CS 70 Discrete Mathematics and Probability Theory
Spring 2021 HW 4

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 $935 = 5 \times 11 \times 17$ divides $n^{80} - 1$, then 5, 11, and 17 do not divide n.

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 $935 = 5 \times 11 \times 17$. We wish to prove that if $n^{80} \equiv 1 \pmod{935}$ then $5, 11, 17 \nmid n$.

Since $n^{80} \equiv 1 \pmod{935}$, we know that $n^{80} = 935k + 1$ for some integer k. Thus, we know $n^{80} \equiv 1 \pmod{5}$, $n^{80} \equiv 1 \pmod{11}$, and $n^{80} \equiv 1 \pmod{17}$.

We will now prove the statement by contradiction. Let us now assume the contrary; i.e., that $n^{80} \equiv 1 \pmod{935}$ and either $5 \mid n$ or $11 \mid n$ or $17 \mid n$. Then we have 3 possible cases:

- If $5 \mid n$ then, $n = 5k$, which implies $n \equiv 0 \pmod{5}$, which in turn implies $n^{80} \equiv 0 \pmod{5}$,
- If $11 \mid n$ then, $n = 11k$, which implies $n \equiv 0 \pmod{11}$, which in turn implies $n^{80} \equiv 0 \pmod{11}$,
- If $17 \mid n$ then, $n = 17k$, which implies $n \equiv 0 \pmod{17}$, which in turn implies $n^{80} \equiv 0 \pmod{17}$,

which are all false as under the assumptions that $n^{80} \equiv 1 \pmod{935}$, since this implies $n^{80} \equiv 1 \pmod{5}$, $n^{80} \equiv 1 \pmod{11}$, and $n^{80} \equiv 1 \pmod{17}$. Thus we have reached a contradiction, and we must have that $5, 11, 17 \nmid n$.

2 Advanced Chinese Remainder Theorem Constructions

In this question we will see some very interesting constructions that we can pull off with the Chinese Remainder Theorem.

(a) (Sparsity of prime powers) Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

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.

Hint: Remember, this is a Chinese Remainder Theorem problem.

(b) (Divisibility of polynomial) Let $f : \mathbb{N} \to \mathbb{N}$ be a function defined as $f(x) = x^3 + 4x + 1$. Prove that for any positive integer k, there exists a t such that $f(t)$ has k distinct prime divisors.

This is a tricky problem, so here is a little bit of a framework for you. Feel free to approach the problem a completely different way!

Define a *special prime* as a prime p that divides $f(x)$ for some x. First prove that the set of special primes S is infinite. This is similar to the proof that the set of primes is infinite.

Upon doing so, finish the proof off with Chinese Remainder Theorem.

Solution:

(a) 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, this x must exist, and thus, $x+1$ through $x+k$ are not prime powers.

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

(b) We first prove that the set of special primes is infinite. Suppose, for the sake of contradiction, that there are a finite number of special primes, and let's call them $s_1, s_2, \ldots, s_n$ for some n. Let $x = s_1 s_2 s_3 \cdots s_n$. Then, $f(x) = x(x^2+4)+1$. Notice that s_i cannot divide $f(x)$, since it is a multiple of s_i plus 1. Therefore, there must be some other prime that divides $f(x)$, and thus we have found another special prime, contradiction.

This proves that the set of special primes is infinite. Therefore, for any k, we can find special primes p_1 through p_k. In particular, there exists t_1 through t_k such that

$$f(t_i) \equiv 0 \pmod{p_i}$$

for all $1 \leq i \leq k$. Now, by Chinese Remainder Theorem, there exists a t such that

$$t \equiv t_i \pmod{p_i}$$

Since $t \equiv t_i \pmod{p_i}$, we see that $f(t) \equiv f(t_i) \pmod{p_i}$. Therefore, $f(t) \equiv 0 \pmod{p_i}$ for $1 \leq i \leq k$. Thus, $f(t)$ has k distinct primes, as desired.

3 FLT Converse

Recall that the FLT states that, given a prime n, $a^{n-1} \equiv 1 \pmod{n}$ *for all* $1 \leq a \leq n-1$. Note that it says nothing about when n is composite.

Can the FLT condition ($a^{n-1} \equiv 1 \mod n$) hold for some or even all a if n is composite? This problem will investigate both possibilities. It turns out that unlike in the prime case, we need to restrict ourselves to looking at a that are relatively prime to n. (Note that if n is prime, then every $a < n$ is relatively prime to n). Because of this restriction, let's define

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

so $|\,S\,|$ is the total number of possible choices for a. Note that $|S| = \phi(n)$ as well!

