Numbers Theory and Cryptography

Divisibility

Defn: If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say that a divides b we can write $a \mid b$ if

$$b = ak$$

for some $k \in \mathbb{Z}$

Example:

$2 \mid 16$ because $16 = 2 \cdot 4$

$3 \mid 90$ because $90 = 3 \cdot 30$

$1 \mid n$ because $n = 1 \cdot n$

$2 \nmid 3$ because we can't write 3 as integers multiple of 2

[4] **Proposition:**

Let a, b and c be integers, where $a \neq 0$, then

1. If $a|b$ and $b|c$, then $a|c$
2. If $a|b$ then $ca|cb$
3. If $a|b$ and $a|c$ then

for all $x, y \in Z$

$$a \mid (bx + cy)$$

proof-1: suppose, $a|b$ and $b|c$

we can write

$$b = ak, \quad c = bl$$

for $k, l \in Z$ so,

$$c = bl$$
$$\Rightarrow c = (ak)l$$
$$\Rightarrow c = a(kl)$$
$$\Rightarrow c = ak'$$

Thus, $a|c$

Claim: If $a \mid 1$, then $a = \pm 1$

proof: suppose,

$a \mid 1$ thus,

$1 = ak$ for $k \in Z$

so, $1 = |a||k|$ and

$1 \leq |a| = |\frac{1}{k}| \leq 1$

thus, $|a| = 1$

and, $a = \pm 1$

Division Algorithm

For all $a, b \in \mathbb{Z}$, with $b > 0$, there exist unique $q, r \in \mathbb{Z}$, such that $a = bq + r$ with $0 \leq r < b$

$q \rightarrow$ quotient
$r \rightarrow$ remainder

Example: $a = 21$, $b = 2$

$$21 = 2 \times 10 + 1$$
$$\downarrow \quad \downarrow$$
$$q \quad r$$

$a = 35$, $b = 6$

$$35 = 6 \times 5 + 5$$
$$\downarrow \quad \downarrow$$
$$q \quad r$$

proof: consider,

$$S = \{ a - bx \mid x \in z,\ a - bx \geq 0 \}$$

Ex: $a = 12,\ b = 5.$

x	$12 - 5x$
-2	22
-1	17
0	12
1	7
2	2
3	-3

$\downarrow \notin S$

$S = \{2, 7, 12, 17, 22, \ldots\}$

claim: $S \neq \phi$

case-1: $a \geq 0 \quad (x = 0)$

$a - b(0) = a \in S$

case-2: $a < 0$, set $x = a$

$a - bxa = a(1 - b)$ $\quad b > 0$

$<0 \quad \times \quad \leq 0$

≥ 0

$a - ba \in S$

Let, $r = \min(S)$, q is the correspondence x value

(*) $r = a - bq$

$\Rightarrow a = bq + r$

Towards a contradiction,

suppose, $r \geq b$

$\Rightarrow r = a - bq \geq b$

$\Rightarrow r - b = a - b(q+1) \geq b - b = 0$

$\Rightarrow r - b \in S$ but $r - b < r = \min(S)$

Proof: suppose that,

q, q' and r, r' are such that

$$a = bq + r = bq' + r'$$

assume: $r' \geq r$

$$bq + r = bq' + r'$$

$$\Rightarrow b(q - q') = r' - r$$

L.H.S: multiple of b

R.H.S: $0 \leq r' - r < b$

$$L.H.S = R.H.S = 0$$

$$\therefore r' - r = 0 \quad | \quad q - q' = 0$$

$$\Rightarrow r' = r \quad | \quad \Rightarrow q = q'$$

Ex: what are the quotient and remainder when -11 is divided by 3?

Soln:

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

or,

$$-11 = 3(-3) - 2$$

$r = -2$ does not satisfy $0 \leq r < 3$

$\therefore$ quotient $= -4$

remainder $= 1$

Modulare arithmatic

- **Congruence**: in cryptography, congruence ($\equiv$) instead of equality ($=$).

Example: $15 \equiv 3 \pmod{12}$

(3 ↓ remainder, 12 ↓ divisor)

$23 \equiv 11 \pmod{12}$

$10 \equiv -2 \pmod{12}$

- $a = b \pmod{m}$

(b ↓ remainder, m ↓ divisors)

i.e., $a = km + b$

[a, b → integers; m → positive integers]

- $a = b \pmod{m}$ is valid when $\frac{a-b}{m}$ is divisible.

- $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Valid or Invalid

$38 \equiv 2 \pmod{12} \rightarrow$ valid

$38 \equiv 14 \pmod{12} \rightarrow$ valid

$5 \equiv 0 \pmod{5} \rightarrow$ valid

$10 \equiv 2 \pmod{6} \rightarrow$ Invalid

$13 \equiv 3 \pmod{13} \rightarrow$ Invalid

$2 \equiv -3 \pmod{5} \rightarrow$ valid

$-8 \equiv 7 \pmod{5} \rightarrow$ valid

$-3 \equiv -8 \pmod{5} \rightarrow$ valid

Properties of modulate arithmatic:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
4. $(a \bmod n) + (b \bmod n) \pmod n = a+b$
5. $(a \bmod n)(b \bmod n) \pmod n = ab$

Example:

1. $[(15 \bmod 8) + (11 \bmod 8)] \bmod 8 = (15+11) \bmod 8$
$= 26 \bmod 8$
$= 2$

2. $[(15 \bmod 8) - (11 \bmod 8)] \bmod 8 = (15-11) \bmod 8$
$= 4 \bmod 8$
$= 4$

3. $[(15 \bmod 8) \times (11 \bmod 8)] \bmod 8 = (15 \times 11) \bmod 8$
$= 165 \bmod 8$
$= 5$

4.

Arithmetic Modulo

1. $a +_m b = (a+b) \bmod m$
2. $a \cdot_m b = (a \cdot b) \bmod m$

Example:

$$7 +_{11} 9 = (7+9) \bmod 11$$
$$= 16 \bmod 11$$
$$= 5$$

$$7 \cdot_{11} 9 = (7 * 9) \bmod 11$$
$$= 63 \bmod 11$$
$$= 8$$

Properties:

1. Commutative Laws: $(a+b) \bmod n = (b+a) \bmod n$

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

2. Associative Laws: $[(a+b)+c] \bmod n = [a+(b+c)] \bmod n$

3. Distributive Laws: $[a \times (b+c)] \bmod n = [(a \times b)+(a \times c)] \bmod n$

4. Identities Laws: $(0+a) \bmod n = a \bmod n$

$(1 \times a) \bmod n = a \bmod n$

5. Additive Inverse: For each $a \in Z_n$, there exists a '$-a$' such that $a+(-a) = 0 \bmod n$

Integers Representations and Algorithms

Representation of Integers:

Let $b \in Z$ and $b > 1$. If $n \in Z^+$, then it can be expressed uniquely in the form,

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where, k is a nonnegative integers.

