CS 70 Discrete Mathematics and Probability Theory
Summer 2021 HW 2

Due: Sunday 7/11, 10:00 PM
Grace period until Sunday 7/11, 11:59 PM

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

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?

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.)

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 $a' < a$.]

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?)

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.

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 $x \in \{0,1,\ldots,N-1\}$, $E(x) \equiv x^e \pmod{N}$, 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 $D(E(x)) = x$.