Primes

2	3	5	7	11	13	17
19	23	29	31	37	41	43
47	53	59	61	67	71	73

Greeks

ϕ - phi

γ - gamma

α - alpha

δ - delta

Primitive Roots

$\mathbb{Z}$ = Integers $-\infty, \ldots -2, -1, 0, 1, 2, \ldots \infty$

$\mathbb{Z}_p = \{0 \ldots p-1\}$ e.g. $\mathbb{Z}_7 = \{0, 1 \ldots 6\}$

$\mathbb{Z}_p^*$ exclude $\emptyset$

Z = Integers $-\infty \ldots -2, -1, 0, 1, 2, \ldots \infty$

R = Real numbers

N = Natural numbers $1, 2, \ldots \infty$

Q = Rational numbers - ratios

XOR

		$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

Like addition mod 2

$1+1 \bmod 2 = 0$

XOR $\equiv$ addition mod 2

XOR is inverse of itself

Mod

$\frac{5}{3} = 1 \quad rem = 2$

$\frac{3}{5} = 0 \quad rem = 3$

Math

$$a^x \cdot a^y = a^{x+y}$$

e.g. $3^2 \cdot 3^5 = 3^7$

$$x^1 = x$$

$$x^0 = 1$$

How to read a Log

$$\log_2 8 = 3 \leftrightarrow 2^3 = 8$$

you can add mod

$$\log_2 8 = 3 \pmod{11} = 2^3 = 8 \pmod{11}$$

Discrete Logarithms 8/30 1:10:00

$\log_r a = e$ or $r^e \bmod p = a$

2 is a PR of 11 since $2^8 \bmod 11 = 3$
thus we write $\log_2 3 = 8$

*PR = Primitive Root

Base Conversion e.g. 485 → HEX

$n = b \cdot q + a$

$485 = 16 \cdot 30 + 5$

$30 = 16 \cdot 1 + 14$ $= 1\ 14\ 5$

$1 = 16 \cdot 0 + 1$ $= 1\ E\ 5$

q is 0 so stop

Decimal Expansion $= a_k b^k + a_{k-1} b^{k-1} \ldots a_1 b + a_0 b^0$

$(1101)_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

$= 8 + 4 + 0 + 1 = 13$

$(1E5)_{16} = 1 \cdot 16^2 + 14 \cdot 16^1 + 5 \cdot 16^0 = 485$

* A = 10; B = 11; C = 12; D = 13; E = 14; F = 15

Binary Modular Exponentiation

$3^{11} = ?$

$(11)_{10} = (1011)_2$

$= 3^8 \cdot 3^2 \cdot 3^1$

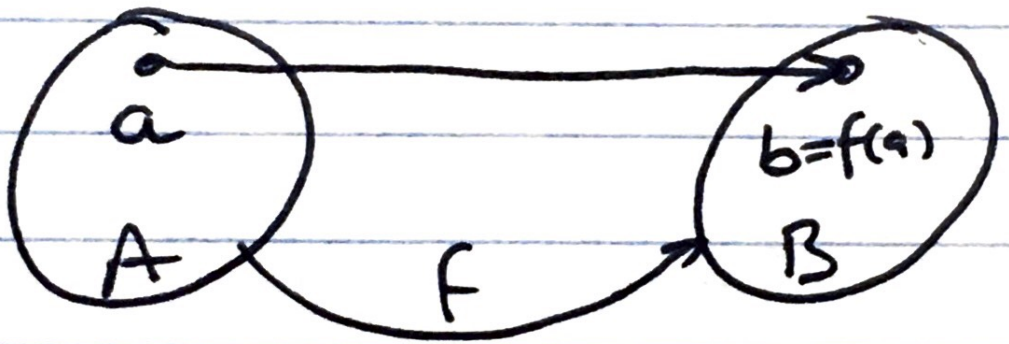
$= 3^{2 \cdot 2 \cdot 2} \cdot 3^2 \cdot 3^1$