$a_0, a_1, \ldots, a_k$ are nonnegative integers, less than b.

$a_k \neq 0$.

1. This representation is called the base b expression of n

2. Denoted by $(a_k a_{k-1} \cdots a_1 a_0)$

Examples:

$(534)_{10} = 5\times10^2 + 3\times10^1 + 4\times10^0 = (534)_{10}$

$(642)_8 = 6\times8^2 + 4\times8^1 + 2\times8^0 = (418)_{10}$

$(10101111)_2 = 1\times2^8 + 0\times2^7 + 1\times2^6 + 0\times2^5 + 1\times2^4 + 1\times2^3 + 1\times2^2 + 1\times2^1 + 1\times2^0$

$= (351)_{10}$

$(2AE0B)_{16} = 2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16 + 11\cdot16^0$

$= (175627)_{10}$

Base Conversion

integers, n, $q \rightarrow$ quotient
base b $a_0 \rightarrow$ remainders

At first,

$$n = bq_0 + a_0 \quad , 0 \leq a_0 < b$$

$$q_0 = bq_1 + a_1 \quad , 0 \leq a_1 < b$$

a_0 is the right most digit in the base b ~~exap~~ expansion of n.

Example: $(12345)_{10} = (\quad)_8$

$12345 = 8 \cdot 1543 + 1$
$1543 = 8 \cdot 192 + 7$
$192 = 8 \cdot 24 + 0$
$24 = 8 \cdot 3 + 0$
$3 = 8 \cdot 0 + 3$

$(12345)_{10} = (30071)_8$

(*) $(177130)_{10} = (\quad)_{16}$

$177130 = 16 \times 11070 + 10$

$11070 = 16 \times 691 + 14$

$691 = 16 \times 43 + 3$

$43 = 16 \times 2 + 11$

$2 = 16 \times 0 + 2$

$(177130)_{10} = (2B3EA)_{16}$

(*) $(241)_{10} = (\quad)_2$

$241 = 2 \cdot 120 + 1$

$120 = 2 \times 60 + 0$

$60 = 2 \times 30 + 0$

$30 = 2 \times 15 + 0$

$15 = 2 \times 7 + 1$

$7 = 2 \times 3 + 1$

$3 = 2 \times 1 + 1$

$1 = 2 \times 0 + 1$

$(241)_{10} = (11110001)_2$

Algorithm: Constructing Base b Expansions:

procedure base b expansion ($n, b \in Z^+ : b > 1$)

$q := n$

$k := 0$

while $q \neq 0$

$a_k = q \bmod b$

$q := q \text{ div } b$

$k := k + 1$

end while

return $(a_{k-1}, \ldots, a_1, a_0)$

{ $(a_{k-1} \ldots a_1 a_0)_b$ is the base b expansion of n

☐ Binary to hexadecimal and octal.

$(11111011\ 1100)_2$ 8+4+2+1

hex:

0011 1110 1011 1100

3 | 14→E | 11→B | 12→C

$\therefore (11\ 1110\ 1011\ 1100)_2 = (3EBC)_{16}$

oct:

011 111 010 111 100

3 | 7 | 2 | 7 | 4

$\therefore (11\ 1110\ 1011\ 1100)_2 = (37274)_8$

☐ $(765)_8 = (\quad)_2$

7 → 111 | 6 → 110 | 5 → 101

$(765)_8 = (111110101)_2$

☐ $(A8D)_{16} = (\quad)_2$

A → 1010 | 8 → 1000 | D → 1101

$\therefore (A8D)_{16} = (1010\ 1000\ 1101)_2$

Algorithm for Integers Operations

Let, binary expansion,

$$a = (a_{n-1} \cdot a_{n-2} \cdots a_1 a_0)_2$$

$$b = (b_{n-1} \cdot b_{n-2} \cdots b_1 b_0)_2$$

addition:

$$a_0 + b_0 = c_0 \cdot 2 + s_0$$

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$$

↓

continue

[$c_0 \rightarrow$ carry in binary which is either 0 or 1]

$$a + b = (s_n s_{n-1} \cdots s_1 s_0)$$

Example: $a = (1110)_2$ and $b = (1011)_2$

$a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1$
$\downarrow \quad \downarrow$
$c_0 \quad s_0$

$a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0$
$\downarrow \quad \downarrow$
$c_1 \quad s_1$

$a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0$
$\downarrow \quad \downarrow$
$c_2 \quad s_2$

$a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1$
$\downarrow \quad \downarrow$
$c_3 \quad s_3$

$\therefore \quad s_4 = c_3 = 1$

$\therefore \quad a + b = (11001)_2$

```
 1 1 1
   1 1 1 0
   1 0 1 1
-----------
 1 1 0 0 1
```

Algorithm: Addition of Integers

procedure: add (a, b: positive integers)

{the binary expansions of a and b are $(a_{n-1}a_{n-2}\cdots a_1 a_0)_2$ and $(b_{n-1}b_{n-2}\cdots b_1 b_0)_2$ respectively}

$c := 0$

for $j := 0$ to $n-1$

$d = \lfloor (a_j + b_j + c)/2 \rfloor$

$s_j := a_j + b_j + c - 2d$

$c := d$

end for

$s_n := c$

return $(s_0, s_1 \cdots s_n)$

{the binary expansion of the sum is $(s_n s_{n-1}\cdots s_0)_2$}

Multiplication:

$$ab = a(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1})$$

$$= a(b_0 2^0) + a(b_1 2^1) + \cdots a(b_{n-1} 2^{n-1})$$

Note:

$ab_j = a$ if $b_j = 1$

$ab_j = 0$ if $b_j = 0$

Each time we multiply a term by 2, we shift its binary expansion one place to the left and add a zero at the tail end of the expansion.

Consequently, we can obtain $(ab_j)2^j$ by shifting the binary expansion of ab_j j places to the left, adding j zero bits at the tail end of this binary expansion.

