CS 70 Discrete Mathematics and Probability Theory
Spring 2022 Koushik Sen and Satish Rao **HW 04**

1 Count and Prove

(a) Over 1000 students organized to celebrate running water and electricity. To count the exact number of students celebrating, the chief organizer lined the students up in columns of different length. If the students are arranged in columns of 3, 5, and 7, then 2, 3, and 4 people are left out, respectively. What is the minimum number of students present? Solve it with Chinese Remainder Theorem.

(b) Prove that for $n \geq 1$, if 2021 divides $n^{70} - 1$, then n is not a multiple of 43 or 47. (Hint: what is the prime factorization of 2021?)

Solution:

(a) Let the number of students be x. The problem statement allows us to write the system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7. \end{aligned} \tag{1}$$

To apply CRT, we first find the multiplicative inverse of 5×7 modulo 3, which is 2. This gives us

$$y_1 = (5 \times 7) \times \left((5 \times 7)^{-1} \pmod 3\right) = 35 \times 2 = 70.$$

Second, we compute the multiplicative inverse of 3×7 modulo 5, which is 1. We have

$$y_2 = (3 \times 7) \times \left((3 \times 7)^{-1} \pmod 5\right) = 21 \times 1 = 21.$$

Finally, the the multiplicative inverse of 3×5 modulo 7 is 1. Thus,

$$y_3 = (3 \times 5) \times \left((3 \times 5)^{-1} \pmod 7\right) = 15 \times 1 = 15.$$

By CRT, we can write down the unique solution x (modulo $105 = 3 \times 5 \times 7$):

$$\begin{aligned} x &= a_1 y_1 + a_2 y_2 + a_3 y_3 \pmod{105} \\ &= 2 \times 70 + 3 \times 21 + 4 \times 15 \pmod{105} \\ &= 263 \pmod{105} \\ &= 53 \pmod{105}. \end{aligned}$$

Now, we have $x = 105k + 53$ for some integer k. The smallest k for $x > 1000$ is 10. Thus, the mininum number of students is $105 \times 10 + 53 = 1103$.

(b) Note that $2021 = 43 \times 47$. We wish to prove that if $n^{70} \equiv 1 \pmod{2021}$ then $43, 47 \nmid n$.

Since $n^{70} \equiv 1 \pmod{2021}$, we know that $n^{70} = 2021k + 1$ for some integer k. Thus, we know $n^{70} \equiv 1 \pmod{43}$ and $n^{70} \equiv 1 \pmod{47}$.

We will now prove the statement by contradiction. Let us now assume the contrary; i.e., that $n^{70} \equiv 1 \pmod{2021}$ and either $43 \mid n$ or $47 \mid n$. Then we have 2 possible cases:

- If $43 \mid n$ then, $n = 43k$, which implies $n \equiv 0 \pmod{43}$, which in turn implies $n^{70} \equiv 0 \pmod{43}$,
- If $47 \mid n$ then, $n = 47k$, which implies $n \equiv 0 \pmod{47}$, which in turn implies $n^{70} \equiv 0 \pmod{47}$,

which are all false as under the assumptions that $n^{70} \equiv 1 \pmod{2021}$, since this implies $n^{70} \equiv 1 \pmod{43}$ and $n^{70} \equiv 1 \pmod{47}$. Thus we have reached a contradiction, and we must have that $43, 47 \nmid n$.

Alternate Solution: We can prove the contrapositive. Suppose that both 43 and 47 divide n. Then since 43 and 47 are relatively prime to each other, this means that their product $43 \times 47 = 2021$ divides n, hence $n \equiv 0 \pmod{2021}$ so $n^{70} \equiv 0 \not\equiv 1 \pmod{2021}$.

2 Fermat's Little Theorem

Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

Solution:

Let $n \in \mathbb{N}$. We begin by breaking down 42 into prime factors: $42 = 7 \times 3 \times 2$. Since 7, 3, and 2 are prime, we can apply Fermat's Little Theorem, which says that $a^p \equiv a \pmod{p}$, to get the congruences

$$n^7 \equiv n \pmod{7}, \tag{2}$$
$$n^3 \equiv n \pmod{3}, \quad \text{and} \tag{3}$$
$$n^2 \equiv n \pmod{2}. \tag{4}$$

