

BIJECTIONS, FLT, CRT, RSA 3

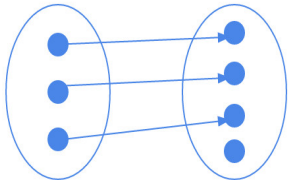
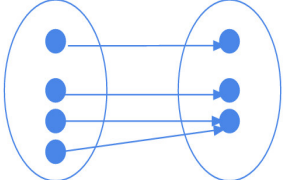
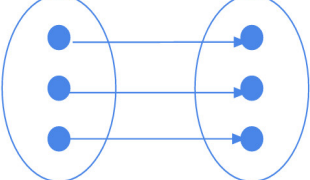
COMPUTER SCIENCE MENTORS 70

September 18 to September 22, 2017

1 Bijections

1.1 Introduction

1. Draw an example of each of the following situations

One to one AND NOT onto (injective but not surjective)	Onto AND NOT one to one (surjective but not injective)	One to one AND onto (bijection, i.e. injective AND surjective)
Solution: . 	Solution: . 	Solution: . 

2. Describe a function that is injective but not surjective and the set over which this applies. How about a function that is surjective but not injective?

Solution: ex: $e^x: \mathbb{R} \rightarrow \mathbb{R}$ is injective (one to one) but not surjective (onto) because while all real numbers map to something, nothing will map to 0 and negative numbers. x2: $x^2: \mathbb{R} \rightarrow \mathbb{R}^+$ is surjective (onto) but not injective (one to one) because

while all positive real numbers have something mapping to them, 4 has -2 and 2 mapping to it.

Note 1: Z_n denotes the integers mod n : $\{0, \dots, n-1\}$

Note 2: in the following questions, the appropriate modulus is taken after applying the function

1.2 Questions

1. Are the following functions **bijections** from Z_{12} to Z_{12} ?

a. $f(x) = 7x$

Solution: Yes: the mapping works, since 7 is coprime to 12, so there exists a multiplicative inverse to 7 in Z_{12} ($7x7 = 49 \bmod 12 = 1$, so $f^{-1}(x) = 7x$), which only occurs if the function is a bijection.

b. $f(x) = 3x$

Solution: No: $f(0) = f(4) = 0$.

c. $f(x) = x - 6$

Solution: Yes: can see its just $f(x) = x$, shifted by 6

2. Are the following functions **injections** from Z_{12} to Z_{24} ?

a. $f(x) = 2x$

Solution: Yes: any two x_1 and x_2 will not equal each other as long as $x_1 \neq x_2$

b. $f(x) = 6x$

Solution: No: 0 and 4 both map to 0

c. $f(x) = 2x + 4$

Solution: Yes: same as $2x$, except shifted

3. Are the following functions **surjections** from Z_{12} to Z_6 ? (Note: that $\lfloor x \rfloor$ is the floor operation on x)

a. $f(x) = \lfloor \frac{x}{2} \rfloor$

Solution: Yes: plug in every even number 0

b. $f(x) = x$

Solution: Yes: plug in 0 through 5

c. $f(x) = \lfloor \frac{x}{4} \rfloor$

Solution: No: the largest value we can get is $f(12)$ which equals 3

4. Why can we not have a surjection from Z_{12} to Z_{24} or an injection from Z_{12} to Z_6 ?

Solution: Because there are more values in Z_{24} than Z_{12} , it is impossible to cover all the values in Z_{24} with mapping from Z_{12} . Similarly, because there are more values in Z_{12} than Z_6 , there is not a unique element in Z_6 to assign to every Z_{12} .

2 Fermat's Little Theorem

2.1 Introduction

Fermat's Little Theorem: For any prime p and any $a \in \{1, 2, \dots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$

1. Prove Fermat's Little Theorem.

Solution: Proof from notes:

Claim: The function $a * x \pmod{p}$ is a bijection where $x \in \{1, 2, \dots, p-1\}$

The domain and range of the function are the same set, so it is enough to show that if $x \neq x'$ then $a * x \pmod{p} \neq a * x' \pmod{p}$.

Assume that $a * x \pmod{p} \equiv a * x' \pmod{p}$.

