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

HW 4

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 $D = \{0, \ldots, n\}$ 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 $\{0, \ldots, 9\}$ to itself?

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

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

Solution:

(a) It is bijective for (i), but fails to be surjective in (ii):

  (i) Firstly, it is injective because if $f(x) = f(y)$, then $10^{-5}x = 10^{-5}y$ and so multiplying by 10^5 on both sides, we get $x = y$, so no two real numbers can be mapped to the same real numbers. Secondly, it is surjective, because for any $y \in \mathbb{R}$, we have $f(10^5 y) = 10^{-5} \cdot 10^5 y = y$, so each y has an $x = 10^5 y$ that maps to it.

  (ii) f is injective for the same reason as above, but it is not a surjection, since the only $x \in \mathbb{R}$ that maps to e.g. 10^{-6} is $x = 10^{-1} \notin \mathbb{Z} \cup \{\pi\}$.

(b) f is injective, but not surjective. There exists a subset $S \subset D$ containing at least two elements of D (in the case of $n = 0$, the two elements are the empty set and 0 itself). However, $f(x)$ always contains exactly one element. Hence there is no $x \in D$ that gets mapped to S.

(c) Yes. Let us show injectivity by noticing that each number between 0 and 9 occurs precisely once in X, and thus precisely once in X' too. As a result, no two digits of X' can be the same. Surjectivity follows from similar reasoning: Since any fixed number $y \in \{0, \ldots, 9\}$ is a digit of X, it must be a digit of X' too, let's call that digit the i_y^{th} digit. Then $f(i_y) = y$.

(d) Not injective nor surjective. Notice that $187 = 11 \cdot 17$. Recall from the proof of correctness of RSA that $a^{1+k(p-1)(q-1)} \equiv a \pmod{pq}$ for primes p and q. Therefore, $2^{10 \cdot 16} \equiv 1 \pmod{187}$. Hence, $f(2^{2 \cdot 16} \pmod{187}) = f(1) = 1$.

(e) This is bijective. Note that this is the encryption function for RSA, where the public key is $(187, 3)$. Since 3 is relatively prime to $(11-1)(17-1)$, we know that there is a private key $d = 3^{-1} \pmod{160}$ such that $x^{3d} \equiv x \pmod{187}$.

Suppose $f(x) = f(y)$. That means $x^3 \equiv y^3 \pmod{187}$. Raise both sides to the d-th power to obtain $x = y$. This proves f is injective.

Take any y in the range. We can construct an x such that $f(x) = y$, by letting $x = y^d$. Then, we know that $f(x) = y^{3d} = y \pmod{187}$, as desired.

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.

Solution:

(a) Since we know the equation holds for all x and y, we know that (let $x = y = 0$):

$$f(f(0)^2 + f(0)) = 0$$

Let $x_0 = f(0)^2 + f(0)$. This proves the desired statement.

(b) Plugging in $x = x_0$ into 1 gives us

$$f(f(y)) = y$$

as desired, since $f(x_0) = 0$.

(c) We first show g is injective. If $g(a) = g(b)$, then $g(g(a)) = g(g(b))$. This means that $a = b$, hence, g is injective.

We now show g is surjective. Let b be any real number. Then, $g(g(b)) = b$, so there exists an input r such that $g(r) = b$, namely, $r = g(b)$.

(d) Plugging in $x = f(t)$ yields

$$f(f(f(t))^2 + f(y)) = f(t) \cdot f(f(t)) + y$$
$$f(t^2 + f(y)) = t \cdot f(t) + y$$

where we used the fact that $f(f(t)) = t$ for all t. Plugging in $x = t$ gives us

$$f(f(t)^2 + f(y)) = t \cdot f(t) + y$$

Therefore, $f(t^2 + f(y)) = f(f(t)^2 + f(y))$ and using the injectivity of f, we know that

$$t^2 + f(y) = f(t)^2 + f(y) \Rightarrow f(t)^2 = t^2$$

(e) The previous part tells us that $f(t) = t$ or $f(t) = -t$ **for each** t. However, we could get $f(a) = a$ for some a and $f(b) = -b$ for some b. Sometimes this is called a pointwise trap.

Let's now show that this cannot happen. Suppose for contradiction there exists such nonzero a and b such that $f(a) = a$ and $f(b) = -b$. Plug in $x = a$ and $y = b$. We get $f(f(a)^2 + f(b)) = af(a) + b$. By definition,

$$f(a^2 - b) = a^2 + b$$

Since $f(a^2 - b) = a^2 - b$ or $-a^2 + b$, we can try each of these cases and observe that one of a or b must be 0.

Therefore, we see that the solutions are $f(x) = x$ or $f(x) = -x$.

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)

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 $a^{\phi(n)} \equiv 1 \pmod{n}$.

4 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 $c = \gcd(n, a) \neq 1$. Clearly $n > 1$, otherwise we would have $\gcd(1, a) = 1$. 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 $lm_2 = dm_1 m_2 \implies a - b = dm_1 m_2$. So, $a = b \mod m_1 m_2$.

(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.

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.

Solution:

(a) In order to make sure that $b_2 \equiv 0 \pmod 3$, we just need to make b_2 a multiple of 3–so we can start with just $b_2 = 3$. However, we now need to make sure we satisfy $b_2 \equiv 1 \pmod 2$, so we multiply this by $3^{-1} \pmod 2$. Since $3 \equiv 1 \pmod 2$, this is just 1. Thus, we so far have $b_2 = 3 \cdot 1$. We now need to make sure b_2 is a multiple of 5 (ie, is equivalent to zero mod 5), so we multiply our current value for b_2 by 5. But now we again need to make sure that b_2 is still equivalent to 1 mod 2, so we multiply by $5^{-1} \pmod 2$, which will again just be 1. Finally, we get $b_2 = 3 \cdot 1 \cdot 5 \cdot 1 = 15$.

(b) Similar to the previous part, we make b_3 just be $2 \cdot (2^{-1} \pmod 3) \cdot 5 \cdot (5^{-1} \pmod 3)$. We have that $2^{-1} \equiv 2 \pmod 3$ and $5^{-1} \equiv 2^{-1} \equiv 2 \pmod 3$, so $b_3 = 2 \cdot 2 \cdot 5 \cdot 2 = 40$. Reducing this to a number modulo 30, we get $b_3 = 10$.

(c) As before, we get $b_5 = 2 \cdot (2^{-1} \pmod 5) \cdot 3 \cdot (3^{-1} \pmod 5)$. Plugging in $2^{-1} \equiv 3 \pmod 5$ and $3^{-1} \equiv 2 \pmod 5$, we get $b_5 = 2 \cdot 3 \cdot 3 \cdot 2 = 36$. Since we want a number modulo 30, we reduce this to $b_5 = 6$.

(d) We can write $x = b_2 + 2b_3 + 3b_5$. This ensures that when we take x modulo 2, we end up getting $x \equiv b_2 + 2b_3 + 3b_5 \equiv 1 + 2(0) + 3(0) \equiv 1 \pmod 2$ as we expected–and similar statements can be made for the other two moduli. Evaluating this numerically, we get that $x = 15 + 2(10) + 3(6) = 53$. Reducing this to a number mod 30, we get $x = 23$.

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 $x+1, x+2, x+3, \ldots x+k$ 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.

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.

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