \\ &\equiv x^{k(p-1)}x \pmod{p} \\ &\equiv 1 \cdot x \pmod{p} \\ &\equiv x \pmod{p} \end{aligned}$$

Part B

Since p is now known (since $N = p$ and no prime factoring is required) and e is public, Eve can compute d as a multiplicative inverse using Euclid's for

$$ed \equiv 1 \pmod{p-1}$$

Part C

With three primes, e and d become $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$, and $x^{ed} \equiv x \pmod{N}$ still needs to hold where $N = pqr$. ed can then be expressed as $ed = k(p-1)(q-1)(r-1)+1$, which then can be used to show the equivalency of x^ed and x

$$\begin{aligned} x^{ed} &\equiv x^{k(p-1)(q-1)(r-1)+1} \pmod{N} \\ &\equiv x^{k(p-1)(q-1)(r-1)}x \pmod{N} \end{aligned}$$

If a number is divisible by pqr, it is also divisible by any of p, q, and r, then if a number is computed modulo N, it is equivalent modulo of each of N's prime factors. Then for any of the $(p-1), (q-1)$, and $(r-1)$, we can use Fermat's Little Theorem, for example:

$$(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 0 \pmod{p}$$

Therefore, $x^{ed} \equiv x \pmod{N}$ for $N = pqr$.