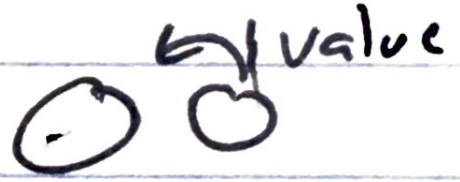
$= 177,147$

$= 2^3 \cdot 2^2 \cdot 2^1 \cdot 2^0$

$= 8 \times 2 1$

Functions = one value is returned





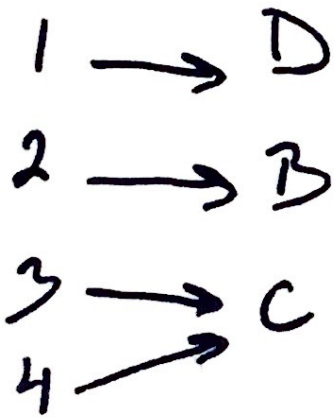
A = domain of f
B = codomain of f
} sets

b = image of a

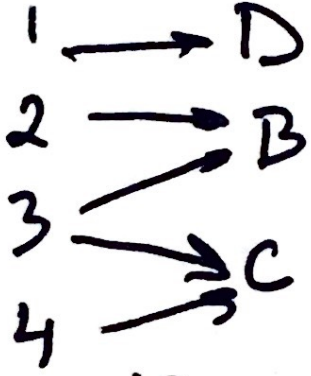
a = preimage of b

f(a) = range

e.g. →



OK

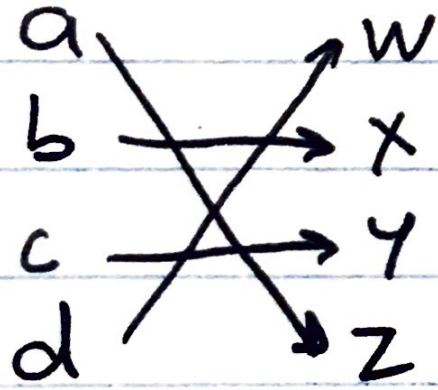


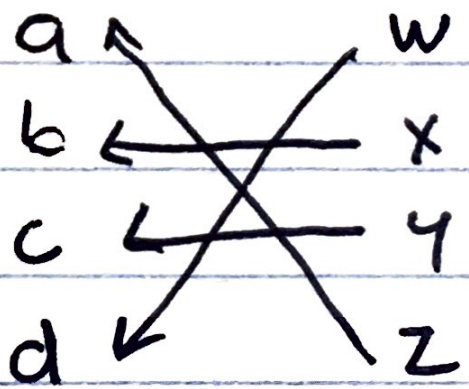
NO

Student → Grades

Inverse functions / Invertible

$A \xrightarrow{f} B$ $\quad$ $A \xleftarrow{F^{-1}} B$





Composition

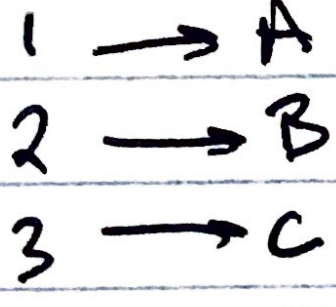
$f: B \to C \qquad g: A \to B$

comp. of f w. g is denoted by $f \circ g$

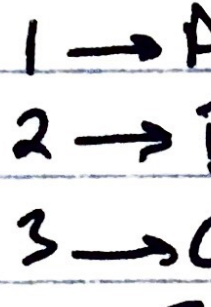
is a func. A to C defined by

$$f \circ g(x) = f(g(x))$$

Bijection = injection + surjection
= Surjective + injective
= one-to-one + onto