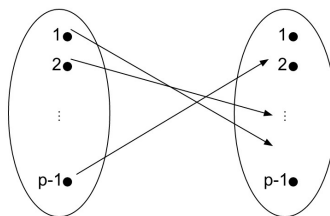
Since $\gcd(a, p) = 1$, a must have an inverse: $a^{-1} \pmod{p}$

$$ax \pmod{p} \equiv ax' \pmod{p}$$

$$a^{-1} * a * x \pmod{p} \equiv a^{-1} * a * x' \pmod{p}$$

$$x \pmod{p} \equiv x' \pmod{p}$$

This contradicts our assumption that $x \neq x' \pmod{p}$. Therefore f is a bijection. We want to use the above claim to show that $a^{p-1} \equiv 1 \pmod{p}$. Note that now we have the following picture:



So if we multiply all elements in the domain together this should equal the product of all the elements in the image:

$$1 * 2 * \dots * (p-1) \pmod{p} \equiv (1a) * (2a) * \dots * ((p-1)a) \pmod{p}$$

$$(p-1)! \pmod{p} \equiv a^{p-1} * (p-1)! \pmod{p}$$

$$1 \equiv a^{p-1} \pmod{p}$$

2.2 Questions

1. Find $3^{5000} \bmod 11$

Solution:

$$(3^{10})^{500} \bmod 11 = 1^{500} \bmod 11 = 1$$

2. Show that $n^7 - n$ is divisible by 42 for any integer n

Solution: $42 = 7 * 3 * 2 \leftarrow$ these factors are prime so lets apply FLT!!

$$n^7 \equiv n \pmod{7}$$

$$n^3 \equiv n \pmod{3}$$

$$n^2 \equiv n \pmod{2}$$

We're interested in n^7 so let's modify the bottom two equations to write n^7 in mod 3 and mod 2

$$n^7 \equiv n^3 * n^3 * n \equiv n * n * n \equiv n^3 \equiv n \pmod{3}$$

$$n^7 \equiv n \pmod{3}$$

$$n^7 \equiv n^2 * n^2 * n^2 * n \equiv n * n * n * n \equiv n^2 * n^2 \equiv n * n \equiv n^2 \equiv n \pmod{2}$$

$$n^7 \equiv n \pmod{2}$$

$$n^7 \equiv n \pmod{7}$$

$$n^7 \equiv n \pmod{3}$$

$$n^7 \equiv n \pmod{2}$$

Wouldn't it be great if the above equations implied that $n^7 \equiv n \pmod{7 * 3 * 2}$?

Let's try to prove that.

Claim: If

$$x \equiv y \pmod{a_1}$$

$$x \equiv y \pmod{a_2}$$

...

$$x \equiv y \pmod{a_n}$$

are true and a_1, \dots, a_n are coprime then $x \equiv y \pmod{a_1 a_2 \dots a_n}$
 $x \equiv y \pmod{a_i} \rightarrow x = y + c_i * a_i$ for some constant c_i

$$x = y + c_1 * a_1$$

$$x = y + c_2 * a_2$$

...

$$x = y + c_n * a_n$$

But this implies that $x = c * lcm(a_1, \dots, a_n) + y$

Since a_1, \dots, a_n are coprime, $lcm(a_1, \dots, a_n) = a_1 * a_2 * \dots * a_n$

So we get $x = c * a_1 * a_2 * \dots * a_n + y$

Therefore $x \equiv y \pmod{a_1 * a_2 * \dots * a_n}$

We can now say that $n^7 \equiv n \pmod{7 * 3 * 2} \equiv n \pmod{42}$.

3 Chinese Remainder Theorem

3.1 Questions

1. Find an integer x such that x is congruent to 3 mod 4 and 5 mod 9.

Solution: In general if x can be expressed as

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

where m_1 and m_2 are relatively prime to each other, CRT tells us that there is a unique number mod $m_1 m_2$ that satisfies this equation.

Since m_1 and m_2 are relatively prime, we can, using Euclid's algorithm, write an equation of the form

$$1 = (m_1^{-1} \pmod{m_2})$$

2. The supermarket has a lot of eggs, but the manager is not sure exactly how many he has. When he splits the eggs into groups of 5, there are exactly 3 left. When he splits the eggs into groups of 11, there are 6 left. What is the minimum number of eggs at the supermarket?

Solution: We have that $x \equiv 3 \pmod{5}$ and $x \equiv 6 \pmod{11}$. We can use the Chinese Remainder Theorem to solve for x .

Recall from the note on modular arithmetic, the solution to x is defined as $x = \sum_{i=1}^k a_i b_i \pmod{N}$, where b_i are defined as $\left(\frac{N}{n_i}\right) \left(\frac{N}{n_i}\right)^{-1}_{\pmod{n_i}}$ and $N = n_1 \cdot n_2 \dots \cdot n_k$.