Now, let's take (3) and multiply it by $n^3 \cdot n$. This gives us

$$n^7 \equiv n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \pmod{3},$$

and since by (3), $n^3 \equiv n \pmod{3}$, this gives

$$n^7 \equiv n \pmod{3}.$$

Similarly, we take (4) and multiply by $n^2 \cdot n^2 \cdot n$ to get

$$n^7 \equiv n^2 \cdot n^2 \cdot n^2 \cdot n \equiv n^4 \pmod{2}.$$

Notice that $n^4 \equiv n^2 \cdot n^2 \equiv n \cdot n \equiv n^2 \pmod 2$, and by (4) $n^2 \equiv n \pmod 2$, so we have

$$n^7 \equiv n \pmod 2.$$

Thus,

$$\begin{aligned} n^7 &\equiv n \pmod 7, && (5) \\ n^7 &\equiv n \pmod 3, \quad \text{and} && (6) \\ n^7 &\equiv n \pmod 2. && (7) \end{aligned}$$

Let $x = n^7 - n$. By the Chinese Remainder Theorem, the system of congruences

$$\begin{aligned} x &\equiv 0 \pmod 7 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 0 \pmod 2 \end{aligned}$$

has a unique solution modulo $2 \cdot 3 \cdot 7 = 42$, and this unique solution is $x \equiv 0 \pmod{42}$. So, we have that $n^7 - n \equiv 0 \pmod{42}$, which means $n^7 - n$ is divisible by 42.

3 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 x such that $x+1, x+2, \ldots, x+k$ are all not powers of primes. We can enforce this by saying that $x+1$ through $x+k$ each must have two distinct prime divisors.

Solution:

We want to find x such that $x+1, x+2, x+3, \ldots, x+k$ are all not powers of primes. We can enforce this by saying that $x+1$ through $x+k$ each must have two distinct prime divisors. So, select $2k$ primes, $p_1, p_2, \ldots, p_{2k}$, and enforce the constraints

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

By Chinese Remainder Theorem, we can calculate the value of x, so this x must exist, and thus, $x+1$ through $x+k$ are not prime powers.

What's even more interesting here is that we could select any $2k$ primes we want!

4 Euler's Totient Function

Euler's totient function is defined as follows:

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

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 $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. (Hint: Use the Chinese Remainder Theorem.)

(d) Argue that if the prime factorization of $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

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

Solution:

(a) Since p is prime, all the numbers from 1 to $p-1$ are relatively prime to p.

So, $\phi(p) = p - 1$.

(b) The only positive integers less than p^k which are not relatively prime to p^k are multiples of p.

Why is this true? This is so because the only possible prime factor which can be shared with p^k is p. Hence, if any number is not relatively prime to p^k, it has to have a prime factor of p which means that it is a multiple of p.

The multiples of p which are $\leq p^k$ are $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. There are p^{k-1} of these.

The total number of positive integers less than or equal to p^k is p^k.

So $\phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$.

(c) Let M be the set of positive integers $1 \leq i \leq m$ such that $\gcd(i,m) = 1$, and let N be the set of positive integers $1 \leq j \leq m$ such that $\gcd(j,n) = 1$. Since $\gcd(m,n) = 1$, the Chinese Remainder Theorem gives that every choice $(i,j) \in M \times N$ corresponds bijectively with an integer $1 \leq k \leq mn$, where $k \equiv i \pmod{m}$ and $k \equiv j \pmod{n}$. Note then that $\gcd(k,m) = \gcd(i,m) = 1$ and $\gcd(k,n) = \gcd(j,n) = 1$. Thus, $\gcd(k,mn) = 1$, so the Chinese Remainder Theorem associates each (i,j) to a unique $1 \leq k \leq mn$ relatively prime to mn.

Moreover, note that each $1 \leq k \leq mn$ relative prime to mn can be associated with an $(i,j) \in M \times N$ such that $k \equiv i \pmod{m}$ and $k \equiv j \pmod{n}$. Thus, we have a bijection between $M \times N$ and the set of positive integers $1 \leq k \leq mn$ relatively prime to mn.

Since $|M| = \phi(m)$, $|N| = \phi(n)$, and the set of positive integers $1 \leq k \leq mn$ relatively prime to mn has cardinality $\phi(mn)$ (by definition), we conclude that $\phi(m)\phi(n) = \phi(mn)$.

(d) Applying part (c) inductively, we conclude that

$$\begin{aligned}\phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\ &= \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1} \\ &= \prod_{i=1}^{k} \frac{p_i - 1}{p_i} p_i^{\alpha_i} \\ &= n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.\end{aligned}$$

5 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).

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

$$\{am_1, am_2, \cdots, am_{\phi(n)}\}$$

is a permutation of the set

$$\{m_1, m_2, \cdots, m_{\phi(n)}\}.$$

In other words, prove that

$$f : \{m_1, m_2, ..., m_{\phi(n)}\} \to \{m_1, m_2, ..., m_{\phi(n)}\}$$

is a bijection, where $f(x) := ax \pmod{n}$.

(b) Prove Euler's Theorem. (Hint: Recall the FLT proof.)

