Number Theory

Friday, September 29, 2023 4:18 PM

1] Division algorithm

We divide a by $n > 0$, we get two unique integers: q and r such that

$$a = q \cdot n + r \quad ; \quad 0 \leq r < n$$

e.g. $17 \div 5$,

$$17 = \underline{3} \cdot 5 + \underline{2}$$

mod

$-11 \div 3$,

$$-11 = (\underline{-4}) \cdot 3 + \underline{1}$$

2] $n \mid a$ means $\exists q$, $a = q \cdot n$; $a, q, n \in \mathbb{Z}$, $n \neq 1$

e.g. $3 \nmid 17$ for $17 = \underline{5} \cdot 3 + \underline{2}$

$3 \mid 18$ for $q = 6$, $18 = q \cdot (3)$

$-3 \mid 6$ for $q = -2$

3] Prime,

$p > 1$ is prime if it has exactly 2 positive divisors : 1 and p.

$n > 1$ is composite if it is not prime.

4] gcd (a, b)

5] EA : $\gcd(a,b) = \gcd(b, a \bmod b)$

6] E.E.A : $\exists s,t$, $\gcd(a,b) = s.a + t.b$

7) Modular arithmetic :

① $a \equiv b \pmod n \iff n \mid (a-b)$

$\iff a \bmod n = b \bmod n$

② $a \pm b \pmod n \equiv (a \bmod n \pm b \bmod n) \bmod n$

$a \times b \pmod n \equiv (a \bmod n) \times (b \bmod n) \pmod n$

Exer $222 \times 3499 \pmod 5$

$2 \times 4 \equiv 8 \equiv 3 \pmod 5$

$220 \times 3498 \pmod 7$

$210 + 7 + 3 \times 3500 - 2$

$3 \times (-2) \equiv -6 \equiv 1$

8] Divisible by 3 or 9 (add the digits)

$4527 = 4 \times 10^3 + 5 \times 10^2 + 2 \times 10^1 + 7$

$\equiv 4 \times 1^3 + 5 \times 1^2 + 2 \times 1^1 + 7 \pmod 3$

$\pmod 9$

by 11 : alternate +/- right -to- left

$4527 = 4 \times 10^3 + 5 \times 10^2 + 2 \times 10^1 + 7$

$\leftarrow + - +$

$6 \equiv 4 \times (-1)^3 + 5 \times (-1)^2 + 2 \times (-1) + 7 \pmod{11}$

$+ \; - \; +$

$$6 \equiv 4 \times (-1)^3 + 5 \times (-1)^2 + 2 \times (-1) + 7 \pmod{11}$$

$$\equiv -4 + 5 - 2 + 7$$

Exer 1)

5960

$-2 \equiv 9$

$+ \; - \; +$

505505371

565①8484 (mod 11)

$(-4)+(-8)$

$-1 = 0$

Exer: ②

$50^{97} \pmod 7$

!

$50 \equiv 1 \pmod 7$

Exer ③

$565①8484 \equiv 5$

9] Fermat Little Theorem

if p is prime then

$\forall a \in \mathbb{Z}_p^*$

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

eg.

$2^{77} \pmod 7$

$\equiv (2^6)^{12} \cdot 2^5$

12

$\equiv 1 \cdot 32 \equiv 4 \pmod 7$

Exer: $5656^{135} \pmod{11}$

(mod 11) (mod 10)

$2^5 \equiv 32 \equiv 10 \pmod{11}$

10] Groups

$(A, *)$ is a group if

① Closure : A is closed under $*$
② assoc. : $(a * b) * c = a * (b * c)$
③ identity : $\exists\, e \in A,\ \forall a \in A,\ a * e = e * a = a$
④ inverse : $\exists a \in A,\ \exists\, a^{-1},\ a^{-1} * a = a * a^{-1} = e$

e.g.

$(\mathbb{Z}_5, +)$ is the additive group modulo - 5

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

identity: 0

inverse:

x	0	1	2	3	4
$-x$	0	4	3	2	1

e.g.