In our case, $a_1 = 3, a_2 = 6, n_1 = 5$ and $n_2 = 11$.

$$b_1 = \left(\frac{55}{5}\right) \left(\frac{55}{5}\right)^{-1}_{\pmod{5}} = 11 \cdot 11^{-1}_{\pmod{5}} = 11 * 1 = 11$$

$$b_2 = \left(\frac{55}{11}\right) \left(\frac{55}{11}\right)^{-1}_{\pmod{11}} = 5 \cdot 5^{-1}_{\pmod{11}} = 5 * 9 = 45$$

$$\text{Therefore, } x \equiv 3 \cdot 11 + 6 \cdot 45 \pmod{55} = 28$$

You can quickly verify that 28 indeed satisfies both conditions.

4 RSA

4.1 Questions

1. How does RSA work?

- a. Alice wants to send Bob a message $m = 5$ using his public key ($n = 26, e = 11$). What cipher text $E(m)$ will Alice send?

Solution:

$$5^1 = 5 \pmod{26}$$

$$5^2 = 5 \pmod{26}$$

$$= -1 \pmod{26}$$

$$5^4 = (-1)^2 \pmod{26}$$

$$= 1 \pmod{26}$$

$$5^8 = 1 \pmod{26}$$

$$5^{11} = 5^8 * 5^2 * 5^1 \pmod{26}$$

$$= 1 * -1 * 5 \pmod{26}$$

$$= -5 \pmod{26}$$

$$= 21 \pmod{26}$$

- b. What is the value of d (Bobs private key) in this scheme? Note that traditional RSA schemes use much larger prime numbers, so its harder to break n down into

its prime factors than it is in this problem.

Solution: $n = 26 \rightarrow$ because $26 = pq$ and $p \neq a * q$ for all a within integers,
 $p = 13, q = 2$

$$d = e^{-1} \mod (13 - 1)(2 - 1)$$

$$d = 11^{-1} \mod 12$$

$$d = 11$$

2. In RSA, if Alice wants to send a confidential message to Bob, she uses Bob's public key to encode it. Then Bob uses his private key to decode the message. Suppose that Bob chose $N = 77$. And then Bob chose $e = 3$ so his public key is $(3, 77)$. And then Bob chose $d = 26$ so his private key is $(26, 77)$.

Will this work for encoding and decoding messages? If not, where did Bob first go wrong in the above sequence of steps and what is the consequence of that error? If it does work, then show that it works.

Solution: e should be co-prime to $(p - 1)(q - 1)$.

$e = 3$ is not co-prime to $(7 - 1)(11 - 1) = 60$, so this is incorrect, since therefore e does not have an inverse $\pmod{60}$.

3. Coin tosses over text messages

You and one of your friends want to get your hands on the new gadget that's coming out. One of you has to wait in line overnight so that you have a chance to get the gadgets while they last. In order to decide who this person should be, you both agree to toss a coin. But you won't meet each other until the day of the actual sale and you have to settle this coin toss over text messages (using your old gadgets). Obviously neither of you trusts the other person to simply do the coin toss and report the results.

How can you use RSA to help fix the problem?

Solution: Firstly, we need some way to create two events of equal probability. One way to do this is have both of you flip a coin, and if you both get the same coin (i.e. "HH" or "TT") then one of you has to wait in line, and if you both get different coins (i.e. "HT" or "TH") then the other one of you needs to wait in line. Since each combination of two flips has probability $\frac{1}{4}$, each of you has a $2 \cdot \frac{1}{4} = \frac{1}{2}$ chance of having to wait in line.

Some form of encryption is necessary in this question, because otherwise, you could send your non-encrypted result to your friend and they could simply lie and say that they got the result that would cause you to have to go wait in line. Consider the following abstraction:

1. I flip a coin, write down my result on a piece of paper, and turn over the piece of paper
2. I give you the paper, you flip your coin, and then turn over my paper

The main idea of the above scheme boiled down to the fact that I was able to give you my result without you being able to see it. After flipping my coin and writing down the result, I'm unable to change my flip, therefore I was forced to "commit"

to my answer. Since you weren't able to see my coin, you had no choice but to actually flip the coin, as you had no additional information.

Let's implement this with RSA.

1. You generate a public key (N, e) , and flip your coin. If you got heads, encrypt some random word beginning with the letter "H". If you got tails, encrypt some random word beginning with the letter "T". The reasoning for this will be evident in the next step.
2. Send your encrypted message to your friend, along with your public key. Sending the public key is important, since it forces you to commit to the result that you got (if you were to send your public key after your friend flipped their coin, you could calculate a public key and private key such that your encrypted message decrypts to whatever you want it to).
3. Since your friend currently has no information about your flip, as you can't decrypt with just the public key, they have no choice but to just flip their coin and relay their result back to you.
4. Now, you send your friend your private key. With your public key and private key, they can decrypt your message to see what your original word was, telling them whether you got heads or tails.