Prime no. → Has exactly two divisors

- If N is prime, then the divisors are 1 & N
- All no have prime factors

Numbers	10	11	100	37		
Prime factorization	$2^1 \times 5^1$	$1^1 \times 11^1$	$2^2 \times 5^2$	$1^1 \times 37^1$		
Prime No.	2, 5	1, 11	2, 5	1, 37		

- 10 is not a prime no but it have prime factors
- A prime no. is a no. greater than 1 and its only two factors itself and one. It can't be divided by any other no. without leaving a remainder.
- 2, 3, 5, 7 are prime no.
- 9 is not a prime but a composite no.

Facts about prime no →

- only even prime 2.
- Smallest prime no 2
- Is 1 a prime no? → No
- Except for 2 and 5, all prime no. ends in digit 1, 3, 7, 9

Prime no. in cryptography →

- Many encryption algo are based on prime no.
- Very fast to multiply two large prime no.
- Extremely computers & intensive to do the reverse.
- Factoring very large prime no. is very hard i.e. like computers a long time

Prime no. ⇒ Has exactly two divisors

- if N is prime, then the divisors are 1 and N
- All no have prime factors.

Numbers	10	11	100	37	308	14688
Prime factorization	$2^1 \times 5^1$	$1^1 \times 11^1$	$2^2 \times 5^2$	$1^1 \times 37^1$	$2^2 \times 7^1 \times 11^1$	$2^5 \times 3^3 \times 17^1$
Prime No.	2, 5	1, 11	2, 5	1, 37	2, 7, 11	2, 5, 17

- 10 is not a prime no. but it have prime factors 2 & 5 and divisible by
- A prime no. is a no. greater than 1, with only two factors itself and one. It can't be divided further by any other no. without leaving a remainder.
- 2, 3, 5, 7 are prime no.
- 9 is not a prime but a composite no.

Facts about prime no. ⇒

- ✱ only even prime = 2
- Smallest prime no = 2
- ✱ Is 1 a prime no.? ⇒ No
- Except for 2 and 5, all prime no. ends in digit 1, 3, 7, 9.

Prime no. in cryptography ⇒

- Many encryption algo. are based on prime no.
- very fast to multiply two large prime no.
- Extremely computer intensive to do the reverse.
- factoring very large prime no. is very hard it take computers a long time.

Primality testing :-

Fermat's primality Test : whether a given no. is prime or not.

Q. Is 'p' prime?

Test

a^p - a → 'p' is prime if this is a multiple of p, for any a

1 < a < p

Q.Eg. Is 5 prime?

p = 5 a ∈ 1, 2, 3, 4 < 5

we start from a = 1

a 1^5 - 1 → '0' → is 0, is a multiple of 5 (note 0 is multiple of any no.)

2^5 - 2 → '30' → 30 is

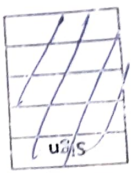
3^5 - 3 → '240' → 240 is

4^5 - 4 → 1020 . 1020 a multiple of 5

So the 5 is a prime no.

Drawback : If no. is big then it will be very time consuming. for eg. p = 3753

a : 1 to 3752



. Miller-Rabin Primality test :

Algorithm : whether n is prime or not.

step 1 find $n-1 = 2^k * m$

step 2 choose 'a' such that $1 < a < n-1$

step 3 Compute $b_0 = a^m \pmod n$, ..., $b_i = b_{i-1}^2 \pmod n$

if b_0 : +1 → Composite no.

-1 → probably prime

if none of the above Compute none b_i

Continue calculating b_i's of until the result is either
+1 or -1.

Eg. Is 561 prime?

Given $n = 561$

Step 1: $n-1 = 2^k * m$

$560 = 2^4 \times 35$

$k = 4$, $m = 35$

Step 2: choosing $a = 2$; $1 < a < 560$

Step 3: $b_0 = a^m \pmod n$

$= 2^{35} \pmod{561}$

$= 263$

$\frac{560}{2^1} = 280$ | $\frac{560}{2^2} = 140$ | $\frac{560}{2^3} = 70$ | $\frac{560}{2^4} = 35$

they are not integers so keep on proceeding until a decimal no comes

$\frac{560}{2^5} = 17.5$

modular exponentiation

So Calculate b_1

$b_1 = b_0^2 \pmod n$

$= 262^2 \pmod{561}$

$= 166$

$b_2 = (166)^2 \pmod n$

$= 67$

$b_3 = (67)^2 \bmod n$

$b_3 = +1 \rightarrow$ composite no.

The fermat's primality test given result for the 561 as prime no.

Modular Arithmetic

In cryptography, congruence ($\equiv$) instead of equality ($=$)

Eg.

15 $\equiv$ 3 mod 12

15 mod 12 = 3

3 mod 12 = 3

$$12 \overline{)15} \quad 1, \quad 15 - 12 = 3$$

23 $\equiv$ 11 mod 12

23 is congruent to 11 mod 12

$$12 \overline{)23} \quad 1, \quad 23 - 12 = 11$$

33 $\equiv$ 3 mod 10

$$10 \overline{)33} \quad 33 - 30 = 3$$

10 $\equiv$ -2 mod 12

when have -ve no. add there two.

$$12 \overline{)10} \quad 10 - 0 = 10, \quad 10 - 12 = -2$$

$\therefore$ $a = b \bmod m$

when a is divided by m we get the remainder b

$$a = mk + b$$

Or

$$a = mq + b$$

why Congruence rather than equality ?