Finally, we obtain ab by adding n integers,

$ab_j 2^j$, $j = 0, 1, 2, \cdots n-1$

Division Algorithm

Given $a, d \in \mathbb{Z}$ with $d > 0$

Find $q = a \text{ div } d$ and $r = a \bmod d$

Example: Find $19 \text{ div } 4$ and $19 \bmod 4$

$19 - 4 = 15$
$15 - 4 = 11$
$11 - 4 = 7$
$7 - 4 = 3$

} subtract 4 times

$\therefore 19 \text{ div } 4 = 4$

$19 \bmod 4 = 3$

Algorithm:

procedure: division algorithm $(a \in Z, d \in Z^+)$

```
q := 0
r := |a|
while r ≥ d                    } count how many times
    r := r - d                   you can subtract the
    q := q + 1                   divisor from dividend
end while
if a < 0 and r > 0             } for negative numbers
    r := d - r
    q := -(q+1)
return (q, r)
```

Example: -19 div 4 and $r = -19 \bmod 4$

$q = 0$

$r = 19$

while: $r \geq 4$ $\quad q = 0$

$19 - 4 = 15 \quad q = 1$

$15 - 4 = 11 \quad q = 2$

$11 - 4 = 7 \quad q = 3$

$7 - 4 = 3 \quad q = 4$

$\therefore q = 4, \; r = 3$

end of while loop

$r = d - r$

$4 - 3 = 1$

$q = -(q+1) = -5$

$\therefore -19 \text{ div } 4 = -5, \quad -19 \bmod 4 = 1$

Modular Exponentiation

Compute $b^n \bmod m$ efficiently

Let, $n = (a_{k-1} \cdot a_{k-2} \cdots a_1 a_0)_2$

$$b^n = b^{a_{k-2} \cdot 2^{k-1} + \cdots + a_1 2^1 + a_0}$$

$$= b^{a_{k-1} \cdot 2^{k-1}} \times b^{a_{k-2} \cdot 2^{k-1}} \times \cdots \times b^{a_1 2^1} \times b^{a_0}$$

Compute: $3^{11} \bmod 5$

$n = 11 = (1011)_2$, $b = 3$, $m = 5$

$$3^{11} = 3^{(1011)_2}$$

$$= 3^{(1 \times 2^3 + 0 \times 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0)}$$

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

then, we need to calculate $3, 3^2, 3^4, 3^8 \pmod 5$

$$3 \bmod 5 = 3$$

$$3^2 \bmod 5 = [(3 \bmod 5) \times (3 \bmod 5)] \bmod 5$$

$$= (3 \times 3) \bmod 5$$

$$= 4$$

$3^4 \bmod 5 = [(3^2 \bmod 5) \times (3^2 \bmod 5)] \bmod 5$

$= (4 \times 4) \bmod 5$

$= 1$

$3^8 \bmod 5 = [(3^4 \bmod 5) \times (3^4 \bmod 5)] \bmod 5$

$= (1 \times 1) \bmod 5$

$= 1$

$3^2 \cdot 3^1 \bmod 5 = [(3^2 \bmod 5) \times (3^1 \bmod 5)] \bmod 5$

$= (4 \times 3) \bmod 5$

$= 2$

$3^8 \cdot 3^2 \cdot 3^1 \bmod 5 = [(3^8 \bmod 5) \times (3^2 \cdot 3 \bmod 5)] \bmod 5$

$= (1 \times 2) \bmod 5$

$= 2$

$\therefore 3^{11} \bmod 5 = 177147 \bmod 5 = 2$

Algorithm: Modular exponentiation

Procedure: mod exp (b ∈ Z , n $(a_{k-1} \cdot a_{k-2} \cdots a_1 a_0)_2$, m ∈ Z^+)

```
x := 1
power := b mod m
for i := 0 to k-1
    if a_i = 1 then x := (x · power) mod m
    power := (power · power) mod m
end for
return (x)  { x equals b^n mod m }
```

(*) longest number generated was (m-1)(m-1)
mod exponent $O((\log m)^2 \cdot (\log n)) \approx O(m^2)$

Compute $3^{171} \bmod 25$:

$$3^{171} = 3^{(10101011)_2}$$

$$= 3^{(1\times2^7+0\times2^6+1\times2^5+0\times2^4+1\times2^3+0\times2^2+1\times2^1+1\times2^0)}$$

$$= 3^{128} \cdot 3^{32} \cdot 3^{8} \cdot 3^{2} \cdot 3^{1}$$

		start		end	
i	a_i	x	power	x	power
0	1	1	3	3	9
1	1	3	9	2	6
2	0	2	6	2	11
3	1	2	11	22	21
4	0	22	21	22	16
5	1	22	16	2	6
6	0	2	6	2	11
7	1	2	11	22	11

return (22)

$$3^{171} \bmod 25 = 22$$

at first $x = 1$

power $= 3 \bmod 25$

$= 3$

loop start:

$x = (x \cdot \text{power}) \bmod m$

$\text{power} = (\text{power} \cdot \text{power}) \bmod m$

$x = (1 \times 3) \bmod 25 = 3$

$\text{power} = (3 \times 3) \bmod 25 = 9$

$a_i = 0$

$x = (3 \times 9) \bmod 25 = 2$

$\text{power} = (9 \times 9) \bmod 25 = 6$

~~$x = (2 \times 6) \bmod 25 =$~~

$\text{power} = (6 \times 6) \bmod 25 = 11$

$a_i = 0$

$x = (2 \times 11) \bmod 25 = 22$

$\text{power} = (11 \times 11) \bmod 25 = 21$

~~$x = (22 \times 21) \bmod 25 =$~~

$\text{power} = (21 \times 21) \bmod 25 = 16$

$x = (22 \times 16) \bmod 25 = 2$

$power = (16 \times 16) \bmod 25 = 6$

also $power = (6 \times 6) \bmod 25 = 11$

$x = (2 \times 11) \bmod = 22$

$power = (11 \times 11) \bmod = 21$

Primes and Greatest Common Divisors

Primes: An integer $p > 1$ is prime if it's only positive factors are 1 and p.

* If a positive integer greater than 1 is not prime then it is composite

Ex:

11 is prime

15 is composite

$15 = 3 \times 5$

The Fundamental theorem of Arithmetic:

For every integers greater than 1 can written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.

Ex: Find the prime factorization of

a) 65
b) 999
c) 100
d) 1024

Sol:

$65 = 5 \times 13$

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Trial Division

Theorem: If n is a composite number, then n has a prime divisor $\leq \sqrt{n}$.

Trial division: Divide n by all primes not exceeding $\sqrt{n}$.

Example: Show that 107 is prime.

The primes $\leq \sqrt{107} \approx 10$ are $\{2, 3, 5, 7\}$

$\frac{107}{2} = 53.5$, $\frac{107}{3} = 35.96$ $\frac{107}{5} = 21.4$

$\frac{107}{7} = 15.29$

$\therefore$ 107 is prime

Example: Find the prime factorization of 9,555.