yes

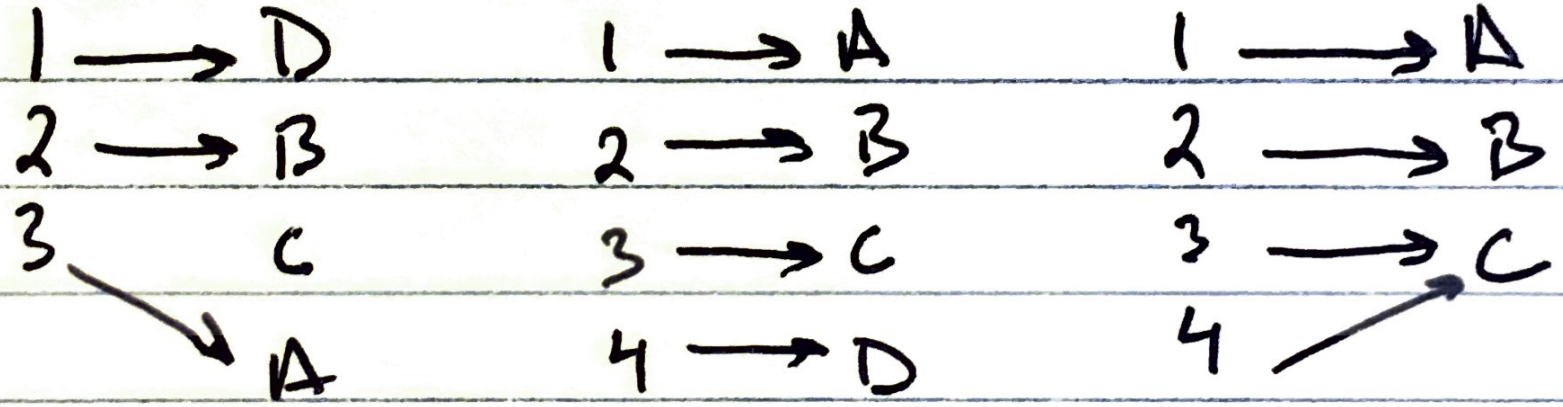


Function + surjective but not injective

NO

Surjection - all el. in 2nd set has an incoming arrow

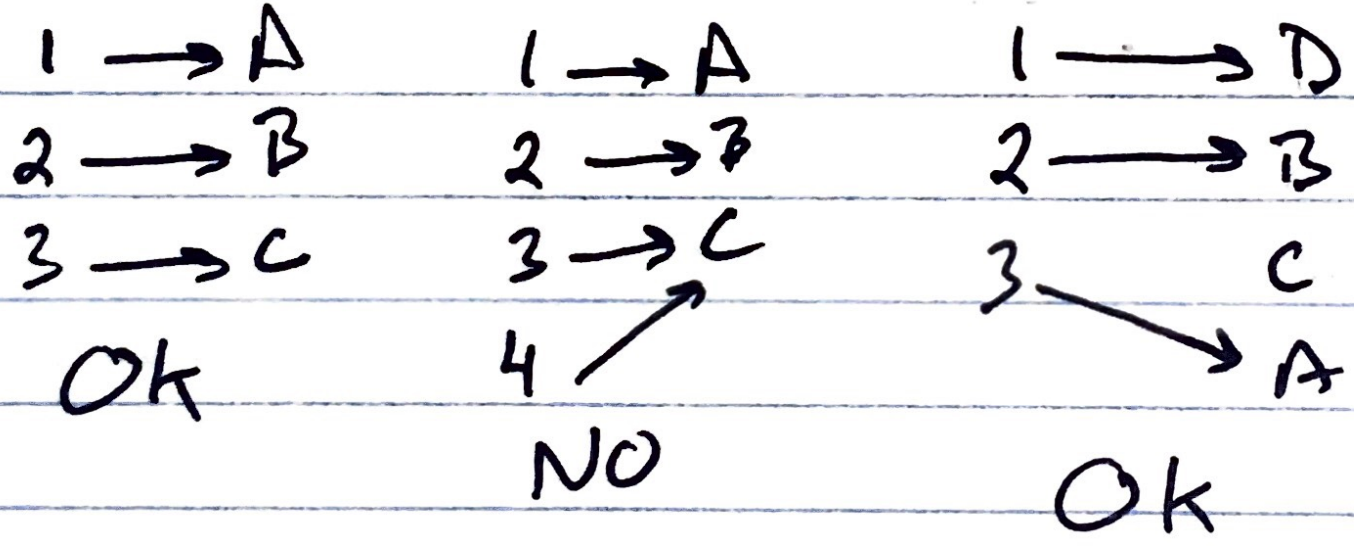
a func is called <u>onto</u>, iff every el. b has an el. a w. $f(a) = b$



NO YES YES

Injection

Must be a function that is 1 to 1



Shift Ciphers

A 0	I 8	Q 16	Y 24
B 1	J 9	R 17	Z 25
C 2	K 10	S 18	
D 3	L 11	T 19	
E 4	M 12	U 20	
F 5	N 13	V 21	
G 6	O 14	W 22	
H 7	P 15	X 23	

Caesar (Shift) Cipher Z_{26}

$$f(n) = n + k \bmod 26$$

$$f^{-1}(n) = n - k \bmod 26 \quad \{ \text{Decryption}$$

k = key

Max key size = 26 = modulus

Affine Ciphers

- includes all shift ciphers
- of the form: $f(n) = an + b \pmod{26}$
- $\gcd(a, m) = 1$

Encrypt "K" when $f(n) = 7n + 3 \bmod 26$

"K" == 10

$f(10) = 7(10) + 3 \pmod{26}$

$= 73 \pmod{26}$

$= 21 =$ "V"