33 = 3 mod 10

23 = 3 mod 10

} both are same

Valid or invalid

* $38 \equiv 2 \pmod{12}$ ✓ (12×3 remainder 2)
* $38 \equiv 14 \pmod{12}$ ✓ (12×2 remainder 14)
* $5 \equiv 0 \pmod{5}$ ✓
* $10 \equiv 2 \pmod{6}$ ✗ invalid
* $2 \equiv -3 \pmod{5}$ ✓

Analogy

circumference 10

thread

No of (Quotient) wraps	Remaining thread (Remainder	Cong
1	25	$35 \equiv 25$
2	15	$35 \equiv 15$
3	5	$35 \equiv 5$

Properties of modular arithmetic →

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

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

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

Property	Expression
Commutative laws	$(a+b) \bmod n = (b+a) \bmod n$ $(a+b) \bmod n = (b*a) \bmod n$
Associative laws	$[(a+b)+c] \bmod n = [a+(b+c)] \bmod n$ $[(a*b)*c] \bmod n = [a*(b*c)] \bmod n$
Distributive laws	$[a*(b+c)] \bmod n = [(a*b)+(a*c)] \bmod n$
Identities	$(0+a) \bmod n = a \bmod n$ $(1*a) \bmod n = a \bmod n$
Additive Inverse $(-w)$	for each $w \in Z_n$, there exist a z such that $w+z = 0 \bmod n$

Modular Exponentiation:-

It is a type of exponentiation performed over a modulus.

$a^b \bmod m$ or $a^b \pmod m$

Eg $23^3 \bmod 30$

$23^3 \bmod 30 \equiv -7^3 \bmod 30$ (i.e $23 \div 30$) remainder will be -7

$= -7^2 * -7 \bmod 30$

$= 49 * -7 \bmod 30$

$= -133 \bmod 30$

$= -13 \bmod 30$

$= -13 + 30$

$= 17$ – is the answer

Eg. 2

Solve $31^{500} \bmod 30$

$31^{500} \bmod 30 \equiv 1^{500} \bmod 30$

$= 1 \bmod 30$

$= 1$

$31 / 30$ remainder is 1

Eg. 3 $242^{329} \bmod 243$

$242^{329} \bmod 243 \equiv -1^{329} \bmod 243$ $\quad -1$

(-1) power odd no.

$= -1 + 243$

$= 242$

Eg. 4 $11^7 \bmod 13$

$= 11 \bmod 13 \times 11 \bmod 13 \times \ldots$ 7 times

$= -2 \times -2 \times -2 \times -2 \times -2 \times -2 \times -2 \bmod 13$

$= -128 \bmod 13$

$= -11 \bmod 13$

$= -11 + 13$

$= 2$

Euclidean algorithm for finding GCD (Greatest common division) →

GCD or HCF (Highest common factor)

GCD of 12 & 33

~~Divisors~~	12	33
~~Common~~ divisor	1, 2, 3, 4, 6, 12	1, 3, 11, 33
~~Max~~ Division	1, 3	
GCD	3	

Euclid's or Euclidian algorithm for finding GCD

(1) Find the GCD (12, 33), biggest no. as A other as B

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

Remainders

$12 \overline{)33}\ 2,\ 24,\ 9$

$9 \overline{)12}\ 1,\ 9,\ 3$

$3 \overline{)9}\ 3,\ 9,\ 0$

Whenever B becomes 0, that time whatever is in A is the GCD.

3 is the GCD by using Euclid's algorithm.

```
EUCLID(a, b)
1. A ← a ; B ← b
2. if B = 0 return A = gcd(a, b)
3.    R = A mod B
4.    A ← B
5.    B ← R
6.    goto 2
```

Multiplicative inverses

$5 \times \frac{1}{5} = 1$

multiplicative inverse of 5 is $\frac{1}{5}$

$A \times A^{-1} = 1$

$6 \times \frac{1}{6} = 1$

what about multiplicative inverse of mod n?

A no. like a when multiplied by b and result is divided by n should have the remainder 1.

then b, is the multiplicative inverse of a.

for eg. $3 \times ? = 1 \bmod 5$

remainder

$3 \times 1 = 3 \bmod 5$

$3 \times 2 = 1 \bmod 5$

$6 \bmod 5 = 1$

so multiplicative inverse of 3 is 2.

** multiplicative inverse exist to two values if they are relatively prime to each other
eg. 3 mod 5, 3 & 5 are relatively prime beg they gcd other common divisor is 1

Extended Euclidean algorithm for multiplicative inverse

Points to remember

A > B

$B \overline{)\, A}^{\,Q}$

R

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
x	1	0	x	2	-5	x

$T_1 = 0$, $T_2 = 1$

$T = T_1 - T_2 \times Q$

Solving for 3 mod