CS 70 Discrete Mathematics and Probability Theory
Summer 2022 Jingjia Chen, Michael Psenka and Tarang Srivastava

HW 3

1 A Number Theoretic Warm-Up

Answer each of the following questions with brief justification.

(a) What is the last digit of 15^{2021}?

(b) What is the inverse of 3 modulo 20?

(c) For how many values of $a \pmod{10}$ does a^{-1} exist modulo 10?

Solution:

(a) Note that the last digit of any odd multiple of 5 is 5, so since 15^{2021} is an odd multiple of 5, its last digit is 5.

(b) We want to find x such that $3x \equiv 1 \pmod{20}$. Since $3 \cdot 7 = 21 \equiv 1 \pmod{20}$, the inverse is 7.

(c) A number hsa an inverse modulo 10 if and only if it is relatively prime to 10, hence the only numbers that don't work are $a \equiv 0, 2, 4, 5, 6, 8$. Thus, $a \equiv 1, 3, 7, 9$ are the only residues that work, so there are 4 values of a that are invertible.

2 CRT Decomposition

In this problem we will find $3^{302} \mod 385$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

(b) Use Fermat's Little Theorem to find $3^{302} \mod p_1$, $3^{302} \mod p_2$, and $3^{302} \mod p_3$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences (modular equations $\mod 385$). Solve the system using the Chinese Remainder Theorem. What is $3^{302} \mod 385$?

Solution:

(a) $385 = 11 \times 7 \times 5$.

(b) Since $3^4 \equiv 1 \pmod 5$, $3^{302} \equiv 3^{4(75)} \cdot 3^2 \equiv 4 \pmod 5$.
Since $3^6 \equiv 1 \pmod 7$, $3^{302} \equiv 3^{6(50)} \cdot 3^2 \equiv 2 \pmod 7$.
Since $3^{10} \equiv 1 \pmod{11}$, $3^{302} \equiv 3^{10(30)} \cdot 3^2 \equiv 9 \pmod{11}$.

(c) $x \equiv 4 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 9 \pmod{11}$.
The answer we get using CRT is $x \equiv 9 \pmod{385}$. So $3^{302} \equiv 9 \pmod{385}$.

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 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod m$ for some $k \geq 0$.

(a) Consider the infinite sequence $a, a^2, a^3, \ldots \pmod m$. Prove that this sequence has repetitions. (**Hint:** Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what is the value of $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

Solution:

(a) There are only m possible values mod m, and so after the m-th term we should see repetitions.

The Pigeonhole principle applies here - we have m boxes that represent the different unique values that a^k can take on $\pmod{m}$. Then, we can view $a, a^2, a^3, \cdots$ as the objects to put in the m boxes. As soon as we have more than m objects (in other words, we reach a^{m+1} in our sequence), the Pigeonhole Principle implies that there will be a collision, or that at least two numbers in our sequence take on the same value $\pmod{m}$.

(b) We will temporarily use the notation a^* for the multiplicative inverse of a to avoid confusion. If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}} && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} && \pmod{m}, \\
a^{i-j} &\equiv 1 && \pmod{m}.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod{m}$ as $a^{i-j-1}a \equiv 1 \pmod{m}$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod{m}$.

5 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) 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

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

6 Using RSA

Kevin and Bob decide to apply the RSA cryptography so that Kevin can send a secret message to Bob.

1. Assuming $p = 3$, $q = 11$, and $e = 7$, what is d? Calculate the exact value.
2. Following part (a), what is the original message if Bob receives 4? Calculate the exact value.

Solution:

(a) $(3-1)(11-1) = 20$, so d is the multiplicative inverse of 7 mod 20. Run egcd$(20,7)$ and get $1 = (-1) \times 20 + (3) \times 7$, so $d = 3$.

Note: You can also try $d = 1, 2, 3, \ldots$ and get $d = 3$.

(b) $N = 3 \times 11 = 33$. $4^d = 4^3 = 64 \equiv 31 \pmod{33}$.

7 Breaking RSA

Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find d as the inverse of e mod $(p-1)(q-1)$. This should be easier than factoring N." Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor N (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring N).

Solution:

Let $a = (p-1)(q-1)$. If Eve knows $a = (p-1)(q-1) = pq - (p+q) + 1$, then she knows

$$N - q - p + 1 = a,$$

$$pq = N.$$

We can write q as $N - p - a + 1$ and substitute into the second equation:

$$p(N - p - a + 1) = N.$$

Then we get the following quadratic function for p:

$$p^2 + (a - N - 1)p + N = 0.$$

We can easily solve this equations and obtain p and q. This is equivalent to factoring N.

8 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

Solution:

$N = pqr$ where p, q, r are all prime. Then, let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \bmod (p-1)(q-1)(r-1)$. People who wish to send me a secret, x, send $y = x^e \bmod N$. I decrypt an incoming message, y, by calculating $y^d \bmod N$.

Does this work? We need to prove that $x^{ed} - x \equiv 0 \pmod{N}$ and thus $x^{ed} \equiv x \pmod{N}$. 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 $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$. As a reminder, we are considering the number: $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$.

We now argue that this number must be 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.

The same reasoning shows that it is divisible by q and r.

One can also use a CRT based argument to argue the correctness of 3 prime RSA. Indeed, as discussed in the previous paragraphs, we need to show that $x^{ed} \equiv x \pmod{N}$, where recall that $N = pqr$. In order to do this, observe that it suffices to prove the following three equivalences:

$$x^{ed} \equiv x \pmod{p}, \tag{1}$$
$$x^{ed} \equiv x \pmod{q}, \tag{2}$$
$$x^{ed} \equiv x \pmod{r}. \tag{3}$$

Why does it suffice? If these 3 statements are indeed true, the uniqueness property established in the CRT implies that $x^{ed} \equiv x \bmod N$. Note that p, q and r are relatively prime so we are allowed to apply the Chinese Remainder Theorem here.

Recall that $e > 1$ is any natural number that is relatively prime to $p-1$, $q-1$ and $r-1$. And d is the multiplicative inverse of e modulo $(p-1)(q-1)(r-1)$. In particular, this means that $ed = k(p-1)(q-1)(r-1)+1$ for some natural number k. Let us try to use this to verify (1):

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

where the last step follows by using Fermat's Little Theorem to claim that for any $a \in \mathbb{N}$, $a^{p-1} \equiv 1 \pmod{p}$. In particular, we choose $a = x^{k(q-1)(r-1)}$ and apply FLT. Note that the original FLT holds with $a = 1, 2, \cdots, p-1$, but we leave it as an exercise to prove that it indeed applies for any natural number $a \in \mathbb{N}$. Thus, we have shown that $x^{ed} \equiv x \pmod{p}$, and a matching argument shows that $x^{ed} \equiv x \pmod{q}$ and $x^{ed} \equiv x \pmod{r}$. This proves equations (1), (2) and (3) and hence shows that $x^{ed} \equiv x \pmod{N}$.