~~$a \equiv b \bmod n$~~

Modular Arithmetic

goal/ = computation in finite sets

modern crypto infinite sets.

Edclidean Alg:

(1) → two prime integers

↓

relatively prime ..

$a = (m)\, b$ $\quad \gcd(56, 15)$

$\gcd(56, 15)$ $\quad 15\overline{)56}$ (

greatest common divisor ? 2 (56 , 15

(m) → . gcd.

$m = \gcd(a, b)$

↳ divisor of a & b.

$a = q\,b + (r_1)$

$0 \le r_1 < b$

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

8, 15 → 1, 2, 4 & 8 (1)

↳ 1, 3, 5 & 15

$a = bq + r$

$d =$

$n = 4$

$a - b$

$= r$

r_1

r_2

$d = \gcd(a, b)$

$d \mid r_1$

$d \mid a \quad \& \quad d \mid b$

$d \mid (a - q_1 b)$

(c)

$b \; r_1$

---

56 115.

$a = q_1 b + r_1$

$56 = 15 \cdot (3) + 11$

$15 = 11(1) + (4)$

$11 = 4(2) + (3)$

$4 = (3)(1) + (1)$

$\gcd(56, 15) = 1$

$28 = 20^\circ$

$0 < r_1 < b$

Extended Euclidean Alg

Rewrite

$56 \cdot s + 15 \cdot t = \gcd(56, 15)$

$s = -4$

$t = 15$

linear combination

$a = (b)(q) + (r)$

remainder is not unique.

$a = 42 \quad m = 9.$

$42 = 9(4) + (6) = (6)$

$42 - 6 = (36) = (9/36)$ ✓

$42 = 9(3) + 15 = 15.$

$42 + 15 = 27 = 9/27.$

$42 = 9(5) + (-3) \quad r = -3.$

$a - (r) = a - r$

$42 - (-3) = 45 \quad 9/45$

equivalence Classes.

$a = 12 \quad m = 5.$

$12 \equiv 2 \bmod 5 = 5/(12-2)$

$12 \equiv 7 \bmod 5 = 5/12-7.$

mod 5:

$= \{\ldots, 0, 5, 10, \ldots 25\}$

$\{\ldots -8, -3, 2, 7, 12, 15 \ldots\}$

{ -10 → 0, 5, 10 ... } A

{ -9, -4, 1, 6, 11 ... } B

} mod 5

Modular Arithmetic.

Congruent Modulo

2 int's a & b. mod n

if

$a \bmod n = b \bmod n$.

$a \equiv b \pmod n$

$b \equiv a \pmod n$

$73 = 4 \pmod{23}$ $\quad 73 \bmod 23 = 4 \bmod 23$.

Pro: $a \equiv b \pmod n$ if $n \mid (a-b)$

$a \equiv b \pmod n$ & $b \equiv a \pmod n$

$a \equiv b \pmod n$ & $b \equiv c \pmod n$

$a \equiv c \pmod n$.

$7 \bmod 4 = 3$

$-11 \bmod 7 = 3$.

$7 - (11 \% 7) = 7 - 4 = 3$.

$-x \bmod y = y - (x \bmod y)$.

if $|x| \bmod y \neq 0$; $|x| \bmod y = = 0$ if

auth

$(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

$(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

$(6+8) \bmod 2 = (6 \bmod 2 + 8 \bmod 2) \bmod 2$

$0 = (0 + 0)$

$(a \times b)$

let $a = 11 \quad b = 15 \quad n = 8$.

$(11 \times 15) \bmod 8 = 165 \bmod 8$

$= 5$

$(11 \bmod 8 \times 15 \bmod 8)$

$3 \times 7 = (21) \bmod 8$

$= 5$

$3^8 \bmod 2$

$= 3^4 \cdot 3^4$

$\Rightarrow (81 \times 81) \bmod 2$

$81 \bmod 2 \times 81 \bmod 2$

1

$11^7 \bmod 13$

~~11×4~~

$11^2 = 121 \equiv 4 \bmod 13 = 4$

$11^4 = (11^2)^2 \equiv 4^2 \bmod 13 = 3 \bmod 13$

$= 3$

$11^7 = 11^2 \times 11^4 \times 11^1$

$= 11 \times 4 \times 3 = 132 \bmod 13$

$= 2$

q	a	b	r	s_1	s_2	t_1	t_2	t
4	52	15	11	1	0	1	0	1

$s_1 = s_2 = 0$

$t_1 = 0, t_2 = 1$

$s = s_1 - s_2 \times q = 1 - 0 \times = 1$

$t = t_1 - t_2 \times q = 1 - 0 \times = 1$

(1)

Computing Inverse under

11 in Z_{26}

M.I.

gcd (26, 11) = 1

$r = t_1 - q t_2$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26

$r_2 \neq 0$

$r_2 = 0$

$t_1 \rightarrow$ M.I

$Z_n \rightarrow \{0, 1, 2 \ldots (n-1)\}$

$Z_2 = \{0, 1\}$

$Z_5 = \{0, 1, 2, 3, 4\}$

$0 - 2(1)$

$1 - (-2)(2) =$

$r_2 = 0 \quad t_1 = (-7)$

$Z_{25} = \{0, 1 \ldots 25\}$.

$t_1 = -7$.

26
-7
$19 \rightarrow M^{-1}$.

$\rightarrow 11 \times M^{-1} \equiv 1 \bmod 26$.

$11 \times 19 \equiv 1 \bmod 26$

$209 \equiv 1 \bmod 26$

$\rightarrow$ M.I 5 in Z_{12}.

$4^{99} \rightarrow$

$\rightarrow 4^3 \cdot 4^{24(4)}$

$4^3 \cdot 4^{24(4)}$

$4^{99} \bmod 35$.

$4^3 \bmod 35$

$(4^{24})^4 \bmod 35$

$1 \times 4^3 \bmod 35$

$64 \bmod 35$.

29

$x \quad \phi(n) \equiv 1 \bmod n$

$24 \quad (1)$

Eulers Theorem

$x^{\phi(n)} \equiv 1 \bmod n$.

x, n co.

$\phi(n) = 1$.

$\phi(n) = n - 1$

$\phi(35) = \phi(7) \cdot \phi(5)$

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

$= 6 \times 4$

$= 24$.

$x = 4$

$x^{\phi(n)} = 4^{\phi(35)} \cdot 99$

$= 4^{24}$.

$4^{24} = 4^2 = 1 \bmod 35$

$\phi(n) =$

$\phi(3) = \{0, 1, 2\}$

$\phi(5) = \{0, 1, 2, 3, 4\}$

$\phi(0) = \{1, 5\} = 2$