DIS 2D

Wednesday, June 27, 2018 12:34 PM

Topics : Bijection. FLT. RSA.

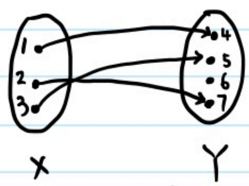
Bijection

- $f: X \to Y$ denotes a mapping / function between $\overset{\text{set}}{X}$ and $\overset{\text{set}}{Y}$

  think of X as the set of inputs, and Y as the set of possible outputs.
  for each $x \in X$, plug it into f, you'll get something in Y.

- X is called domain . Y is called codomain

e.g.



This is a function (with a "lonely" y)

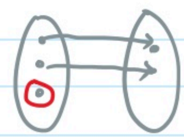
$X = \{1,2,3\}$. $Y = \{4,5,6,7\}$

f is defined as follows:

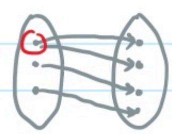
$f(1) = 4$

$f(2) = 5$

$f(3) = 7$



NOT a function

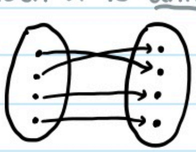


NOT a function

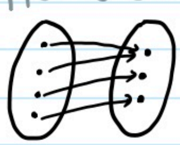
But, we might want to look at a subset of "not lonely" Y ...

- Range of $f = \{y \in Y : f(x) = y$ for some $x \in X\}$
- injection / one-to-one "i" looks like "one"

  each x is unique mapped to one y.



injective

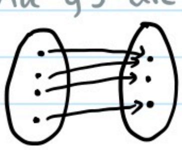


NOT injective

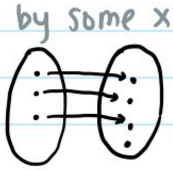
Prove f is injection : Assume $f(x_1) = f(x_2)$. Show $x_1 = x_2$.

- Surjection / onto

  All y's are mapped by some x.



surjective



NOT surjective

Prove f is surjection: Let $y \in Y$. Show there exists $x \in X$ $\underset{}{\overset{\text{such that}}{\text{s.t.}}}$ $f(x) = y$.

- Bijection : Surjection + injection

  |domain| = |range| range = codomain

That was a lot of terms. Make sure you understand:

terms:
- ☐ mapping / function
- ☐ domain
- ☐ codomain
- ☐ range
- ☐ injection / one-to-one
- ☐ prove f is an injection
- ☐ surjection / onto
- ☐ prove f is a surjection
- ☐ bijection

Fermat's Little Theorem

- $f(x) = ax \pmod{p}$

  domain $\{0, \dots, p-1\}$

  codomain $\{0, \dots, p-1\}$

  $f^{-1}(x)$ exists $\Leftrightarrow$ $f(x)$ is bijective $\Leftrightarrow$ $\gcd(a, p) = 1$

- Fermat's Little Theorem:

  p prime, $a \not\equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

  Pf: Let $f(x) = ax \pmod{p}$

  $a \not\equiv 0 \pmod{p} \Rightarrow f$ is bijective

  $\Rightarrow$ codomain = range

  We know domain = codomain, so domain = range.

  $$\text{domain} = \{0, 1, \dots, p-1\}$$

  $$f(0) \quad f(1) \quad f(p-1)$$

  $$\text{range} = \{a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)\} \pmod{p}$$

  domain = range

  $$\Rightarrow 1 \cdot 2 \cdot \cdots (p-1) \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \pmod{p}$$

  $$\prod_{x=1}^{p-1} x \equiv \prod_{x=1}^{p-1} ax \pmod{p}$$

  $$\prod_{x=1}^{p-1} x \equiv a^{p-1} \prod_{x=1}^{p-1} x \pmod{p}$$

  all $x = 1, \dots, p-1$ have a multiplicative inverse in mod p.

  Thus, $1 \equiv a^{p-1} \pmod{p}$ □

2nd version of FLT:

p prime $\Rightarrow \forall a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

$a \equiv 0 \pmod{p}$ is okay in this version.

RSA

RSA protocol:

Pick two large primes p and q. Let $N = pq$.

Pick an integer e.

Public key: (N, e)

Decryption key: $d \equiv e^{-1} \pmod{(p-1)(q-1)}$

Now we've got all "numbers" we need. Let's decrypt/encrypt.

Encryption function: $E(m) = m^e \pmod N$

Decryption function: $D(m) = m^d \pmod N$

Correctness? $D(E(m)) = m$?