Solution:

(a) This problem mirrors the proof of Fermat's Little Theorem, except now we work with the set $\{m_1, m_2, \cdots, m_{\phi(n)}\}$.

Since m_i and a are both coprime to n, so is $a \cdot m_i$. Suppose $a \cdot m_i$ shared a common factor with n, and WLOG, assume that it is a prime p. Then, either $p|a$ or $p|m_i$. In either case, p is a common factor between n and one of a or m_i, contradiction.

We now prove that f is injective. Suppose we have $f(x) = f(y)$, so $ax \equiv ay \pmod{n}$. Since a has a multiplicative inverse $\pmod{n}$, we see $x \equiv y \pmod{n}$, thus showing that f is injective.

We continue to show that f is surjective. Take any y that is relatively prime to n. Then, we see that $f(a^{-1}y) \equiv y \pmod{n}$, so therefore, there is an x such that $f(x) = y$. Furthermore, $a^{-1}y \pmod{n}$ is relatively prime to n, since we are multiplying two numbers that are relatively prime to n.

(b) Since both sets have the same elements, just in different orders, multiplying them together gives

$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv am_1 \cdot am_2 \cdot \ldots \cdot am_{\phi(n)} \pmod{n}$$

and factoring out the a terms,

$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv a^{\phi(n)} \left(m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)}\right) \pmod{n}.$$

Thus we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

6 RSA Practice

Consider the following RSA schemes and solve for asked variables.

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

Solution:

(a) The private key d is defined as the inverse of $e \pmod{(p-1)(q-1)}$. Thus we need to compute $9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. Find inverse of e mod $(5-1)(11-1) = 40$. Compute $\text{egcd}(40,9)$:

$$\begin{aligned} \text{egcd}(40,9) &= \text{egcd}(9,4) && [4 = 40 \bmod 9 = 40 - 4(9)] \\ &= \text{egcd}(4,1) && [1 = 9 \bmod 4 = 9 - 2(4)]. \\ 1 &= 9 - 2(4). \\ 1 &= 9 - 2(40 - 4(9)) \\ &= 9 - 2(40) + 8(9) = 9(9) - 2(40). \end{aligned}$$

We get $-2(40) + 9(9) = 1$. So the inverse of 9 is 9. So $d = 9$.

(b) 4 is the encoded message. We can decode this with $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. $4^9 \equiv 14 \pmod{55}$. Thus the original message was 14.

(c) The answer from the second part was 14. To encode the number x we must compute $x^e \bmod N$. Thus, $14^9 \equiv 14 \cdot (14^2)^4 \equiv 14 \cdot (31^2)^2 \equiv 14 \cdot (26^2) \equiv 14 \cdot 16 \equiv 4 \pmod{55}$. This verifies the second part since the encoded message was suppose to be 4.

7 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 and d in the encryption and decryption function, respectively. Prove that 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 how you can do so, and include a proof of correctness showing that $D(E(x)) = x$.

Solution:

(a) Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.
We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$.
In other words, $x^{ed} \equiv x \pmod{p}$ for all $x \in \{0, 1, \ldots, N-1\}$.
Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1)+1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

- x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod{p}$.
- x is not a multiple of p: Then

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

, by using FLT.

And for both cases, we have shown that x is recovered by $D(E(x))$.

(b) Since Eve knows $N = p$, and $d \equiv e^{-1} \pmod{p-1}$, now she can compute d using EGCD.

(c) Let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \pmod{(p-1)(q-1)(r-1)}$. People who wish to send me a secret, x, send $y = x^e \pmod{N}$. We decrypt an incoming message, y, by calculating $y^d \pmod{N}$.

Does this work? We prove that $x^{ed} - x \equiv 0 \pmod{N}$, and thus $x^{ed} = x \pmod{N}$.
To prove that $x^{ed} - x \equiv 0 \pmod{N}$, we factor out the x to get
$x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$.

We now show that $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$ is divisible by p, q, and r. Thus, it is divisible by N, and $x^{ed} - x \equiv 0 \pmod{N}$.
To prove that it is divisible by p:

- if x is divisible by p, then the entire thing is divisible by p.
- if x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus it is divisible by p.

To prove that it is divisible by q:

- if x is divisible by q, then the entire thing is divisible by q.
- if x is not divisible by q, then that means we can use FLT on the inside to show that $(x^{q-1})^{k(p-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{q}$. Thus it is divisible by q.

To prove that it is divisible by r:

- if x is divisible by r, then the entire thing is divisible by r.
- if x is not divisible by r, then that means we can use FLT on the inside to show that $(x^{r-1})^{k(p-1)(q-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{r}$. Thus it is divisible by r.