CS 70 Discrete Mathematics and Probability Theory
Spring 2019 Satish Rao and Babak Ayazifar

HW 4

Due: Monday, February 25, 2019 at 10 PM

Sundry

Before you start your homework, 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 Bijective or not?

Decide whether the following functions are bijections or not. Please prove your claims.

(a) $f(x) = 10^{-5}x$

   (i) for domain $\mathbb{R}$ and range $\mathbb{R}$

   (ii) for domain $\mathbb{Z} \cup \{\pi\}$ and range $\mathbb{R}$

(b) $f(x) = \{x\}$, where the domain is $D = \{0, \dots, n\}$ and the range is $\mathscr{P}(D)$, the powerset of D (that is, the set of all subsets of D).

(c) Consider the number $X = 1234567890$, and obtain X' by shuffling the order of the digits of X. Is $f(i) = (\mathrm{i}+1)^{\text{st}}$ *digit of* X' a bijection from $\{0, \dots, 9\}$ to itself?

(d) $f(x) = x^5 \pmod{187}$, where the domain is $\{0, 1, 2, 3, \dots, 186\}$ and the range is $\{0, 1, 2, 3, \dots, 186\}$.

(e) $f(x) = x^3 \pmod{187}$, where the domain is $\{0, 1, 2, 3, \dots, 186\}$ and the range is $\{0, 1, 2, 3, \dots, 186\}$.

2 Functional Equation

Usually, in math problems, we give you a function f and ask you to prove some properties about it. Here, we're going to flip it around: we tell you the property of the function f, and you will try to find all functions that have said property.

Let $f : \mathbb{R} \to \mathbb{R}$ be a function that satisfies the following equation for all x and y:

$$f(f(x)^2 + f(y)) = xf(x) + y \tag{1}$$

We will find all functions f that satisfy this property.

(a) First, show that there exists a x_0 such that $f(x_0) = 0$. As a hint, you know that equation (1) is true for all x and y, so try plugging in some specific values of x and y to see if you get anywhere.

(b) Leverage the previous part to get that $f(f(y)) = y$ for all $y \in \mathbb{R}$.

(c) Prove that for any function g, if $g(g(y)) = y$, then g is bijective.

(d) Plug in $x = f(t)$ into (1). Also plug in $x = t$ into (1). You can simplify your equations using the fact proven in part (b). Combine these two equations, use the fact that f is bijective, to conclude that $f(t)^2 = t^2$ for all t.

(e) Use the previous part to find all functions f that satisfy equation (1). Note that it is not as simple as taking the square root of both sides! Justify your answer.

3 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)

4 FLT Converse

Recall that the FLT states that, given a prime n, $a^{n-1} \equiv 1 \pmod{n}$ *for all* $1 \le a \le n-1$. 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

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

so $\mid S \mid$ 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, $a^{560} \equiv 1 \pmod{561}$.

5 Mechanical Chinese Remainder Theorem

In this problem, we will solve for x such that

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

(a) Find a number $0 \leq b_2 < 30$ such that $b_2 \equiv 1 \pmod{2}$, $b_2 \equiv 0 \pmod{3}$, and $b_2 \equiv 0 \pmod{5}$.

(b) Find a number $0 \leq b_3 < 30$ such that $b_3 \equiv 0 \pmod{2}$, $b_3 \equiv 1 \pmod{3}$, and $b_3 \equiv 0 \pmod{5}$.

(c) Find a number $0 \leq b_5 < 30$ such that $b_5 \equiv 0 \pmod{2}$, $b_5 \equiv 0 \pmod{3}$, and $b_5 \equiv 1 \pmod{5}$.

(d) What is x in terms of b_2, b_3, and b_5? Evaluate this to get a numerical value for x.

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 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.