UNIT-3

Number theory & cryptography

Number Theory:- Number theory provides the mathematical foundation for many cryptographic algorithms. Its concepts, such as modular arithmetic Prime numbers and discrete logarithms are crucial for ensuring data security. Divisibility and the division algorithm

Divisibility

b divides a if there is no remainder on division.

The notation $b|a$ is commonly used to mean b divides a. Also if $b|a$ we say that b is a divisor of a.

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24.

$13|182, -5|30, -3|33, 17|0$

Simple properties.

① If $a|1$ then $a = \pm 1$

② If $a|b$ and $b|a$ then $a = \pm b$

③ Any $b \neq 0$ divides 0

④ If $a|b$ and $b|c$ then $a|c$.

eg $11|66$ and $66|198 \Rightarrow 11|198$

⑤ If $b|g$ and $b|h$ then $b|(mg+nh)$ for arbitrary integers m and n.

⑥ If $b|g$ then g is of the form $g = b \times g_1$ for some integer g_1.

⑦ If $b|h$ then h is of the form $h = b \times h_1$ for some integer h_1.

So $mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1)$

and therefore b divides $mg + nh$.

$b = 7, g = 14, h = 63, m = 3, n = 2$

$7|14$ and $7|63$

To show $7|(3 \times 14 + 2 \times 63)$

we have $(3 \times 14 + 2 \times 63) = 7(3 \times 2 + 2 \times 9)$

and it obvious that $7|(7(3 \times 2 + 2 \times 9))$.

Name : Semester / Section : Branch :

Roll No. : Subject : Invigilator Signature with Date :

The division Algorithm

Given any positive integer n and any non negative integer a, if we divide a by n we get an integer quotient q and an integer remainder r that obey the following relationship

$$a = qn + r \qquad 0 \leq r < n$$

$$q = \lfloor a/n \rfloor$$

q = quotient

n = divisor

r = reminder.

eg 1

$a = 11 \quad n = 7$

$11 = 1 \times 7 + 4$

$r = 4$

$q = 1$

eg 2

$a = -11, \quad n = 7$

$-11 = (-2) \times 7 + 3$

$-11 = -14 + 3$

$r = 3$

$q = -2$

$$q = \left\lfloor \frac{a}{n} \right\rfloor$$

$$q = \left\lfloor \frac{-11}{7} \right\rfloor \approx -1.571$$

$$q = -2$$

The Euclidean Algorithm

→ one of the basic techniques of number theory is the Euclidean algorithm

→ simple procedure for determining the greatest common divisor for two positive integers.

→ Two integers are relatively prime if and only if their only common positive integer factor is 1.

Greatest common divisor

gcd (a, b).

the greatest common divisor of a, b is the largest integer that divides both a and b.

eg ⇒ gcd (a, b) = c

1. c is a divisor of 'a' and 'b'.
2. Any divisor of 'a' and 'b' is a divisor of c.

Understanding GCD

Example

gcd (60, 36)

	60	36
Divisors	1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60	1, 2, 3, 4, 6, 9, 12, 18, 36
Common divisors	1, 2, 3, 4, 6, 12	
GCD	12	

GITAM

(Deemed to be University)

HYDERABAD - 502 329

Name : Semester / Section : Branch :

Roll No. : Subject : Invigilator Signature with Date :

1. Find the GCD of 48 and 18 using the euclidean algorithm.

Step 1 gcd (48, 18)

$a = 48 \quad b = 18$

$a = bq + r$

$48 = 2 \times 18 + 12$

$18 \overline{)48}$ quotient 2, 36, remainder 12

Step 2

$a = 18 \quad b = 12$

$a = bq + r$

$18 = 12 \times 1 + 6$

$12 \overline{)18}$ quotient 1, 12, remainder 6

Step 3

$a = 12 \quad b = 6$

$a = bq + r$

$12 = 2 \times 6 + 0$

$6 \overline{)12}$ quotient 2, 12, remainder 0

$\boxed{\gcd(48, 18) = 6.}$

2. gcd (56, 98)
3. gcd (81, 153)
4. gcd (101, 103)
5. gcd (12345, 54321)

gcd (12345, 54321)

Step 1

$a = 54321 \quad b = 12345$

$a = bq + r$

$54321 = 12345 \times 4 + 4941$

$$\begin{array}{r} 4 \\ 12345 \overline{)\,54321} \\ 49380 \\ \hline 4941 \end{array}$$

