DMS (19/05/22)

Invertible ⟹ Inverse exists.

Non-Invertible ⟹ Inverse does not exist.

Relatively Prime ⇒ If GCD of 2 numbers is 1, then they are relatively Prime.

e.g GCD(9, 14) = 1.

Two integer (a, b) are relatively prime iff GCD(a, b) = 1

Kisi bhi Z_n mai, a^{-1} of every element a, exist, if (other than 0 & 1) a & n are relatively prime.

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$Z_{10} = \{\cancel{0}, \cancel{1}, 2, \cancel{3}, 4, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}\}$

N I N N N I N I

Euclidean Algorithm.

↳ Effective way to find GCD.

- GCD (85, 34)

$85 = 34(2) + 17$.

$34 = 17(2) + 0$.

17 is the GCD.

- GCD (1331, 1001) using Euclidean Method.

$1331 = 1001(1) + 330$

$1001 = 330(3) + 11$.

$330 = 11(30) + 0$

GCD

- GCD (9888, 6060)

$9888 = 6060(1) + 3828$.

$6060 = 3828(1) + 2232$.

$3828 = 2232(1) + 1596$.

$2232 = 1596(1) + 636$.

$1596 = 636(2) + 324$.

$636 = 324(1) + 312$.

$324 = 312(1) + 12$.

$312 = 12(26) + 0$.

GCD = 12

$1331x + 1001y = 11$.

Reverse the Eucledean Algorithm

$11 = 1001 - 330(3)$

$11 = 1001 - [1331 - 1001](3)$

$11 = 1001 - [331(3) + 1001(3)$

$11 = 1001(4) - 1331(3)$

$11 = 1001(4) + 1331(-3)$

($1001 \rightarrow y$, $-3 \rightarrow x$)

- $(213, 117)$

$213 = 117(1) + 96$.

$117 = 96 + 21$

$96 = 21(4) + 12$.

$21 = 12(1) + 9$.

$12 = 9(1) + 3$.

$9 = 3(3) + 0$. $\boxed{3 = GCD}$

$213x + 117y = 3$

$3 = 12 - 9$.

$3 = 12 - [21 - 12]$.

$3 = 12 - 21 + 12$

$3 = 12(2) - 21$

$3 = [96 - 21(4)](2) - 21$

$3 = 96(2) - 21(8) - 21$

$3 = 96(2) - 21(9)$

$3 = 96(2) - (9)[117 - 96]$

$= 96(2) - 117(9) + 96(9)$

$3 = 96(11) - 117(9)$

$3 = [213 - 117](11) - 117(9)$

$3 = 213(11) - 117(20)$

$3 = 213(11) + 117(-20)$.

$\Rightarrow$ $\boxed{x = 11}$, $\boxed{y = -20}$

- $252x + 198y = 18$

$252 = 198(1) + 54$.

$198 = 54(3) + 36$.

$54 = 36(1) + 18$

$36 = 18(2) + 0$

$\boxed{18 = GCD}$

$18 = 54 - 36$.

$18 = 54 - [198 - 54(3)]$

$18 = 54 - 198 + 54(3)$

$18 = 54(4) - 198$

$18 = [252 - 198](4) - 198$.

$18 = 252(4) - 198(5)$

$18 = 252(4) + 198(-5)$

$\boxed{x = 4}$, $\boxed{y = -5}$

DMS (31/05/22)

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

Relatively Prime.

GCD $(a, n) = 1$ $a^{-1} \bmod n$ exists.

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

- Calculate $5^{-1} \bmod 7$

$7 = 5(1) + 2$

GCD = 1 ⇒ $5^{-1} \bmod 7$ exist

$5 = 2(2) + 1$

$1 = 5 - 2(2)$

$= 5 - [7 - 5](2)$

$= 5 - 7(2) + 5(2)$

$1 = 5(3) - 7(2)$. $= 5(3) + 7(-2)$.

$5^{-1} \bmod 7 = 3 \bmod 7$.

$5 \cdot 3 \bmod 7 = 1 \bmod 7$.

$7 \overline{)15}$ (2), 14, (1)

verification

L.H.S

$15 \bmod 7 = 1 \bmod 7$.

L.H.S = R.H.S,

So $5^{-1} \bmod 7 = 3 \bmod 7$.

$Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

- $8^{-1} \bmod 11$.

$11 = 8(1) + 3$.

$8 = 3(2) + 2$.

$3 = 2(1) + 1$

$2 = 1(2) + 0$.

GCD = 1 , so 8^{-1} Mod 11 exist

$1 = 3 - 2(1)$

$= 3 - 3[8 - 3(2)]$

$= 3 - 8 + 3(2)$

$1 = -8 + 3(3)$

$= -8 + [11 - 8](3)$

$= -8 + 11(3) - 8(3)$

$= 11(3) - 8(4)$

$1 = 11(3) + 8(-4)$

$-4 \text{ Mod } 11 = 7 \text{ Mod } 11$

$\boxed{8^{-1} \text{ Mod } 11 = 7 \text{ Mod } 11}$

Verification:

If $((8 \times 7) \text{ Mod } 11 == 1 \text{ Mod } 11)$

then it is true else false.

$8 \times 7 = 56$

$11 \overline{)56}$ (5), 55, remainder 1

Proved.

$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

• 6^{-1} Mod 9.

Not exist, because 6 & 9 are not relatively Prime

• $7^{-1} \text{Mod } 9$.

$9 = 7(1) + 2$.

$7 = 2(3) + 1$

$2 = 1(2) + 0$.

GCD = 1, $7^{-1} \text{Mod } 9$ exist.

$1 = 7 - 2(3)$.

$= 7 - [9 - 7](3)$

$= 7 - 9(3) + 7(3)$.

$= 7(4) - 9(3)$.

$1 = 7(4) + 9(-3)$.

(7^{-1})

$\Rightarrow \quad 7^{-1} \text{Mod } 9 = 4 \text{ Mod } 9$.

Proof: $(7 \times 4) \text{ Mod } 9 = 28 \text{ Mod } 9$

$\cong 1 \text{ Mod } 9$.

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

• $8^{-1} \text{ Mod } 10 \Rightarrow$ Not exist.

• $9^{-1} \text{Mod } 10$

$10 = 9(1) + 1$

$9 = 1(9) + 0$

GCD = 1 $\Rightarrow$ $9^{-1} \text{Mod } 10$ exist.

$1 = 10 - 9(1)$

$= 10 - 9[10 - 9]$

$= 10 - 9(10) + 9(9)$

$1 = 10 + 9(9)$

$9 \text{ Mod } 10 = 9 \text{ Mod } 10$.

Proof:

$9^{-1} \text{ Mod } 10 = 9 \text{ Mod } 10$.

$9 \times 9 \text{ Mod } 10 = 81 \text{ Mod } 10$.

$\cong 1 \text{ Mod } 10$

Affine Cipher.

⇒ Two keys involved

$key = k(a, b)$.

$y = (ax + b) \text{ Mod } 26$.

$x = a^{-1}(y - b) \text{ Mod } 26$

- Encrypt VOTE, key = k(5, 7)

V	O	T	E
x_1	x_2	x_3	x_4
21	14	19	4

$y_1 = [5(21) + 7] \text{ Mod } 26$

$= 112 \text{ Mod } 26 \cong 8 \text{ Mod } 26$.

$= I$

[illegible]