The primes $\leq \sqrt{9,555} \approx 63$ are $\{2, 3, 5, 7, 11, \ldots$

$\frac{9555}{2} = 4777.5$

$\frac{9555}{3} = 3185$ $\quad \frac{3185}{3} = 1061.666\ldots$

$\frac{3185}{5} = 637$ $\quad \frac{637}{5} = 127.4$

$\frac{637}{7} = 91$ $\quad \frac{91}{7} = 13$

$\therefore 9555 = 3 \times 5 \times 7^2 \times 13$

The Siere of Enatosthenes

Goal → Find all primes $\leq n$

Let, $P_1, P_2, \cdots P_k$ be all the primes $\leq n$

for $i = 1 : k$

delete all numbers between 1 and n tha
are multiples of P_i

end for

Example: Find all primes ≤ 40

$\sqrt{40} \approx 6.32$

primes are {2, 3, 5}

delete multiples of 2, 3 and 5

① 2 3 4 5 6 7 8 9 10

11 12 13 14 15 16 17 18 19 20

21 22 23 24 25 26 27 28 29 30

31 32 33 34 35 36 37 38 39 40

∴ prime numbers:

2, 3, 5, 7, 11, 13,

17, 19, 23, 29, 31

37

Greatest Common Divisors:

Let a and b be integers, not both zero. The largest integers d such that $d|a$ and $d|b$ is called the greatest common divisors of a and b. the greatest common divisors of a and b is denoted by gcd(a, b).

Ex: what is the greatest common divisors of 18 and 45?

18 → divisors → 1, 2, 3, 6, 9, 18

45 → divisors → 1, 3, 5, 9, 15, 45

$\therefore$ gcd(18, 45) = 9

(*) what is the greatest common divisor of 16 and 21 ?

16 : 1, 2, 4, 8, 16

21 : 1, 3, 7, 21

$\gcd(16, 21) = 1$

(*) $a, b \in \mathbb{Z}$ are relatively prime if

$$\gcd(a, b) = 1$$

Prime factorization method:

Suppose, a and b two positive integers

$$a = p_1^{a_1} \times p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} \times p_2^{b_2} \cdots p_n^{b_n}$$

$$\therefore \gcd(a,b) = p_1^{\min(a_1,b_1)} \; p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

least common multiple (lcm)

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

Example: Find the gcd and lcm of 120 and 500.

Sol^{n}:

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

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

$$\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$$

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

$$= 20$$

$$\text{lcm}(120, 500) = 2^{\max(3,2)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,3)}$$

$$= 2^3 \cdot 3^1 \cdot 5^3$$

$$= 3000$$

(*) $ab = 120 \times 500$

$= 60,000$

$ab = \gcd(120, 500) \cdot \text{lcm}(120, 500)$

$= 20 \times 3000$

$= 60,000$

Euclid Algorithm for finding GCD:

① Find the GCD (12, 33)

Q → Quotient
R → Remainder
A → Bigestone

A/B

Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
X	3	0	X

result

∴ GCD (12, 33) = 3

Algorithm:

procedure ; gcd (a, b : positive integers) [a ≥ b]

```
x := a
y := b
while y ≠ 0
    r := x mod y
    x := y
    y := r
return (x), {gcd (a,b) is x}
```

Bezout's Theorem

If a and b are positive integers, then there exists integers x, y such that:

$$\gcd(a,b) = \underbrace{ax + by}_{\text{Bezout coefficient}}$$

Ex:

$$\gcd(4,16) = 4$$

$$4(5) + 16(-1) = 4$$

($x = 5$, $y = -1$)

$$4 \times (1) + 16(0) = 4$$

($x = 1$, $y = 0$)

Extended Euclidean Algorithm: (Finding Bezouts coefficient

Example:

$40, 64 = (a, b)$, $\quad gcd(40, 64) = 8$

$d = 8$

$40 | 64 = 1 + 24$

$24 | 40 = 1 + 16$

$16 | 24 = 1 + 8$

$8 | 16 = 2 + 0$

↓

gcd → using Euclidean algorithm

$64 = 1 \times 40 + 24$

$40 = 1 \times 24 + 16$

$24 = 1 \times 16 + 8$

$16 = 2 \times 8 + 0$

$24 = 64 - 1 \times 40$

$16 = 40 - 1 \times 24$

$8 = 24 - 1 \times 16$

$8 = 24 - 1 \times 16$

$= 24 - 1 \times (40 - 1 \times 24)$

$= 24 - 40 + 24$

$= 2 \times 24 - 40$

$= 2 \times (64 - 1 \times 40) - 40$

$= 2 \times 64 - 2 \times 40 - 40$

$= 2 \times 64 - 3 \times 40$

↓ x, ↓ y

Bezout coefficients

∴

Linear Congruence

Congruent :

Defⁿ: Given $n \in N$. and $a, b \in Z$,

we can say a is congruent to b modulo n and write $a \equiv b \pmod{n}$ if $n \mid a-b$.

→ a and b have the same remainders when it's divided by n.

Ex:

1. $8 \equiv 3 \pmod{5}$

   $5 \mid 8-3$

2. $20 \equiv 4 \pmod{8}$

   $8 \mid 20-4$

3. $13 \equiv -1 \pmod{7}$

   $7 \mid 13-(-1)$

proposition:

$\equiv \pmod n$ is a equivalence relation

That is:

1. For all $a \in Z$

$$a \equiv a \pmod n \quad \text{[reflexive]}$$

2. For all $a, b \in Z$

if $a \equiv b \pmod n$ then

$$b \equiv a \pmod n \quad \text{[symmetry]}$$

3. For all $a, b, c \in Z$

if $a \equiv b \pmod n$ and

$b \equiv c \pmod n$ then

$$a \equiv c \pmod n$$

[transitivity]

proof: suppose, $a \equiv b \pmod n$

$b \equiv c \pmod n$

$n \mid a-b$ $\quad \cdot\cdot$ $n \mid b-c$

$\therefore a-b = nk$ —(i) $\quad \therefore b-c = nl$ —(ii)

(i) + (ii) $\quad a-c = n(l+k)$

$\therefore a \equiv c \pmod n$

Def^n: For $x \in \mathbb{Z}$ define the equivalence class x with respect to $\equiv \pmod n$ by following.

$$[x] = \{a \in \mathbb{Z} \mid a \equiv x \pmod n\}$$

Example: $n = 3$, $x = 0$

$$[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}$$

$$= \{0, \pm 3, \pm 6, \cdots\}$$

$$[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}$$

$$= \{\cdots, -5, -2, 1, 4, 7, 10 \cdots\}$$

$$[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}$$

$$= \{\cdots, -4, -1, 2, 5, 8, \cdots\}$$

⊛ **Fact:** There are exactly n equivalent classes modulo n

$[0], [1], [2], \ldots\ldots\ldots, [n-1]$

Def^n: Fix n, the set of least residues is given by $\{0, 1, \ldots\ldots\ldots, n-1\}$

claim: For all $a \in \mathbb{Z}$, a is congruent to exactly one of the least residues modulo n.