* n is the letter to encrypt

Decrypt "V" when $f(n) = 7n + 3 \bmod 26$

"V" = 21

$c \equiv an + b \pmod m$ // c = cipher text

Solve for n

$c - b \equiv an \pmod m$ // Find MI of a $\longrightarrow$

$\bar{a}(c-b) \equiv \bar{a}an \pmod m$ // $\gcd(a,m) = 1$? $\bar{a}$ exists

$n \equiv \bar{a}(c-b) \pmod m$

$n \equiv 15(21-3) \pmod{26} = 10 =$ "K"

$C \equiv an+b$

$21 \equiv 7n+3 \pmod{26}$

$21-3 \equiv 7n \pmod{26}$

Find m1 of 7

① Use E. Alg. to get gcd(26,7)

$26 = 7\times3+5 \Rightarrow 5 = 26-7\times3$

$7 = 5\times1+2 \Rightarrow 2 = 7-5\times1$

$5 = 2\times2+1 \Rightarrow 1 = 5-2\times2$

$2 = 1\times2+0$

② Substitution

$1 = 5-2\times2$

$1 = 5-2(7-5\times1)$

$1 = 5-2\times7+2\times5\times1$

$1 = -2\times7+3\times5\times1$

$1 = -2\times7+3(26-7\times3)\times1$

$1 = -2\times7+3\times26-7\times3\times3$

$1 = -2\times7+3\times26-7\times9$

$1 = 3\times26-2\times7-7\times9$

$1 = \underbrace{3}_{s}\times26\underbrace{-11}_{t}\times7$

m1 of 7 mod 26 is −11. Add 26 to get 15

Cryptosystems

P is the set of plaintext strings

C is the set of cipher strings

K is the keyspace (set of all possible keys)

E is the set of encryption functions

D is the set of decryption functions

Block ciphers

9/6 - 0:32:00

- Replace blocks of letters w. other blocks of letters

- Messes w. letter frequency

Character/Monoalphabetic ciphers

- replace each letter of the alphabet by another letter.

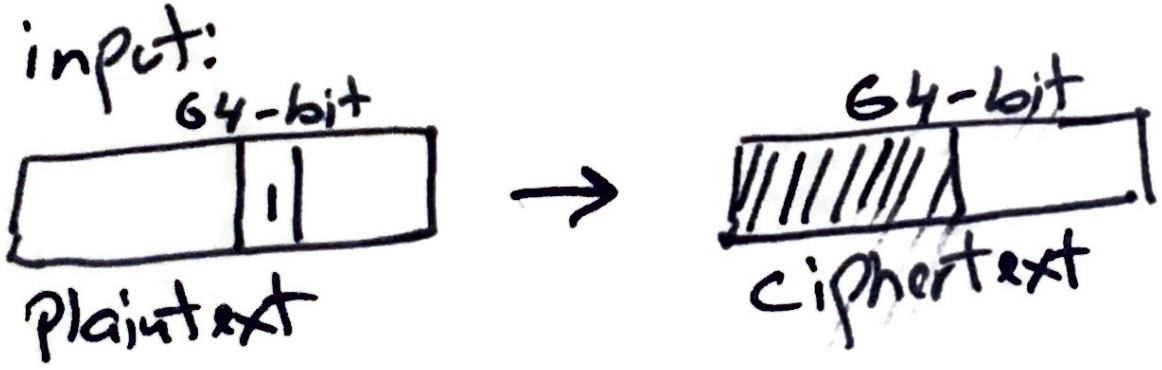
- vulnerable to cryptoanalysis based on letter frequency

Operations

Confusion: An an enc. op. where the relationship between key and ciphertext is obscured. Destroy any detectable conn. between the key and ciphertext.

Diffusion: An enc. op. where the influence of one plaintext symbol is spread over many ciphertext symbols. Helps hide statistical properties of plaintext. Destroy any detectable conn. between the plaintext and the ciphertext. →

A good diffusion operation means:
changing one bit results in changing half of the bits in the cipher text.



DES - Data Encryption Standard (retired)
- Private/symmetric
- Created 1977
- Uses block size of 64-bit
- Uses key size of 56-bit
- Today we use 3DES
- In 2000, it was replaced by ~~2000~~ AES
  - Advanced Enc. Std.

3DES

K_1 K_2 K_3

$K_{1.1-1.16}$ $K_{2.1-2.16}$ $K_{3.1-3.16}$

a Primitive Root modulo a prime p

is an integer r s.t. every nonzero element of Z_p is a power of r.

e.g. Since every non-zero el. of $Z_7 = \{1,2,3,4,5,6\}$ can be generated by a power of 3, 3 is a primitive root of 7.

