Modular Arithmetic

$a \bmod n = r$

$a = 11 \qquad n = 7$

$$\begin{array}{r} 1 \\ 7\overline{)\,11} \\ 7 \\ \hline 4 \end{array}$$

$11 \bmod 7 = 4$

$a = -11 \qquad n = 7$

$$\begin{array}{r} 2 \\ 7\overline{)\,-11} \\ 14 \\ \hline 3 \end{array}$$

$-11 \bmod 7 = 3$

Congruent Modulo

(1)

$a = 73 \qquad b = 4 \qquad n = 23$

$a \bmod n$

$73 \bmod 23$

$= 4$

$b \bmod n$

$4 \bmod 23$

$= 4$

$a \bmod n = b \bmod n$

$a = b \bmod n$

$73 = 4 \bmod 23$

(2)

$7 = 4 \bmod 3$

$$\begin{array}{r} 2 \\ 3\overline{)\,7} \\ 6 \\ \hline 1 \end{array} \qquad \begin{array}{r} 1 \\ 3\overline{)\,4} \\ 3 \\ \hline 1 \end{array}$$

Both 7 and 4 have remainder of 1

when divided by 3

Euclidean Algo Revisted

$a \geq b \geq 0$

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

$$\gcd(55,22) = \gcd(22, 55 \bmod 22)$$
$$= \gcd(22,11)$$
$$= \gcd(11,0) = 11$$

$$\gcd(18,12) = \gcd(12,6) = \gcd(6,0) = 6$$

$$\gcd(11,10) = \gcd(10,1) = \gcd(1,0) = 1$$

Extended Euclidean Algo

$\gcd(42,30)$ $\quad a = 42 \quad b = 30$

$$ax + by = d = \gcd(a,b)$$

$$42x + 30y$$

$x = 0$	$y = 0$
$y = -3 \Rightarrow -90$	$x = -3 \Rightarrow -126$
$y = -2 \Rightarrow -60$	$x = -2 \Rightarrow -84$
$y = -1 \Rightarrow -30$	$x = -1 \Rightarrow -42$
$y = 0 \Rightarrow 0$	$x = 0 \Rightarrow 0$
$y = 1 \Rightarrow 30$	$x = 1 \Rightarrow 42$
$y = 2 \Rightarrow 60$	$x = 2 \Rightarrow 84$
$y = 3 \Rightarrow 90$	$x = 3 \Rightarrow 126$

Extended Euclidean Algo Example

i	r	x	y_0	q_i
-1	1759	1	0	-
0	550	0	1	-
1	109	1	-3	3
2	5	-5	16	5

① $r_i = ax_i + by_i$

$r_{-1} = a$ $\quad a = 1759 \quad x_{-1} = 1 \quad y_{-1} = 0$

$r_0 = b$ $\quad b = 550 \quad x_0 = 0 \quad y_0 = 1$

② $r_1 = ax_1 + by_1$

$x_i = x_{(i-2)} - q_i x_{i-1} \Rightarrow x_{-1} - q_1 x_0$ $\quad q_1 = \lfloor a/b \rfloor$

$x_1 = x_{-1} - q_1 x_0$ $\quad q_1 = \frac{1759}{550} = 3$

$1 - 3(0) = 1$

$$\begin{array}{r} 3 \\ 550 \overline{)1759} \\ 1650 \\ \hline 109 \end{array}$$

$y_1 = y_{-1} - q_1 y_0$

$0 - 3(1) = -3$

$r_1 = 1759 + 550(-3) \Rightarrow 109$

③ $x_2 = x_0 - q_2 x_1$ $\quad q_2 = \lfloor \frac{b}{r_1} \rfloor$

$0 - q_2(1) = -q_2 \Rightarrow -5$

$$\begin{array}{r} 5 \\ 109 \overline{)550} \\ 545 \\ \hline 5 \end{array}$$

$y_2 = y_0 - q_2 y_1 \Rightarrow 1 - 5(-3) = 16$

$r_2 = ax_2 + by_2$

$= 1759(-5) + 550(16) = 5$

$\Rightarrow r_2 = b \bmod r_1 \quad , r_3 = r_1 \bmod r_2$

PRIME Number

$91 = 7 * 13$

$3600 = 2^4 \times 3^2 \times 5^2$

$11011 = 7 \times 11^2 \times 13$

Fermat Theorem

① $p = 5 \quad a = 3$

$a^p = a \bmod p$

$3^5 = 3 \bmod 5$

$243 = 3 \bmod 5$

② $p = 5 \quad a = 10$

$a^p = 10^5 = 100000 = 10 \bmod 5$

Euler Totient Function $\varphi(n)$

$\varphi(1) = 1$

$\varphi(P) = P - 1$

$\varphi(19) = 19 - 1 = 18$

$\varphi(29) = 28$

$n = 10$

1, 2, 3, 4, 5, 6, 7, 8, 9

1, 10

Factors 1 Relative Prime

1, 2, 5, 10

2, 10 Not Relative Prime

1, 2

1, 2, 5, 10

3, 10

1, 3 Relative Prime

1, 2, 5, 10

4, 10

1, 2, 4 Not Relative Prime

1, 2, 5, 10

5, 10 Not Relative Prime

1, 5

1, 2, 5, 10

10 = 1, 3, 7, 9

$\varphi(10) = 4$

$$\varphi(15) = \varphi(3) \times \varphi(5)$$

$$\varphi(P) = P-1$$

$$= (3-1) \times (5-1)$$

$$= 2 \times 4 = 8$$

$$\varphi(21) = \varphi(3) \times \varphi(7)$$

$$(3-1) \times (7-1)$$

$$= 12$$

Euler Theorem

$$a^{\varphi(n)} = 1 \bmod n$$

(1) $a = 3$ $n = 10$

$$\varphi(n) = \varphi(10) = 4$$

$$a^{\varphi(n)} = 3^4 = 81 = 1 \bmod 10$$

$$= 1 \bmod n$$

(2) $a = 2$ $n = 11$

$$\varphi(11) = 10$$

$$a^{\varphi(n)} = 2^{10} = 1024 = 1 \bmod 11$$

$$= 1 \bmod n$$