proof: use div alg. with a and n

$a = nq + r$ with ~~$r = 0 = n-1$~~ $0 \leq r \leq n-1$

$a - r = nq$

$\therefore a \equiv r \pmod{n}$

Some more properties of $\equiv \pmod{n}$

prop: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

then, $a+c \equiv b+d \pmod{n}$

$ac \equiv bd \pmod{n}$

proof: $a \equiv b \pmod{n}$

$\Rightarrow a-b = nk$ — (i)

$c \equiv d \pmod{n}$

$\Rightarrow c-d \equiv nl$ — (ii)

(i) + (ii) $a+c-b-d = n(k+l)$

$\Rightarrow a+c-(b+d) = nk', \quad k \in \mathbb{Z}$

$\therefore a+c \equiv b+d \pmod{n}$

$a-b = nk$

$\Rightarrow a = b+nk$ — (i)

$c-d = nl$

$\Rightarrow c = d+nl$ — (ii)

(i) × (ii), $ac = bd + nbl + ndk + n^2kl$

$\Rightarrow ac = bd + n(kd + lb + nkl)$

$\therefore ac - bd = nk', \quad k \in \mathbb{Z}$

$\therefore ac \equiv bd \pmod{n}$

Prop: If $a \equiv b \pmod{m}$ and $n \mid m$, then $a \equiv b \pmod{n}$

proof: $a \equiv b \pmod{m}$ and $n \mid m$.

$a - b = mk$ $\qquad m = nl$

$\Rightarrow a - b = nlk$

$\therefore a \equiv b \pmod{n}$

Ex: $5 \equiv 1 \pmod{4}$ $\qquad 2 \mid 4$

$\therefore 5 \equiv 1 \pmod{2}$

When we can cancel c in $ca \equiv cb \pmod{n}$?

prop: For $a, b, c \in \mathbb{Z}$, we have

$$ca \equiv cb \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{\gcd(n,c)}}$$

proof: suppose,

$$ca \equiv cb \pmod{n}$$

$$\Rightarrow n \mid ca - cb$$

$$\rightarrow n \mid c(a-b)$$

$$\Rightarrow c(a-b) = nk, \quad k \in \mathbb{Z}$$

Let, $d = \gcd(n,c)$

$$c(a-b) = nk$$

$$\Rightarrow \frac{c}{d}(a-b) = \frac{n}{d}k$$

$$\Rightarrow a-b = \frac{n}{d}k' \quad [k' \in \mathbb{Z}, \ k' = \frac{k}{d}]$$

$$\therefore a \equiv b \pmod{\frac{n}{d}}$$

$$\therefore \boxed{a \equiv b \pmod{\frac{n}{\gcd(n,c)}}}$$

$\because \gcd\left(\frac{c}{d}, \frac{n}{d}\right) = 1$

$\frac{c}{d}, \frac{n}{d}$ relatively prime.

so, $a-b$ definally comes from multiple of $\frac{n}{d}$.

Ex:

$2a \equiv 0 \pmod 4$

$\Rightarrow 2a \equiv 2.0 \pmod 4$

$3x \equiv 12 \pmod{15}$

$3x \equiv 3.4 \pmod{15}$

$\therefore x \equiv 4 \pmod{\frac{15}{\gcd(3,15)}}$

$x \equiv 4 \pmod{\frac{15}{3}}$

$x \equiv 4 \pmod 5$

Find all $n \in N$.

$$24 \equiv 10 \pmod{n}$$

$$\therefore n \mid 24-10$$

$$\Rightarrow n \mid 14$$

$$\therefore n \in \{1, 2, 7, 14\}$$

Ex:

$$24 \equiv 0 \pmod{2} \qquad 24 \equiv 3 \pmod{7}$$

$$10 \equiv 0 \pmod{2} \qquad 10 \equiv 3 \pmod{7}$$

Find all $n \in N$.

$$32 \equiv 20 \pmod{n}$$

$$n \mid 32-20$$

$$\Rightarrow n \mid 12$$

$$n \in \{1, 2, 3, 4, 6\}$$

Ex:

$$32 \equiv 2 \pmod{6}$$

$$20 \equiv 2 \pmod{6}$$

Find the least residue:

Ex: $28^{13} \pmod{10}$

Note: $28 \equiv -2 \pmod{10}$

$13 = 8+4+1$

$28^{13} \equiv (-2)^{13} \equiv (-2)^8 \cdot (-2)^4 \cdot (-2)^1$

$(-2)^0 = 1$

$(-2) = -2$

$(-2)^2 = 4$

$(-2)^4 = 16 \pmod{10} = 6$

$(-2)^8 = 36 \pmod{10} = 6$

$(-2)^8 \cdot (-2)^4 \cdot (-2)^1$

$= 6 \times 6 \times -2$

$= 36 \times -2$

$= 6 \times -2$

$= -12 \pmod{10}$

$= 8 \pmod{10}$

[$36 \pmod{10} = 6$]

$28^{13} \pmod{10}$

$= 8 \pmod{10}$

Find the least residue:

$$12! \pmod{13}$$

$$= 1.2.3.4.5.6.7.8.9.10.11.12 \pmod{13}$$

$$= 1\times2\times3\times4\times5\times6\times(-6)\times(-5)\times(-4)\times(-3)\times(-2)\times(-1) \pmod{13}$$

$$= 1\times2\times3\times4\times5\times6\times6\times5\times4\times3\times2\times1 \pmod{13}$$

$$= (2\times6)^{\checkmark}\times(3\times4)^{\checkmark}\cdot5^{\checkmark} \pmod{13}$$

$$= 12^{\checkmark}\times12^{\checkmark}\times5^{\checkmark} \pmod{13}$$

$$= (-1)^{\checkmark}\times(-1)^{\checkmark}\times(-1) \pmod{13}$$

$$= -1 \pmod{13}$$

$$= 12 \pmod{13}$$

Linear Congruence

proposition: The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a,n) \mid b$

proof: (forward) Suppose that, x_0 is a solution.

$$ax_0 \equiv b \pmod{n}$$

$$\Rightarrow n \mid ax_0 - b$$

$$\Rightarrow ax_0 - b = nk \quad \text{for } k \in \mathbb{Z}$$

$$\Rightarrow b = ax_0 - nk$$

$$= ax_0 + (-k)n$$

$$= l \gcd(a,n) \quad \text{for } l \in \mathbb{Z}$$

$\therefore \gcd(a,n) \mid b$

[is a multiple of $\gcd(a,n)$ ↓ Bezout's coefficient]

proof: suppose that,

(backward) $\gcd(a,n) \mid b$

$\Rightarrow b = \gcd(a,n) \cdot m$ for $m \in \mathbb{Z}$

we can write, $\gcd(a,n) = ay + nz$

for $y, z \in \mathbb{Z}$

$\therefore b = (ay + nz)m$

$\Rightarrow b = aym + n(zm)$

$\Rightarrow b - a(ym) = n(zm)$

$\therefore a(ym) \equiv b \pmod{n}$

$\therefore ym$ is a solution to

$ax \equiv b \pmod{n}$

Ex: $4x \equiv 3 \pmod{18}$

Soln:

$\gcd(4, 18) = 2$

$2 \nmid 3$ means 3 is not divisible by 2

so, it has no soln.