Claim: $m^{ed} \equiv m \pmod N$, $\forall m \in \{0, 1, \ldots, N-1\}$

Pf: By definition, $ed = 1 + k(p-1)(q-1)$ for some $k \in \mathbb{N}$.

Then, $m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot m^{k(p-1)(q-1)}$

case 1: $m \equiv 0 \pmod p$

$\Rightarrow m \cdot m^{k(p-1)(q-1)} \equiv 0 \pmod p$

$\Rightarrow m^{ed} \equiv m \pmod p$

$\Rightarrow p \mid m^{ed} - m$

case 2: $m \not\equiv 0 \pmod p$

$\Rightarrow m^{p-1} \equiv 1 \pmod p$

$\Rightarrow (m^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \pmod p$

$\Rightarrow m \cdot m^{k(p-1)(q-1)} \equiv m \cdot 1 \pmod p$

$\Rightarrow m^{ed} \equiv m \pmod p$

$\Rightarrow p \mid m^{ed} - m$

$\left.\begin{array}{l}\text{Thus, } p \mid m^{ed} - m. \\ \text{Similarly, } q \mid m^{ed} - m.\end{array}\right\} \Rightarrow pq \mid m^{ed} - m$, which is $N \mid m^{ed} - m$

$\Rightarrow m^{ed} \equiv m \pmod N$

Q4.

Suppose Alice sends either "yes" or "no" to Bob.

(a) If Alice and Bob use the standard RSA procedure, describe how Eve could find out which message Alice sent.

Sol: [Recall that encoding (encryption) is fast in RSA.
Also recall that RSA is essentially a mapping and its inverse (decrption).]

Eve can make a chart:

"yes"	D("yes")
"no"	D("no")

For each of Alice's message, compare the message with the 2^{nd} column to decrypt.

(b) Describe how Alice and Bob might modify the RSA procedure to stop Eve from using this exploit.

Sol: [One-time pad is nice, in the sense that each time you encrypt the same message, the encrypted message can be different. Thus, Eve wouldn't be able to make a chart as above.
The problem becomes, how do we choose and securely send the one-time pad?]

Alice pick a random pad. Encrypt it using Bob's public key. Send the encrypted pad (encrypted using RSA) and the encrypted message (encrypted using one-time pad) to Bob.

DIS 3A

Sunday, July 1, 2018 2:43 PM

Topics: CRT. Polynomials

Chinese Reminder Theorem

motivation: we learned how to solve for x in mod m. What if I want to find a $x \in \mathbb{Z}$, that simutaneously satisfies multiple congruence relations in different mod m.

Q1. (a) Find x that satisfies the following congruence relations:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod 7$$

Sol: [Idea: think of each mod as a coordinate
Write x as $2y_1 + 3y_2 + 4y_3$ so that each y_i takes care of one coordinate.
That is, we want $y_1 \equiv 1 \pmod 3$, $y_1 \equiv 0 \pmod 5$, $y_1 \equiv 0 \pmod 7$
$y_2 \equiv 0 \pmod 3$, $y_2 \equiv 1 \pmod 5$, $y_2 \equiv 0 \pmod 7$
$y_3 \equiv 0 \pmod 3$, $y_3 \equiv 0 \pmod 5$, $y_3 \equiv 1 \pmod 7$]

Apply CRT:

$$y_1 = (5\times 7) \times ((5\times 7)^{-1} \pmod 3) = 35 \times 2 = 70$$
$$y_2 = (3\times 7) \times ((3\times 7)^{-1} \pmod 5) = 21 \times 1 = 21$$
$$y_3 = (3\times 5) \times ((3\times 5)^{-1} \pmod 7) = 15 \times 1 = 15$$

(b) For $n \geq 1$, $935 \mid n^{80} - 1 \Rightarrow 5 \nmid n, 11 \nmid n, 17 \nmid n$

Sol: [How do I introduce mod 5, mod 11, and mod 17?]

$935 \mid n^{80} - 1 \Rightarrow n^{80} - 1 = 935k \Rightarrow n^{80} = 935k + 1$

$$\Rightarrow n^{80} \equiv 1 \pmod 5$$
$$n^{80} \equiv 1 \pmod{11}$$
$$n^{80} \equiv 1 \pmod{17}.$$

Assume $5 \mid n$, that is $n \equiv 0 \pmod 5$.

$\Rightarrow n^{80} \equiv 0 \pmod 5$.

Thus, $5 \nmid n$.

Similarly, $11 \nmid n$, $17 \nmid n$. $\square$