(a) Prove that for every a and n that are not relatively prime, FLT condition fails. In other words, for every a and n such that $\texttt{gcd}(n,a) \neq 1$, we have $a^{n-1} \not\equiv 1 \pmod{n}$.

(b) Prove that the FLT condition fails for most choices of a and n. More precisely, show that if we can find a single $a \in S(n)$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, we can find at least $|S(n)|/2$ such a. (Hint: You're almost there if you can show that the set of numbers that fail the FLT condition is at least as large as the set of numbers that pass it. A clever bijection may be useful to compare set sizes.)

The above tells us that if a composite number fails the FLT condition for even one number relatively prime to it, then it fails the condition for most numbers relatively prime to it. However, it doesn't rule out the possibility that some composite number n satisifes the FLT condition entirely: *for all* a relatively prime to n, $a^{n-1} \equiv 1 \mod n$. It turns out such numbers do exist, but they were found through trial-and-error! We will prove one of the conditions on n that make it easy to verify the existence of these numbers.

(c) First, show that if $a \equiv b \mod m_1$ and $a \equiv b \mod m_2$, with $\gcd(m_1, m_2) = 1$, then $a \equiv b \pmod{m_1 m_2}$.

(d) Let $n = p_1 p_2 \cdots p_k$ where p_i are distinct primes and $p_i - 1 \mid n-1$ for all i. Show that $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in S(n)$

(e) Verify that for all a coprime with 561, $a^{560} \equiv 1 \pmod{561}$.

Solution:

(a) Let $c = \texttt{gcd}(n,a) \neq 1$. Clearly $n > 1$, otherwise we would have $\texttt{gcd}(1,a) = 1$. Suppose on the contrary that $a^{n-1} \equiv 1 \pmod{n}$.

Note that $a^{n-1} \equiv 1 \pmod{n}$ if and only if there exists $k \in \mathbb{N}$, $a^{n-1} - nk = 1$. Since $c \mid n$ and $c \mid a$, we must have $c \mid (a^{n-1} - nk)$ for every $k \in \mathbb{N}$. On the other hand $c \neq 1$, thus $c \nmid 1$, contradicting the fact that $a^{n-1} - nk = 1$. As a result, $a^{n-1} - nk \neq 1$ for every $k \in \mathbb{N}$, and thus $a^{n-1} \equiv 1 \pmod{n}$.

(b) The key to this argument is that we've already found one a that breaks the FLT condition. Let N_f be the set of integers coprime with n that fail the FLT condition, and N_p be the set of integers coprime with n that pass it. Note that $N_f \cup N_p = S(n)$, so $| N_f | + | N_p | = | S(n) |$. Therefore, our goal is to show that $|N_f| \geq |N_p|$, so that $|N_p| < \frac{S(n)}{2}$ immediately follows.

Assume there's another number b for which $b^{n-1} \equiv 1 \mod n$, i.e. $b \in N_p$. Consider $(a \cdot b)^{n-1} = a^{n-1} b^{n-1} = a^{n-1} \not\equiv 1 \mod n$, by assumption. So, given any b that satisfies the FLT condition, we can construct a number ab that breaks it! But is $ab \mod n$ unique? Yes, because $ax \mod n$ is a bijection, since $\gcd(a,n) = 1$. So for every $b \in N_p$, $ab \in N_f$, and $| N_p | \leq | N_f |$.

(c) This is a specialized version of the CRT where we can combine the moduli without calculating inverses. If $a = b \mod m_1$, then $a = km_1 + b$ for some k in $\mathbb{Z}$. If $a = b \mod m_2$, then $a = lm_2 + b$ for some $l \in \mathbb{Z}$. We want to relate the two moduli, so rewrite this as $a - b = lm_2$ and

$a-b=km_1$, or $lm_2=km_1$. Since m_1 and m_2 are coprime, $m_1 \mid l \implies l=dm_1$ for some $d \in \mathbb{Z}$. Substituting back in, we find $lm_2=dm_1m_2 \implies a-b=dm_1m_2$. So, $a=b \mod m_1m_2$.

(d) Since p_i are prime, we know that $a^{p_i-1}=1 \mod p_i$. Since $p_i-1 \mid n-1$, $a^{n-1}=a^{j(p_i-1)}=(a^{p_i-1})^j=1 \mod p_i$. This holds for all a coprime with p_i. Thus, if we restrict ourselves to a that are coprime with all p_i, we have a set of k equations $a^{n-1}=1 \mod p_i$. By the last part, we can conclude $a^{n-1}=1 \mod n$, for any a that is coprime with all of the p_i. This condition is the same as a coprime with n, so we've shown n passes the FLT condition for "primality".