$(\mathbb{Z}_5^*, +)$ is the multiplicative group modulo - 5

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$\mathbb{Z}_n^* = \{x \mid 0 \le x < n,\ \gcd(x, n) = 1\}$

$\mathbb{Z}_1^* = \{0\}$

$\mathbb{Z}_2^* = \{1\}$

identity: 1

inverse:

x	1	2	3	4
x^{-1}	1	3	2	4

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

Inverse

x	1	3	7	9
x^{-1}	1	7	3	9

11] Group order : is the number of elements in the group.

$|G|$

e.g. $|\mathbb{Z}_5| = |\{0, 1, 2, 3, 4\}| = 5$

$|\mathbb{Z}_{10}^*| = 4$

12] The order of $a \in G$.

$\text{ord}(a)$ = the smallest $k \geq 1$, s.t.

$a^k = e$

e.g. $|\mathbb{Z}_{15}^*| = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$

$\text{ord}(4)$? $4^1 = 4$

$4^2 = 1 \Rightarrow \text{ord}(4) = 2$

$\text{ord}(2) = 4$. $2^1, 2^2, 2^3, 2^4 = 1$

13] Euler Phi function

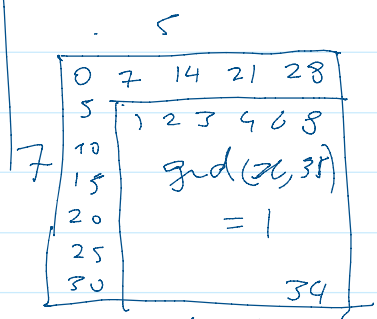
$\phi(n) = |\mathbb{Z}_n^*|$

e.g. $\phi(15) = 8$

$\phi(35) = (5-1)(7-1) = 24$ | $35 = 5 \times 7$

$$\phi(35) = (5-1)(7-1) = 24$$

$35 = 5 \times 7$



Alg: $\phi(n)$

① $\phi(1) = 1$

② $\phi(p^k) = (p-1)\,p^{k-1}$

③ $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m) = 1$

e.g. $\phi(35) = \phi(5) \cdot \phi(7)$

$= 4 \cdot 6 = 24$

e.g. $\phi(100) = \phi(2^2 \cdot 5^2)$

$= \phi(2^2) \cdot \phi(5^2)$

$= (2-1)(2^1) \cdot (5-1)(5^1)$

$= 2 \cdot 20$

$= 40$

14] Euler Theorem

Let $a \in G$, and $|G| = n$, then

$$a^n = e$$

In $\mathbb{Z}_n^*$, $a^{\phi(n)} \equiv 1 \pmod n$

e.g.

$13^{82} \pmod{15}$

mod $\phi(15)$

$\phi(15) = \phi(3 \cdot 5) = 2 \cdot 4$

$(-2)^2 \equiv 4 \pmod{15}$

mod 15 ↓ mod $\phi(15)$

$\phi(15) = \phi(3 \cdot 5) = 2 \cdot 4 = 8$

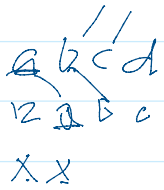
Review :

if one letter is changed in P, then how many letters will change in C? using.

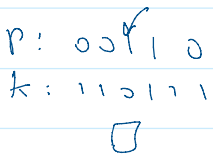
① Enigma : one letter

② Vigenere : one

③ Auto-key. 2



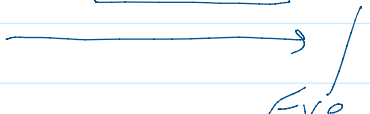
④ OT pad : one



14.

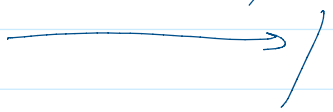
encrypt — comp.

① Zip (E (file))



Comp — encrypt

② E (zip(file))



more secure
more efficient.

11.

#11.

a) 4950

$$\sum_{i=1}^{99} i = \frac{(99+1)}{2} \times 99$$

b) 100 / or 99

c) 100 or 99