

BIJECTIONS, MODULAR ARITHMETIC, FLT, CRT, RSA 3

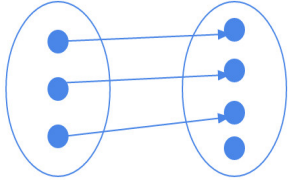
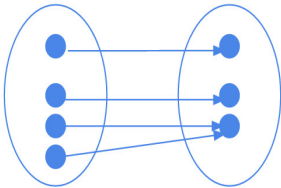
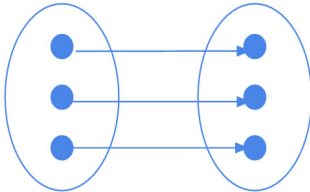
COMPUTER SCIENCE MENTORS 70

September 17 to September 21, 2018

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)
<p>Solution: .</p> 	<p>Solution: .</p> 	<p>Solution: .</p> 

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: One example is $e^x: \mathbb{R} \rightarrow \mathbb{R}$ 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.

Another example is $x^2: R \rightarrow R^+$ 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.

1.2 Questions

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. 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, there exists a multiplicative inverse to 7 in Z_{12} ($7 \times 7 = 49 \bmod 12 = 1$, so $f^{-1}(x) = 7x$), which only occurs if the function is a bijection.

b. $f(x) = 3x$

Solution: No. For example, $f(0) = f(4) = 0$.

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

Solution: Yes. It's 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. For example, 0 and 4 both map to 0.

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

Solution: Yes. This is the same as part (a), 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.

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} by mapping from Z_{12} . Similarly, because there are more values in Z_{12} than Z_6 , there are not enough unique elements in Z_6 to assign one to every element in Z_{12} .

2 Modular Arithmetic

2.1 Questions

1. What are the tens and units digits of 7^{1900} ?

Solution: Since we're only looking for the tens and units digits, we can just find the $7^{1900} \bmod 100$, the remainder when 7^{1900} is divided by 100. We write down the first few powers of $7 \bmod 100$ and see that $7^4 = 2401 = 1 \pmod{100}$. So, $7^{1900} \bmod 100 = 7^{4 \times 475} = 1^{475} = 1 \bmod 100$. So, our units digit is 1 and tens digit is 0.

2. Solve $2x = 3 \bmod 7$.

Solution: $2^{-1} \bmod 7 = 4$ so $x = 3(2^{-1}) = 12 = 5 \bmod 7$.

3 Fermat's Little Theorem

3.1 Introduction

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

Proof: 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 $a * x \pmod{p} \equiv a * x' \pmod{p}$.

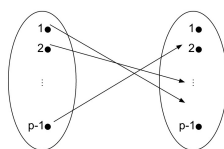
Since $\gcd(a, p) = 1$, a must have an inverse: $a^{-1} \pmod{p}$

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

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

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

This contradicts our assumption that $x \neq x' \pmod{p}$. Therefore the function 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:

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

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

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

3.2 Questions

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

Solution:

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

2. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$.

Solution: By FLT:

$$2^6 \equiv 1 \bmod 7$$

$$3^6 \equiv 1 \bmod 7$$

$$4^6 \equiv 1 \bmod 7$$

$$5^6 \equiv 1 \bmod 7$$

$$6^6 \equiv 1 \bmod 7$$

Apply the above facts to simplify each portion of the equation:

$$2^{20} = 2^2 * (2^6)^3 \rightarrow 2^{20} \bmod 7 \equiv 2^2 \bmod 7 \equiv 4 \bmod 7$$

$$3^{30} = (3^6)^5 \rightarrow 3^{30} \bmod 7 \equiv 1 \bmod 7$$

$$4^{40} = 4^4 * (4^6)^6 \rightarrow 4^{40} \bmod 7 \equiv 4^4 \bmod 7 \equiv 4 \bmod 7$$

$$5^{50} = 5^2 * (5^6)^8 \rightarrow 5^{50} \bmod 7 \equiv 5^2 \bmod 7 \equiv 4 \bmod 7$$

$$6^{60} = (6^6)^{10} \rightarrow 6^{60} \bmod 7 \equiv 1 \bmod 7$$

$$\begin{aligned} 2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7 &\equiv 4 + 1 + 4 + 4 + 1 \bmod 7 \\ &\equiv 14 \bmod 7 \equiv 0 \bmod 7 \end{aligned}$$

4 Chinese Remainder Theorem

4.1 Introduction

Chinese Remainder Theorem: The Chinese Remainder theorem says that a sequence of remainders with pairwise coprime divisors defines a unique remainder modulo the product of those divisors. Formally, 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.

In simple cases, we can often use extended Euclid's algorithm to find x . However, a failsafe equation is given by:

$$x = \sum_{i=1}^k a_i b_i \pmod{N}, \text{ where } b_i \text{ are defined as } \left(\frac{N}{n_i}\right) \left(\frac{N}{n_i}\right)^{-1}_{\pmod{n_i}} \text{ and } N = n_1 \cdot n_2 \dots \cdot n_k.$$

4.2 Questions

1. Find an integer x such that x is congruent to $3 \pmod{4}$ and $5 \pmod{9}$.

Solution: We can express x as:

$$x \equiv 3 \pmod{4}$$

$$x \equiv 5 \pmod{9}$$

where 4 and 9 are relatively prime to each other. We write the congruence with the largest modulus as an equation, $x = 9t + 5$. We substitute into the other congruence and solve for t . $9t + 5 \equiv 3 \pmod{4}$, which means $9t \equiv 2 \pmod{4}$ and $t \equiv 2 \pmod{4}$. We write this congruence as an equation, $t = 4s + 2$, and substitute into the equation for x . $x = 9(4s + 2) + 5 = 36s + 23$. So $x = 23 \pmod{36}$ is the solution. Note that $\text{lcm}(4, 9) = 36$.

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.

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

Solution: $42 = 7 * 3 * 2$ ← these factors are prime so we can apply FLT. We know that:

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

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

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

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

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

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

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

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

So now we have that:

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

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

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

By CRT, we can say that $n^7 \equiv n \pmod{7 * 3 * 2} \equiv n \pmod{42}$.

5 RSA

5.1 Introduction

RSA: Given two large primes, p and q , and a message x ,

$$\begin{aligned}N &= pq \\ E(x) &= x^e \bmod N \\ D(x) &= x^d \bmod N\end{aligned}$$

where e is relatively prime to $(p-1)(q-1)$, and $ed = 1$. The pair (N, e) is the recipient's **public key**, and d is the recipient's **private key**. The sender sends $E(x)$ to the recipient, and the recipient uses $D(x)$ to recover the original message.

5.2 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:

$$\begin{aligned}5^1 &= 5 \bmod 26 \\ 5^2 &= 25 \bmod 26 \\ &= -1 \bmod 26 \\ 5^4 &= (-1)^2 \bmod 26 \\ &= 1 \bmod 26 \\ 5^8 &= 1 \bmod 26 \\ 5^{11} &= 5^8 * 5^2 * 5^1 \bmod 26 \\ &= 1 * -1 * 5 \bmod 26 \\ &= -5 \bmod 26 \\ &= 21 \bmod 26\end{aligned}$$

- b. What is the value of d (Bob's 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, $p = 13, q = 2$

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

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

$$d = 11$$

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 e does not have an inverse $\pmod{60}$.