$3^1 = 3$, 3^2 is $9 \bmod 7 = 2$, $3^3 = 27 \bmod 7 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$

Finding gcd using Prime Factorization

Find gcd(24, 36)

$24 = 2 \cdot 2 \cdot 2 \cdot 3$

$= 2^3 \cdot 3$

Select the no. w. the lower power for each base

$36 = 2 \cdot 2 \cdot 3 \cdot 3$

$= 2^2 \cdot 3^2$

from 2^3, (2^2) From 3^2, (3)

then $2^2 \cdot 3 = 12$

$\gcd(24, 36) = 12$

→

e.g. $\gcd(a,b) = p_1^{\min(a,b)} p_2^{\min(a_2,b_2)}$

$\gcd(120,500) =$

$120 = 2^3 \cdot 3 \cdot 5$

$500 = 2^2 \cdot 5^3$

$= 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)}$

$= 2^2 \cdot 3^0 \cdot 5^1 = 4 \cdot 1 \cdot 5 = 20$

*LCM - use $x^{\max(a,b)}$

Relatively Prime

a and b are relatively prime if their gcd = 1. e.g., 17, 22

aka: Coprime / mutually prime

Euclidian Alg. - used to compute gcd

gcd(91, 287)

1. Divide the larger no. by the smaller one.

$287 = 91 \cdot 3 + 14$

$91 = 14 \cdot 6 + 7$

$14 = (7) \cdot 2 + 0$

gcd(287, 91) =
gcd(91, 14) =
gcd(14, 7) = 7

Congruence Relation

if a and b are integers and m is a positive int, then a is congruent to b mod m if m divides $a - b$

e.g. $17 \equiv 5 \pmod 6$ because
6 divides $17 - 5 = 12$. No remainder

Linear Congruence

Solve $3x \equiv 4 \pmod 7$ MI e.g.

-2 is MI for 3

$-2 \cdot 3x \equiv 4 \cdot -2 \pmod 7$

$-6x \equiv -8 \pmod 7$

$-6x + 7 \equiv -8 + 7 + 7 \pmod 7$

$x \equiv 6 \pmod 7$ $x = 6, 13, 20 \ldots$

Additive Inverse

if $m = 16$ and $a = 9$

The additive inverse of a is $m - a$

$16 - 9 = 7$

.....

Multiplicative Inverse

e.g. →

$a \times_m a^{-1} = 1$ must yield 1

5 is the MI of 3 mod 7 because

$5 \cdot 3 = 15 \equiv 1 \pmod 7$

5 and 3 are the MI of each other

* if $\gcd(a,b) = 1$, then a MI of a mod b must exist

Find MI of 3, 7

① Use E. alg. to find gcd = 1

② Notice that gcd = 1, so a MI exists

③ Use Ext. E. alg. to find s and t.

s = 1 t = -2 so -2 is the MI of 3 mod 7

$-2 \cdot 3 \pmod 7 = -6 \pmod 7 \equiv 1$

add a 7

Find mult inverse of 101 and 4620 — 101 mod 4620

① E. alg. ② Ex E. alg.

$4620 = 101 \cdot 45 + 75$

$101 = 75 \cdot 1 + 26$

$75 = 26 \cdot 2 + 23$

$26 = 23 \cdot 1 + 3$

$23 = 3 \cdot 7 + 2$

$3 = 2 \cdot 1 + 1$

$2 = ① \cdot 2 + 0$

$\gcd(101, 4620) = 1$ so a mult. inverse exists.

