CIS 3362 8/22/2025

Affine Cipher

$f(x) = (ax + b) \bmod n$

$a^{-1} \times a \equiv 1 \bmod n$

($a^{-1} \bmod n$)

Find $f^{-1}(x)$

$x \equiv ay + b \bmod n$

$x - b \equiv ay \bmod n$

$?\cdot ay \equiv ?(x-b) \bmod n$

$$\boxed{f^{-1}(x) \; (a^{-1} \bmod n)(x-b) \bmod n}$$

Since

$3 \times 5 \equiv 1 \bmod 7$

$5 \equiv 3^{-1} \bmod 7$

$3 \equiv 5^{-1} \bmod 7$

General form Decryption func

How to compute $a^{-1} \bmod n$ when it exists, efficiently? (iff $\gcd(a,n) = 1$.)

Euclidean Algorithm → compute greatest common divisor of 2 ints

Extended Euclidean Algorithm → is to find integers x, y s.t. $ax + by = \gcd(a,b)$.

$77^{-1} \mod 108$

Step 1 - run Euclidean Alg 108, 77

quotient ↙ remainder ↙

$108 = 1 \times 77 + 31$

$77 = 2 \times 31 + 15$

$31 = 2 \times 15 + 1$

$15 = 15 \times 1$

if $a > b$

$\gcd(a,b) = \gcd(b, a \bmod b)$

$\gcd$ (last non-zero remainder)

GOAL STATE

$108x + 77y = 1$

$77 - 2 \times 31 = 15$

$108 - 1 \times 77 = 31$

sub for 31

$31 - 2 \times 15 = 1$

$31 - 2(77 - 2 \times 31) = 1$

$31 - 2 \times 77 + 4 \times 31 = 1$

$5 \times 31 - 2 \times 77 = 1$

$5 \times (108 - 1 \times 77) - 2 \times 77 = 1$

$5 \times 108 - 5 \times 77 - 2 \times 77 = 1$

$5 \times 108 - 7 \times 77 = 1 \mod 108$

$5 \times 108 - 7 \times 77 \equiv 1 \mod 108$

$0 - 7 \times 77 \equiv 1 \mod 108$

$-7 \times 77 \equiv 1 \mod 108$

$77 \times ? \equiv 1 \mod 108$?

$77^{-1} \equiv -7 \equiv 101 \mod 108$

if $a \equiv b \pmod n$

$f(a) \equiv f(b) \pmod n$ for all poly functions

$$3 \times \underline{17}^3 \equiv 3 \times \underline{3}^3 \pmod 7$$

because $17 \equiv 3 \pmod 7$

$a \equiv a \pm kn \pmod n$

always add to subtract any multiple of n (mod value).

Find $124^{-1} \mod 287$

$287 = 2 \times 124 + 39$ → $287 - 2 \times 124 = 39$

$124 = 3 \times 39 + 7$ → $124 - 3 \times 39 = 7$

$39 = 5 \times 7 + 4$ → $39 - 5 \times 7 = 4$

$7 = 1 \times 4 + 3$ → $7 - 1 \times 4 = 3$

$4 = 1 \times 3 + \boxed{1}$ gcd

$4 - 1 \times 3 = 1$

$4 - 1(7 - 1 \times 4) = 1$

$4 - 1 \times 7 + 1 \times 4 = 1$

$2 \times 4 - 1 \times 7 = 1$

$2(39 - 5 \times 7) - 1 \times 7 = 1$

$2 \times 39 - 10 \times 7 - 1 \times 7 = 1$

$2 \times 39 - 11 \times 7 = 1$

$2 \times 39 - 11(124 - 3 \times 39) = 1$

$2 \times 39 - 11 \times 124 + 33 \times 39 = 1$

$35 \times 39 - 11 \times 124 = 1$

$35(287 - 2 \times 124) - 11 \times 124 = 1$

$35 \times 287 - 70 \times 124 - 11 \times 124 = 1$

$(35 \times 287 - 81 \times 124 = 1) \mod 287$

$0 - 81 \times 124 \equiv 1 \mod 287$

$-81 \times 124 \equiv 1 \mod 287$

$124^{-1} \equiv -81 \equiv \boxed{206 \mod 287}$

What is $1083^{-1} \mod 287$

$$287 \overline{)1083} \quad 3 \text{ R } 222$$
$$-861$$
$$222$$

$$= 222^{-1} \mod 287$$

$124^{-1} \mod 287$ is 206

$$124^{-1} \equiv 206 \pmod{287}.$$

Find $124^{-1} \mod 287$

$$\vdots$$

$$\boxed{206}$$