Ex: $4x \equiv 6 \pmod{18}$

Soln:

$\gcd(4, 18) = 2$

$\therefore 2 \mid 6$, so, there is a solution.

$4x = 18k + 6$ for $k \in \mathbb{Z}$

$k = 0$, $4x = 6$ ✗

$k = 1$, $4x = 18 \cdot 1 + 6$

$\Rightarrow x = 6$

$k = 2$, $4x = 18 \times 2 + 6$ ✗

$k = 3$, $4x = 18 \times 3 + 6$

$\Rightarrow x = 15$

$x \equiv 6 \pmod{18}$

$x \equiv 15 \pmod{18}$

Prop: Suppose, $\gcd(a,n) \mid b$, then $ax \equiv b \pmod{n}$ has $\gcd(a,n)$ distinct solutions; separated by $\frac{n}{\gcd(a,n)}$.

Proof: Let, $d = \gcd(a,n)$

Suppose that, x_0 is a solution.

Consider, $x_0 + \frac{n}{d}k$ for $k \in \mathbb{Z}$.

So, now,

$$\begin{aligned} a\left(x_0 + \frac{n}{d}k\right) &= ax_0 + \left(\frac{a}{d}k\right)n \\ &\equiv ax_0 \pmod{n} \\ &\equiv b \pmod{n} \end{aligned}$$

So, $x_0 + \frac{n}{d}k$ are solution to $ax \equiv b \pmod{n}$

These are separated by $\frac{n}{d} = \frac{n}{\gcd(a,n)}$

$x_0 + \frac{n}{d}k$ is a solution $\forall\ k \in \mathbb{Z}$

⊛ How many are incongruent?

suppose,

$$x_0 + \frac{n}{d}k_1 \equiv x_0 + \frac{n}{d}k_2 \pmod{n}$$

$$\Rightarrow \frac{n}{d}(k_1 - k_2) \equiv 0 \pmod{n}$$

$$\therefore d \mid k_1 - k_2$$

$$\therefore k_1 \equiv k_2 \pmod{d}$$

$$k_1 \equiv k_2 \pmod{\gcd(a,n)}$$

∴ there are $\gcd(a,n)$ incongruent solution.

Example: $15x \equiv 20 \pmod{25}$

$\gcd(15, 25) = 5$

$5 \mid 20$, so there is a solution

and, there are 5 solution

these are separated by $\frac{25}{5} = 5$

$15x \equiv 20 \pmod{25}$

$\Rightarrow 3.5x \equiv 4.5 \pmod{25}$

$\Rightarrow 3x \equiv 4 \pmod{\frac{25}{\gcd(15,25)}}$

$\Rightarrow 3x \equiv 4 \pmod{5}$

$\boxed{x = 3}$

so, the solution will be

$x \equiv 3 \pmod{25}$

$x \equiv 8 \pmod{25}$

$x \equiv 13 \pmod{25}$

$x \equiv 18 \pmod{25}$

$x \equiv 23 \pmod{25}$

Strategy for solving $ax \equiv b \pmod{n}$

(i) a is invertible modulo n iff

$$\gcd(a,n) = 1$$

$$\Rightarrow ax + ny = 1$$

$$\therefore x = a^{-1}$$

$$ax = 1 \pmod{n}$$

(ii) $ca \equiv cb \pmod{n}$

$$\Leftrightarrow a \equiv b \left(\mod \frac{n}{\gcd(c,n)}\right)$$

(iii) $ax \equiv b \pmod{n}$ has a solution iff

$$\gcd(a,n) \mid b$$

(iv) if $ax \equiv b \pmod{n}$ has a solution then there are $\gcd(a,n)$ solution separated by $\frac{n}{\gcd(a,n)}$.

Ex:

$12x \equiv 16 \pmod{32}$

$\gcd(12, 32) = 4$

$4 \mid 16$, so there is a solution

there are 4 solution

separated $\frac{32}{4} = 8$.

$12x \equiv 16 \pmod{32}$

$\Rightarrow 4 \cdot 3x \equiv 4 \cdot 4 \pmod{32}$

$\Rightarrow 3x \equiv 4 \pmod{\frac{32}{4}}$

$\Rightarrow 3x \equiv 4 \pmod{8}$

$\therefore \boxed{x = 4}$

$\therefore$ solution, $x \equiv 4 \pmod{32}$

$x \equiv 12 \pmod{32}$

$x \equiv 16 \pmod{32}$

$x \equiv 24 \pmod{32}$

Inverse modulo n

When can we find $a, b \in \mathbb{Z}$, $ab \equiv 1 \pmod{n}$?

Example: $n = 9$, ~~0~~, 1, 2, ~~3~~, 4, 5, ~~6~~, 7, 8

$$1 \cdot 1 \equiv 1 \pmod 9$$

$$\Rightarrow 1^{-1} = 1 \pmod 9$$

$$2 \cdot 5 \equiv 1 \pmod 9$$

$$\therefore 2^{-1} \equiv 5 \pmod 9$$

$$5^{-1} \equiv 2 \pmod 9$$

$3x \not\equiv 1 \pmod 9$ for all x

$6x \not\equiv 1 \pmod 9$ for all x

$$8 \cdot 8 \equiv 1 \pmod 9$$

$$\therefore 8^{-1} = 8 \pmod 9$$

prop: $a \in \mathbb{Z}$ is invertible $(\bmod n)$ iff $\gcd(a,n) = 1$.

forward, a is invertible $(\bmod n)$

There is $b \in \mathbb{Z}$ such that

$$ab \equiv 1 \pmod n$$

$$\Rightarrow n \mid ab - 1$$

$$\Rightarrow ab - 1 = nk \quad \text{for } k \in \mathbb{Z}$$

$$\Rightarrow ab - nk = 1 \equiv 1 \gcd(a,n)$$

$$\therefore \gcd(a,n) \mid 1$$

$$\boxed{\therefore \gcd(a,n) = 1}$$

Backward, $\gcd(a,n) = 1$

so, $ax + ny = 1$

$$\Rightarrow ax = 1 - ny$$

$$\therefore ax = 1 \cdot ny$$

$$ax \equiv 1 \pmod n$$

Find all inverse pairs (mod 20) :