③ substitution →

$1 = 3 - 2 \cdot 1$

$2 = 23 - 3 \cdot 7$

$3 = 26 - 1 \cdot 23$

$23 = 75 - 26 \cdot 2$

$26 = 101 - 1 \cdot 75$

$75 = 4620 - 101 \cdot 45$

$1 = 3 - 1(23 - 3 \cdot 7)$

$= -1 \cdot 23 + 3 \cdot 7 + 3$

$= -1 \cdot 23 + 3 \cdot 8$

$= -1 \cdot 23 + (26 - 1 \cdot 23) \cdot 8$

$= -1 \cdot 23 + 8 \cdot 26 - 8 \cdot 23$

$= -9 \cdot 23 + 8 \cdot 26$ →

$= \cancel{\text{illegible}}23$

$= -9 \cdot (75 - 26 \cdot 2) + 8 \cdot 26$

$= -9 \cdot 75 + 18 \cdot 26 + 8 \cdot 26$

$= -9 \cdot 75 + 26 \cdot 26$

$= -9 \cdot 75 + (26 \cdot (101 - 1 \cdot 75))$

$= -9 \cdot 75 + 26 \cdot 101 - 26 \cdot 75$

$= -35 \cdot 75 + 26 \cdot 101$

$= -35 \cdot (4620 - 101 \cdot 45) + 26 \cdot 101$

$= -35 \cdot 4620 + \cancel{1601}\ 1575 \cdot 101 + 26 \cdot 101$

$1 = \underbrace{-35}_{s} \cdot 4620 + \underbrace{1601}_{t} \cdot 101$

Bézout coefficients: -35 and 1601

1601 ~~illegible~~ of 101 mod 4620

1601 mI of 101 mod 4620
-35 mI of 4620 mod 101

$1601 * 101 \overset{4620}{\equiv} 1$

8/30 0:45

$1601 * 101 \bmod 4620$
$= 1$

Fermat's Little Thm.

$$a^{p-1} \equiv 1 \pmod{p}$$ * p is prime

e.g. $p = 11$ $a^{10} \equiv 1 \pmod{11}$

e.g. 8/30 0:58

* a not divisible by p
* $a^p \equiv a \pmod{p}$ →

Find $7^{222} \bmod 11$

$7^{222} = 7^{10 \cdot 22 + 2} \equiv (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 5 \pmod{11}$

Find $13^{145} \bmod 13$

$13^{12 \cdot 12 + 1} \equiv (13^{12})^{12} \cdot 13^1 = 1^{12} \cdot 13^1 = 13 \bmod 13$

$= 0$

$\downarrow$

$13^{12} \equiv 1 \pmod{13}$

Eulers Theorem: generalization of Fermat's Lillle thm ($a^{p-1} \equiv 1 \pmod{p}$)

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

note: $\phi(m) = p-1$

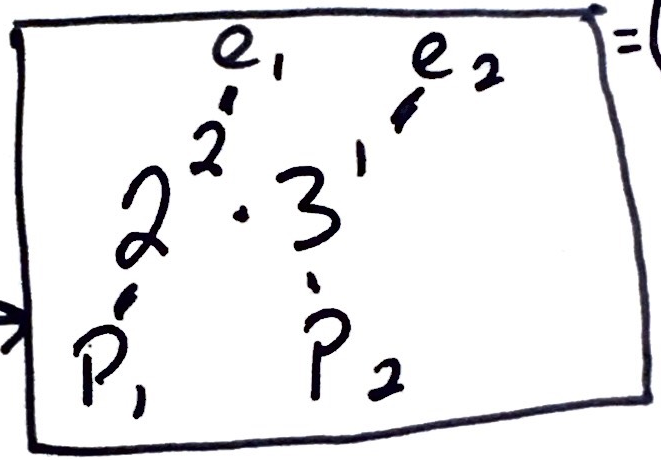
e.g. $m = 12$ $a = 5$ $\gcd(12, 5) = 1$

① do prime factorization for 12

$12 = 2 \cdot 6$

$= 2 \cdot 2 \cdot 3$

$= 2^2 \cdot 3^1$



$= (2^2 - 2^1)(3^1 - 3^0)$

$= 4$

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

$5^4 \equiv 625 \equiv 1 \pmod{12}$

Euler's phi function - prime factorization

① Find prime factorization of m

② Use $\phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})$

e.g. $m = 6 = 2^1 \cdot 3^1 \rightarrow p_1 = 2 \quad p_2 = 3 \quad e_1 = 1 \quad e_2 = 1$

$$\phi(6) = \underbrace{(2^1 - 2^0)}_{i=1} \underbrace{(3^1 - 3^0)}_{i=2} = (2-1)(3-1) = 2$$

→

if $m = prime_1 \cdot prime_2$

then $\phi(m) = (p-1)(q-1)$

i.e.

$$\phi(6) = 2 = (2-1)(3-1)$$

Euler's phi function using gcd

- given a set of m integers $\{0, 1, \ldots m-1\}$ how many numbers in the set are relatively prime to m?

relatively prime means $\gcd(a,b) = 1$

$\gcd(0,6) = 6$

$\gcd(1,6) = 1$ ←

$\gcd(2,6) = 2$

$\gcd(3,6) = 3$

$\gcd(4,6) = 2$

$\gcd(5,6) = 1$ ←

$\phi(6) = 2$