Step 2

$a = 12345 \quad b = 4941$

$a = 4941 \times 2 + 2463$

$12345 = 4941 \times 2 + 2463$

$$\begin{array}{r} 2 \\ 4941 \overline{)\,12345} \\ 9882 \\ \hline 2463 \end{array}$$

Step 3

$a = 4941 \quad b = 2463$

$4941 = 2463 \times 2 + 15$

$$\begin{array}{r} 2 \\ 2463 \overline{)\,4941} \\ 4926 \end{array}$$

Step 4

$a = 2463 \quad b = 15$

$2463 = 15 \times 164 + 3$

$$\begin{array}{r} 164 \\ 15 \overline{)\,2463} \\ 2460 \\ \hline 3 \end{array}$$

Step 5

$a = 15 \quad b = 3$

$15 = 3 \times 5 + 0$

When the remainder becomes 0 the divisor at that step (15) is the GCD

GCD (54321, 12345) = 3.

Algorithm:-

Step 1: Start with two numbers

let a and b

if $a < b$, swap them $a \geq b \geq 0$.

Step 2: use division to find the reminder

Divide a by b using division algorithm

$$a = b \cdot q + r$$

q = quotient

r = reminder

Step 3: Replace and repeat

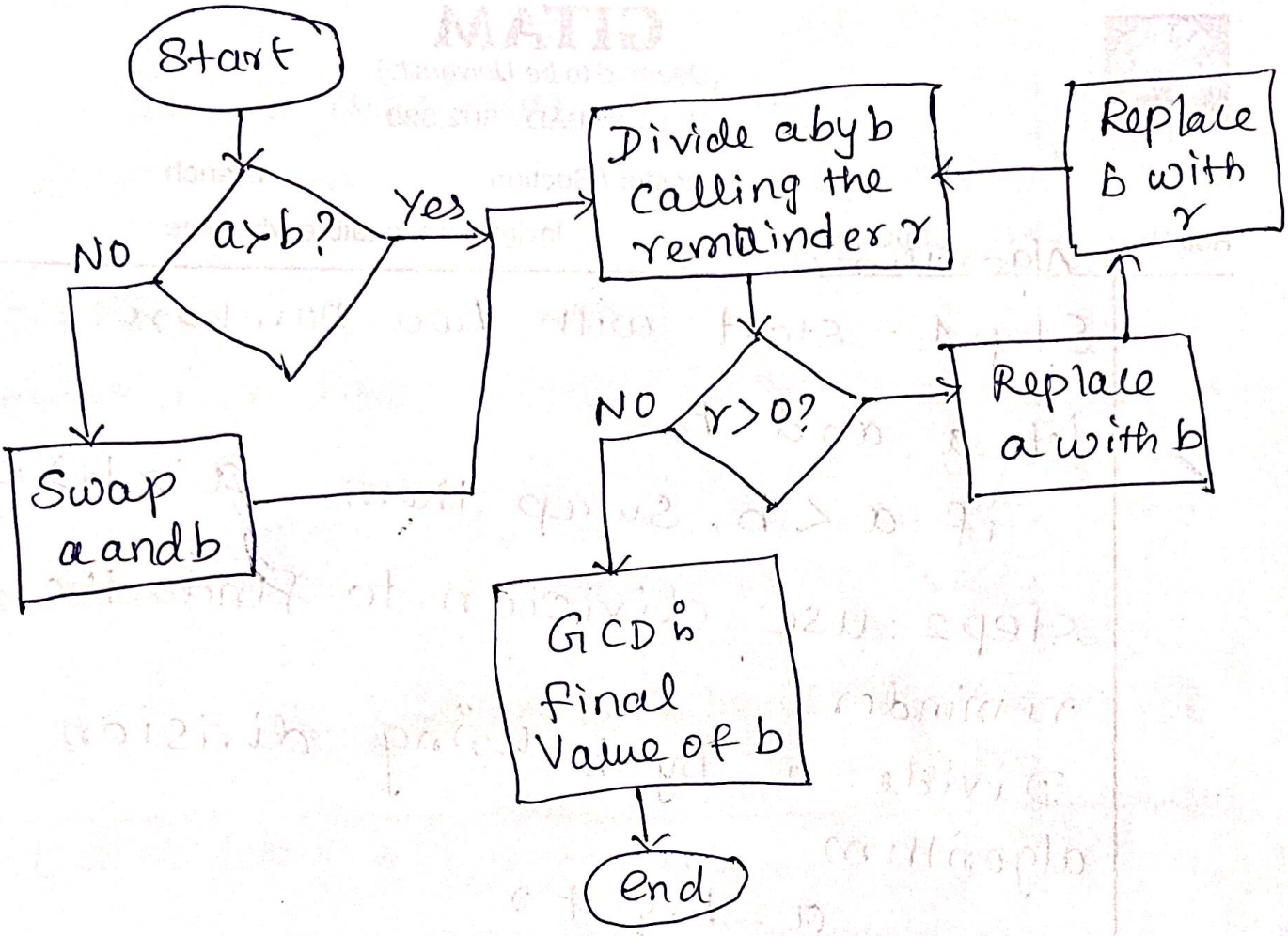
Replace a with b

Replace b with r

Repeat the process until the reminder (r) becomes 0.

Step 4: Stop when the remainder is 0

When $r = 0$, the GCD is the Last non-zero remainder



Modular Arithmetic

If a is an integer and n is a positive integer we define a mod n to be the remainder when a is divided by n. The integer n is called the modulus.

eg $45 \bmod 20 = 5$

$11 \bmod 3 = 2$

$11 \bmod 40 = 11$

$11 \bmod 11 = 0$

$$20\overline{)45}\ 2,\ 40,\ 5$$

$$3\overline{)11}\ 3,\ 9,\ 2$$

Properties of modular Arithmetic for Integers in Z_n

	Property	
1.	Commutative Laws	$(w+x) \bmod n = (x+w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
2.	Associative Law	$[(w+x)+y] \bmod n = [w+(x+y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
3.	Distributive Law	$[w \times (x+y)] \bmod n = [(w \times x)+(w \times y)] \bmod n$
4	Identities	$(0+w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
5.	Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w+z \equiv 0 \bmod n$.

eg