(element should be relatively prime to 20) $\{1, 3, 7, 9, 11, 13, 17, 19\}$

* $1^{-1} \equiv 1 \pmod{20}$
* $3.7 \equiv 1 \pmod{20}$

  $3^{-1} \equiv 7 \pmod{20}$

  $7^{-1} \equiv 3 \pmod{20}$
* $9.9 \equiv 1 \pmod{20}$

  $9^{-1} \equiv 9 \pmod{20}$
* $11.11 \equiv 1 \pmod{20}$

  $\therefore 11^{-1} \equiv 1 \pmod{20}$
* $13 \times 17 \equiv 1 \pmod{20}$

  $\therefore 13^{-1} \equiv 17 \pmod{20}$

  $17^{-1} \equiv 13 \pmod{20}$

* $19 \equiv -1 \pmod{20}$

  $19 \times 19 = (-1)^2 \equiv 1 \pmod{20}$

  $\therefore 19^{-1} = 19 \pmod{20}$

(*) Find $34^{-1} \pmod{143}$

Soln:

$\gcd(34, 143) = 1$

$\therefore 34x + 143y = 1$

$143 = 4 \times 34 + 7$

$34 = 4 \times 7 + 6$

$7 = 1 \times 6 + 1$

$7 = 143 - 4 \times 34$

$6 = 34 - 4 \cdot 7$

$= 34 - 4 \cdot (143 - 4 \cdot 34)$

$= 17 \times 34 - 4 \cdot 143$

$1 = 7 - 1 \times 6$

$1 = 143 - 4 \times 34 - 1 \cdot (17 \times 34 - 4 \cdot 143)$

$1 = 5 \cdot 143 - 21 \cdot 34$

$34(-21) = 1 - 5 \cdot 143$

$\therefore 34 \times (-21) \equiv 1 \pmod{143}$

$34^{-1} \equiv -21 \pmod{143}$

$\therefore 34^{-1} \equiv 122 \pmod{143}$

Chinese remainder theorem:

$$X \equiv 1 \pmod 3$$
$$X \equiv 2 \pmod 4$$
$$X \equiv 4 \pmod 5 \quad \text{solve } x = ?$$

Soln:

$$N = 3 \times 4 \times 5 = 60$$
$$N_1 = 4 \times 5 = 20$$
$$N_2 = 3 \times 5 = 15$$
$$N_3 = 3 \times 4 = 12$$

$N_1 X_1 \equiv 1 \pmod 3$

$\Rightarrow 20 X_1 \equiv 1 \pmod 3$

$N_2 X_2 \equiv 1 \pmod 4$

$\Rightarrow 15 X_2 \equiv 1 \pmod 4$

$N_3 X_3 \equiv 1 \pmod 5$

$\Rightarrow 12 X_3 \equiv 1 \pmod 5$

Now,

$20X_1 \equiv 1 \pmod 3$ $\quad 20 \equiv 2 \pmod 3$

$\Rightarrow 2X_1 \equiv 1 \pmod 3$

$X_1 = 2$

$X_1 \equiv 2 \pmod 3$

$15X_2 \equiv 1 \pmod 4$ $\quad 15 \equiv 3 \pmod 4$

$\Rightarrow 3X_2 \equiv 1 \pmod 4$

$X_2 = 3$

$X_2 \equiv 3 \pmod 4$

$12X_3 \equiv 1 \pmod 5$ $\quad 12 \equiv 2 \pmod 5$

$\Rightarrow 2X_3 \equiv 1 \pmod 5$

$X_3 = 3$

$X_3 \equiv 3 \pmod 5$

$X = X_1N_1b_1 + X_2N_2b_2 + X_3N_3b_3$

$= 2 \times 20 \times 1 + 3 \times 15 \times 2 + 3 \times 12 \times 4$

$= 214$

$214 \equiv 34 \pmod{60}$

$\therefore \quad x \equiv 34 \pmod{60}$

Solve $x \equiv 2 \pmod 4$

$x \equiv 1 \pmod 5$

$x \equiv 3 \pmod 9$

$x \equiv 7 \pmod{13}$

$N = 4 \times 5 \times 9 \times 13 = 2340$

$N_1 = 5 \times 9 \times 13 = 585$

$N_2 = 4 \times 9 \times 13 = 468$

$N_3 = 4 \times 5 \times 13 = 260$

$N_4 = 4 \times 5 \times 9 = 180$

$N_1 X_1 \equiv 1 \pmod 4$

$585 \equiv 1 \pmod 4$

$\Rightarrow 585 X_1 \equiv 1 \pmod 4$

$\therefore 1 X_1 \equiv 1 \pmod 4$

$\therefore X_1 \equiv 1 \pmod 4$

$N_2 X_2 \equiv 1 \pmod 5$. $468 \equiv 3 \pmod 5$.

$\Rightarrow 468 X_2 \equiv 1 \pmod 5$

$\Rightarrow 3 X_2 \equiv 1 \pmod 5$

$X_2 = 2$

$\therefore X_2 \equiv 2 \pmod 5$

$N_3 x_3 \equiv 1 \pmod 9$ $\quad 260 \equiv 8 \pmod 9$

$\Rightarrow 260 x_3 \equiv 1 \pmod 9$

$\Rightarrow 8 x_3 \equiv 1 \pmod 9$

$\boxed{x_3 = 8}$

$x_3 \equiv 8 \pmod 9$

$180 \equiv 11 \pmod{13}$

$N_4 x_4 \equiv 1 \pmod{13}$

$\Rightarrow 180 x_4 \equiv 1 \pmod{13}$

$\Rightarrow 11 x_4 \equiv 1 \pmod{13}$

$x_4 = 6$

$\therefore x_4 \equiv 6 \pmod{13}$

$X = x_1 N_1 b_1 + x_2 N_2 b_2 + x_3 N_3 b_3 + x_4 N_4 b_4$

$= 1 \times 585 \times 2 + 2 \times 468 \times 1 + 8 \times 260 \times 3 + 6 \times 180$

$= 15906$

$15906 \equiv 1866 \pmod{2340}$

$\therefore X \equiv 1866 \pmod{2340}$

Solve:

$$X \equiv 3 \pmod 5$$
$$X \equiv 2 \pmod 6$$
$$X \equiv 1 \pmod 7$$

$N = 5 \times 6 \times 7 = 210$

$N_1 = 6 \times 7 = 42$

$N_2 = 5 \times 7 = 35$

$N_3 = 5 \times 6 = 30$

$N_1 X_1 \equiv 1 \pmod 5$

$\Rightarrow 42 X_1 \equiv 1 \pmod 5$ $[42 \equiv 2 \pmod 5]$

$\Rightarrow 2 X_1 \equiv 1 \pmod 5$

$\boxed{X_1 = 3}$

$\therefore X_1 \equiv 3 \pmod 5$

$N_2 X_2 \equiv 1 \pmod 6$

$\Rightarrow 35 X_2 \equiv 1 \pmod 6$ $[35 \equiv 5 \pmod 6]$

$\Rightarrow 5 X_2 \equiv 1 \pmod 6$

$\therefore \boxed{X_2 = 5}$

$\therefore X_2 \equiv 5 \pmod 6$

$N_3 x_3 \equiv 1 \pmod 7$

$\Rightarrow 30 x_3 \equiv 1 \pmod 7$

$\Rightarrow 2 x_3 \equiv 1 \pmod 7$ [$30 \equiv 2 \pmod 7$.