(e) $561=3\times 11\times 17$, and $2 \mid 560$, $10 \mid 560$, and $16 \mid 560$. By the above condition, 561 passes the FLT test.

4 Simplifying Some "Little" Exponents

For the following problems, you must both calculate the answers and show your work.

(a) What is $7^{3,000,000,000} \mod 41$?

(b) What is $2^{2017} \bmod 11$?

(c) What is $2^{(5^{2017})} \bmod 11$?

Solution:

(a) Notice that $3,000,000,000$ is divisible by 40. So this is congruent to 1, by Fermat's Little Theorem, i.e. $7^{3,000,000,000} \equiv 7^{40\times 75,000,000} \equiv 1^{75,000,000} \pmod{41} \equiv 1 \pmod{41}$.

(b) By Fermat's Little Theorem, or direct calculation, we see that $2^{10} \equiv 1 \pmod{11}$. Thus, $2^{2017} \equiv 2^{10\times 201+7} \equiv (2^{10})^{201}\times 2^7 \equiv 1^{201}\times 2^7 \equiv 128 \equiv 7 \pmod{11}$.

(c) Building on the idea from the previous part, we just need to determine the exponent's value modulo 10. As the exponent 5^{2017} is divisible by 5, but is not divisible by 2, we have that it must be equal to 5 modulo 10. It follows that $2^{(5^{2017})} \equiv 2^5 \equiv 32 \equiv -1 \equiv 10 \pmod{11}$.

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 $am_1, am_2, \cdots, am_{\phi(n)}$ is a permutation of $m_1, m_2, \cdots, m_{\phi(n)}$. 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 with Just One Prime

Given the message $x \in \{0, 1, \ldots, N-1\}$ and $N = pq$, where p and q are prime numbers, conventional RSA encrypts x with $y = E(x) \equiv x^e \pmod{N}$. The decryption is done by $D(y) \equiv y^d \pmod{N}$, where d is the inverse of $e \pmod{(p-1)(q-1)}$.

Alice is trying to send a message to Bob, and as usual, Eve is trying to decipher what the message is. One day, Bob gets lazy and tells Alice that he will now use $N = p$, where p is a 1024-bit prime number, as part of his public key. He tells Alice that it's okay, since Eve will have to try out 2^{1024} combinations to guess x. It is very likely that Eve will not find out the secret message in a reasonable amount of time! In this problem, we will see whether Bob is right or wrong. Assume that Eve has found out about this new setup and that she knows the public key.

Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{p}$, and $D(y) \equiv y^d \pmod{p}$. Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.

(a) 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 compute d in the decryption function? If so, by what algorithm and approximately how many iterations does it take for it to terminate?

(c) Given part (b), how would Eve recover x and what algorithm would she use? Approximately how many iterations does it take to terminate?

(d) Based on the previous parts, can Eve recover the original message in a reasonable amount of time? Explain.

Solution:

(a) We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$. In other words, $x^{ed} \equiv x \pmod{p}$ $\forall x \in \{0, 1, \ldots, N-1\}$.
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 $x^{ed} \equiv x^{k(p-1)+1} \equiv x^{k(p-1)}x \equiv 1^k x \equiv x \pmod{p}$, by using FLT.

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

(b) Since Eve knows the value of $N = p$, and the fact that $d \equiv e^{-1} \pmod{p-1}$, she can compute d using EGCD. Since EGCD decreases the largest number by at least a factor of two every two iterations, Eve needs at most $2n$ iterations, where n is the number of bits of the larger input. This means at most 2048 iterations.

(c) Since Eve now has d from part 3, and the encrypted message y, she can calculate x directly by using $D(y) = x \equiv y^d \pmod{p}$. She can now use exponentiation by repeated squaring, giving her no more than 1024 iterations.

(d) Assuming each recursive call in EGCD and exponentiation by squaring have reasonable operation time costs, Eve only needs at most 3×1024 iterations, which can easily be done with today's computing power.

7 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:

$$x^{ed} \equiv x \pmod{p}, \tag{2}$$
$$x^{ed} \equiv x \pmod{q}, \tag{3}$$
$$x^{ed} \equiv x \pmod{r}. \tag{4}$$

Why does it suffice? If these 3 statements are indeed true, the uniqueness property established in the CRT implies that $x^{ed} \equiv x \mod N$. 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 (2):

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

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 (2), (3) and (4) and hence shows that $x^{ed} \equiv x \pmod{N}$.