BIJECTIONS, FLT, CRT, RSA 3

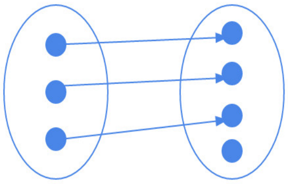
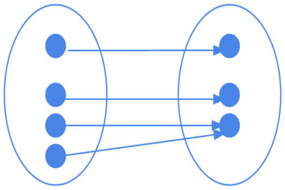
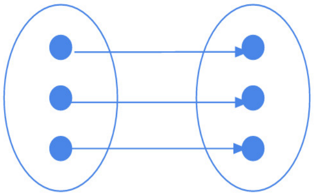
COMPUTER SCIENCE MENTORS 70

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: $R \rightarrow R$ 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: $R \rightarrow R^+$ 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: $\{0, \ldots, n-1\}$
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} ($7x7 = 49mod12 = 1$, 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 $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \mod p$

1. Prove Fermat's Little Theorem.

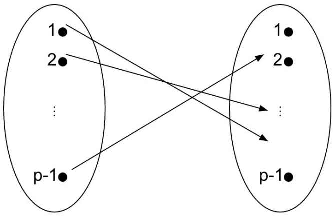
Solution: Proof from notes:
Claim: The function $a * x \mod p$ is a bijection where $x \in \{1, 2, \ldots, p-1\}$
The domain and range of the function are the same set, so it is enough to show that if $x \neq x'$ then $a * x \mod p \neq a * x' \mod p$.
Assume that $a * x \mod p \equiv a * x' \mod p$.
Since $gcd(a, p) = 1$, a must have an inverse: $a^{-1}(modp)$

$$ax \mod p \equiv ax \mod p$$

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

$$x \mod p \equiv x' \mod p$$

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

$$1 * 2 * \ldots * (p-1) \mod p \equiv (1a) * (2a) * \ldots * ((p-1)a) \mod p$$
$$(p-1)! \mod p \equiv a^{p-1} * (p-1)! \mod p$$
$$1 \equiv a^{p-1} \mod p$$

2.2 Questions

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

Solution:

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

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!!

$$n^7 \equiv n \mod 7$$
$$n^3 \equiv n \mod 3$$
$$n^2 \equiv n \mod 2$$

Were interested in n^7 so lets modify the bottom two equations to write n^7 in mod 3 and mod 2

$$n^7 \equiv n^3 * n^3 * n \equiv n * n * n \equiv n^3 \equiv n \mod 3$$
$$n^7 \equiv n \mod 3$$

$$n^7 \equiv n^2 * n^2 * n^2 * n \equiv n * n * n * n \equiv n^2 * n^2 \equiv n * n \equiv n^2 \equiv n \mod 2$$
$$n^7 \equiv n \mod 2$$

$$n^7 \equiv n \mod 7$$
$$n^7 \equiv n \mod 3$$
$$n^7 \equiv n \mod 2$$

Wouldnt it be great if the above equations implied that $n7 \equiv n \mod 7 * 3 * 2$?
Lets try to prove that.
Claim: If

$$x \equiv y \mod a_1$$
$$x \equiv y \mod a_2$$
$$\ldots$$

$$x \equiv y \mod a_n$$

are true and $a_1, \ldots, a_n$ are coprime then $x \equiv y \mod a_1 a_2 \ldots a_n)$
$x \equiv y \mod a_i \to x = y + c_i * a_i$ for some constant c_i

$$x = y + c_1 * a_1$$

$$x = y + c_2 * a_2$$

$$\ldots$$

$$x = y + c_n * a_n$$

But this implies that $x = c * lcm(a_1, \ldots, a_n) + y$
Since $a_1, \ldots, a_n$ are coprime, $lcm(a_1, \ldots, a_n) = a_1 * a_2 * \ldots * a_n$
So we get $x = c * a_1 * a_2 * \ldots * a_n + y$
Therefore $x \equiv y \mod a_1 * a_2 * \ldots * a_n$
We can now say that $n^7 \equiv n \mod 7 * 3 * 2 \equiv n \mod 42$.

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 an 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

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

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:

$$\begin{aligned} x &= 1(mod 5) & y &= 0(mod 5) \\ x &= 0(mod 11) & y &= 1(mod 11) \\ x &= 11p(mod 55) & y &= 5q(mod 55) \\ p &= 11^{-1}(mod 5) & y &= 5^{-1}(mod 11) \\ p &= 1(mod 5) & y &= 9(mod 11) \end{aligned}$$

$x = 3 * 1 + 9 * 11 = 102(mod 55)$

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:

$$\begin{aligned} 5^1 &= 5 \mod 26 \\ 5^2 &= 5 \mod 26 \\ &= -1 \mod 26 \\ 5^4 &= (-1)^2 \mod 26 \\ &= 1 \mod 26 \\ 5^8 &= 1 \mod 26 \\ 5^{11} &= 5^8 * 5^2 * 5^1 \mod 26 \\ &= 1 * -1 * 5 \mod 26 \\ &= -5 \mod 26 \\ &= 21 \mod 26 \end{aligned}$$

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 Bobs 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 $\mod 60$.

3. **Coin tosses over text messages**
   You and one of your friends want to get your hands on the new gadget thats 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 wont 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: If there was a way for me to make my choice (i.e. toss the coin) without revealing to my friend what the result was before s/he makes her/his decision, then we would be in good shape. RSA enables us to do just that. One can commit to a choice without revealing what that choice really is. So here is how we proceed:

   1. One issue we need to consider is that if ″heads″ and ″tails″ are the only things we’re encrypting and decrypting, then given some public key and an encrypted message it’s easy to simply encrypt ″heads″ and encrypt ″tails″ and check which one matches the received encrypted message.
   2. I select a public key (N,e) and a private key d. I toss a coin. If I get ″heads″, I choose some random word that begins with an H. If I get ″tails″, I choose some random word that begins with a T. I do this so that my friend can’t ″reverse engineer″ the encrypted message to figure out what my result was. Instead of sending the result to my friend, I first encrypt my word using the public key (N,e). Then I send my friend the public key along with the encrypted message.
   3. My friend is supposedly (read the next part for why the word supposedly is used) unable to see what the result of the coin toss was and therefore cannot

cheat. So s/he makes her/his choice (what HEADS and TAILS mean) and sends it to me, using the same technique (some word starting with H for heads and T for tails).

4. Once I have successfully received the result, I reveal the result of the coin toss by sending my friend my word in plain text (i.e. with no encryption). My friend can now verify that I have not cheated (i.e. I have not changed the result) by encrypting the result using the public key I have given her/him and making sure it was the same as the encrypted message I send her/him. Note that RSA encryption and decryption are both bijections, therefore if I know the encrypted version of two messages are the same, then those two messages must be the same.

Note that I cannot cheat here, because I commit to the result of the coin toss before I know my friends choice. Commitment is a very useful primitive (used in many places in cryptography) that enables a party to convincingly commit to a choice without revealing it until they choose to reveal it. The party should not be able to change their mind after the commitment which is what the scheme guarantees.