$\boxed{x_3 = 4}$

$\therefore x_3 \equiv 4 \pmod 7$

$X = N_1 x_1 b_1 + N_2 x_2 b_2 + N_3 x_3 b_3$

$= 42 \times 3 \times 3 + 35 \times 5 \times 2 + 30 \times 4 \times 1$

$= 848$

$\therefore X \equiv 8 \pmod{210}$

Fermat's Little Theorem

If gcd $(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$

proof:

consider, $S = \{a, 2a, 3a, \ldots\ldots (p-1)a\}$

Claim: All element of S are incongruent mod p.

In other words,

their residue mod p

for the set, $S' = \{1, 2, 3 \ldots\ldots p-1\}$

Take, $ka, la \in S$ $\quad \boxed{1 \le k \ne l \le p}$

suppose:

$$ka \equiv la \pmod{p}$$

$$p \mid (k-l)a$$

$p \nmid a \rightarrow$ because gcd $(a, p) = 1$

$p \nmid k-l \rightarrow$ because $1 \le k \ne l \le p$

So, $a.2a.3a \cdots\cdots (p-1)a \equiv (p-1)a! \pmod{p}$

$\Rightarrow a^{p-1}.(p-1)! \equiv (p-1)! \pmod{p}$

$\Rightarrow -a^{p-1} \equiv -1 \pmod{p}$ [wilson theo

$\therefore \boxed{a^{p-1} \equiv 1 \pmod{p}}$

Wilson Theorem

If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$

Lemma: If $a^2 \equiv 1 \pmod{p}$ then

$a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$

Proof:

suppose that, $a^2 \equiv 1 \pmod{p}$

$\Rightarrow p \mid a^2 - 1$

$\Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow p \mid a-1$ or $p \mid a+1$

$\Rightarrow a \equiv 1 \pmod{p}$ or $a \equiv 1 \pmod{p}$

In particular, the only integers who are their own inverses $\pmod{p}$ are $\pm 1 \pmod{p}$

proof:

consider,

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots\cdots (p-2)(p-1) \pmod p$$

* Every numbers between $2, \cdots\cdots, p-2$ has a unique inverse not equal to itself.

pair each inverse pair together,

$$(p-1)! = 1 \cdot (2 \cdot 2^{-1} \cdot 3 \cdot 3^{-1} \cdots\cdots (p-2) \cdot (p-2)^{-1}) \cdot (p-1) \cdot \pmod p$$

$$= (p-1) \pmod p$$

$$= -1 \pmod p$$

$$\therefore \boxed{(p-1)! \equiv -1 \pmod p}$$

Example: $X = 17! \pmod{19}$

Soln

$18! \equiv -1 \pmod{19}$ → we know

$18X \equiv 18! \pmod{19}$.

$\Rightarrow (-1)X \equiv -1 \pmod{19}$

$\Rightarrow X \equiv 1 \pmod{19}$

$\therefore 17! \equiv 1 \pmod{19}$

Ex: $5^{3571} \pmod{11}$

write,

$3571 = 357.10 + 1$

$5^{3571} = 5^{375.10+1}$

$= (5^{10})^{375} * 5^1$

$= 1 \cdot 5$

$= 5 \pmod{11}$

$a^{p-1} \equiv 1 \pmod{p}$

$\therefore 5^{10} \equiv 1 \pmod{11}$

Ex: $4^{100,000} \pmod{19}$

$a^{p-1} \equiv 1 \pmod{p}$

$4^{18} \equiv 1 \pmod{19}$

$100,000 = 5555 \cdot 18 + 10$

$4^{100,000} = 4^{5555 \cdot 18 + 10}$

$= (4^{18})^{5555} \cdot 4^{10}$

$= (1)^{5555} \cdot 4^{10}$

$= 4^{10} \pmod{19}$

$= 4^{8} \cdot 4^{2} \pmod{19}$

$= 5 \times -3 \pmod{19}$

$= -15 \pmod{19}$

$= 4 \pmod{19}$

$4^1 \equiv 4 \pmod{19}$

$4^2 \equiv 16 \pmod{19}$

$\equiv -3 \pmod{19}$

$4^4 \equiv 9 \pmod{19}$

$4^8 \equiv 81 \pmod{19}$

$\equiv 5 \pmod{19}$

Wilson theorem:

$$(p-1)! \equiv -1 \pmod{p}$$

(*) $(p-2)! \equiv 1 \pmod{p}$

proof, we know, $(p-1)! \equiv -1 \pmod{p}$

$$\Rightarrow (p-1)(p-2)! \equiv (p-1) \pmod{p}$$

$$\therefore (p-2)! \equiv 1 \pmod{p}$$

$$\therefore \boxed{(p-2)! \equiv 1 \pmod{p}}$$

Ex: $66 \cdot 67 \cdot 68 \cdots 77$ reduce all mod 13

$\therefore 66 \cdot 67 \cdot 68 \cdots 77$

$\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdots 12 \pmod{13}$

$\equiv (13-1)! \pmod{13}$

$\equiv -1 \pmod{13}$

$\equiv 12 \pmod{13}$

Ex: $134 \cdot 135 \cdots 149$ reduce all mod 19

$X = 134 \cdot 135 \cdots 149$

$X \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdots 16 \pmod{19}$

$\Rightarrow X \equiv 16! \pmod{19}$

$\Rightarrow 17X \equiv 17! \pmod{19}$

$\Rightarrow 17X \equiv (19-2)! \pmod{19}$

$\therefore 17X \equiv 1 \pmod{19}$

$\therefore X \equiv 9 \pmod{19}$

$17 \times 9 \equiv 1 \pmod{9}$

$\therefore 17^{-1} \equiv 9 \pmod{9}$