CS 70 Discrete Mathematics and Probability Theory
Summer 2021 HW 2

1 Proctoring Procedures

Please read these proctoring instructions carefully and follow up in the corresponding Piazza thread if you have any questions. When you are finished reading these, please complete the assignment Proctoring Procedures on Gradescope.

2 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.

3 Short Answer: Modular Arithmetic

(a) What is the multiplicative inverse of $n-1$ modulo n? (Your answer should be an expression that may involve n)

(b) What is the solution to the equation $3x = 6 \pmod{17}$?

(c) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n = 2 \pmod{3}$ for $n \geq 1$? (True or False)

(d) Given that $(7)(53) - m = 1$, what is the solution to $53x + 3 = 10 \pmod{m}$? (Answer should be an expression that is interpreted $\pmod{m}$, and shouldn't consist of fractions.)

Solution:

(a) The answer is $n-1 \pmod{n}$. We can see this by noting that it is $-1 \pmod{n}$, or more directly, $(n-1)(n-1) \equiv n^2-2n+1 \equiv 1 \pmod{n}$.

(b) The answer is $x \equiv 2 \pmod{17}$. Muliply both sides by 6 (the multiplicative inverse of 3 modulo 17) and reduce.

(c) The statement is true. We can see this by taking the recursive formula modulo 3. This gives us that $R_n \equiv R_{n-1} \pmod{3}$, hence since $R_1 \equiv 2 \pmod{3}$, every R_i must also be 2 modulo 3.

(d) Note that since $7 \cdot 53 - m = 1$, we can take both sides modulo m and find that $7 \cdot 53 \equiv 1 \pmod{m}$, hence 7 is the inverse of 53 modulo m. Thus, we can solve the equation by subtracting by 3 on both sides and multiplying by 7, giving that $x \equiv 49 \pmod{m}$.

4 Nontrivial Modular Solutions

(a) What are all the possible squares modulo 4? Show that any solution to $a^2+b^2 \equiv 3c^2 \pmod{4}$ must satisfy $a^2 \equiv b^2 \equiv c^2 \equiv 0 \pmod{4}$.

(b) Using part (a), prove that $a^2+b^2 = 3c^2$ has no non-trivial solutions (a,b,c) in the integers. In other words, there are no integers a, b, and c that satisfy this equation, except the trivial solution $a=b=c=0$.

[*Hint:* Consider some nontrivial solution (a,b,c) with the smallest positive value for a (why are we allowed to consider this?). Then arrive at a contradiction by finding another solution (a',b',c') with $a' < a$.]

Solution:

(a) Checking by hand, the only squares modulo 4 are 0 and 1 (for example, $3^2 \equiv 1 \pmod{4}$). Considering the equation $a^2+b^2 \equiv 3c^2 \pmod{4}$, this means that $a^2+b^2 \pmod{4}$ can only be one of the following: 0, 1, 2.

None of these possibilities is consistent with $c^2 \equiv 1 \pmod{4}$, so we must have $c^2 \equiv 0 \pmod{4}$. This forces $a^2 \equiv b^2 \equiv 0 \pmod{4}$, so a^2, b^2, c^2 are all divisible by 4.

(b) We first show that if (a,b,c) is a solution to $a^2+b^2 = 3c^2$, then $a=0$ implies that $b=c=0$. In other words, if $a=0$, then the solution must be trivial. To see why this is the case, suppose that $a=0$. Then b and c need to satisfy $b^2 = 3c^2$. This is only possible if $b=c=0$, as otherwise the right side of the equation would have an odd number of factors of 3, while the left side of the equation would have an even number of factors of 3, which is impossible. Thus, any nontrivial solution must have $a \neq 0$.

Now, notice that if (a,b,c) is a solution to $a^2+b^2 = 3c^2$, then $(-a,b,c)$ is also a solution. Let's assume that some nontrivial solution exists, and (a,b,c) is the solution with the smallest positive value of a. This "smallest" solution must exist by the well-ordering principle. It's not meaningful to consider the solution with the smallest overall value of a because of our first observation that $-a$ is also part of another solution.

If (a,b,c) is a solution to the original equation, then this is also a solution to

$$a^2+b^2 \equiv 3c^2 \pmod 4.$$

From Part (a), we know that a^2,b^2,c^2 are all divisible by 4, which in turn means that a,b,c are all divisible by 2. If we divide the entire original equation by 4, we see that

$$\left(\frac{a}{2}\right)^2+\left(\frac{b}{2}\right)^2=3\left(\frac{c}{2}\right)^2.$$

Indeed, $(a/2,b/2,c/2)$ is another solution with a smaller positive value of a where all the values are integers. We've reached a contradiction to our initial assumption, which was that (a,b,c) was the solution with the least positive value of a. Thus, there does not exist a nontrivial solution to $a^2+b^2=3c^2$.

5 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 $n^{70} \equiv 0 \not\equiv 1 \pmod{2021}$.

6 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 $x+1, x+2, x+3, \dots x+k$ 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, $p_1, p_2, \dots, p_{2k}$, 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 $s_1, s_2, \dots, s_n$ for some n. Let $x = s_1 s_2 s_3 \cdots s_n$. Then, $f(x) = x(x^2+4)+1$. Notice that each s_i cannot divide $f(x)$, since $f(x)$ is a multiple of that 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 $1 \le i \le k$. 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 $1 \le i \le k$. Thus, $f(t)$ has k distinct primes, as desired.

7 Tweaking RSA

(a) 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 $x \in \{0,1,\dots,N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$. 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 $x \in \{0,1,\dots,N-1\}$.
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.