Apply $a = 11$, $n = 8$, $b = 15$

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

RHS

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8$

$[3 + 7] \bmod 8 = 10 \bmod 8 = 2$

LHS

$(a+b) \bmod n$

$(11+15) \bmod 8 = 2$

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

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

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8$

$[3 - 7] \bmod 8 = -4 \bmod 8 = 4$

$(a-b) \bmod n$

$(11-15) \bmod 8$

$-4 \bmod 8 = 4$

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

Properties of modular Arithmetic for Integers in Z_n

	Property	
1.	Commutative Laws	$(w+x) \bmod n = (x+w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
2.	Associative Law	$[(w+x)+y] \bmod n = [w+(x+y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
3.	Distributive Law	$[w \times (x+y)] \bmod n = [(w \times x)+(w \times y)] \bmod n$
4	Identities	$(0+w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
5.	Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w+z \equiv 0 \bmod n$.

Mod of Negative numbers

$$-a \bmod n = n - (a \bmod n)$$

eg $-11 \bmod 3$

$a = -11 \quad b = 3$

$$-11 \bmod 3 = 3 - (11 \bmod 3)$$
$$= 3 - 2 = 1$$

eg $$-11 \bmod 40 = 40 - (11 \bmod 40)$$
$$= 40 - 11 = 29$$

eg $$-11 \bmod 5 = 5 - (11 \bmod 5)$$
$$= 5 - 1$$
$$= 4.$$

$a = qn + r \quad r \leq r \leq n ; \quad q = \lfloor a/n \rfloor$

$$a = [a/n] \times n + (a \bmod n)$$

Congruent modulo :-

Two integers a and b are said to be congruent modulo n.

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

then $a \equiv b \pmod n$

$a = 6, n = 10.$

eg $73 \bmod 23 = 4$

$4 \bmod 23 = 4$

$a \equiv b \bmod n$

$73 \equiv 4 \bmod 23$

$73 \bmod 23 \equiv 4$

a is congruent to b with respect to n

Properties of congruences

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

eg $73 \bmod 23$

$4 \bmod 23$

if $23 \mid (73-4) = \frac{69}{23}$

2. $a \equiv b \pmod n$ implies $b \equiv a \pmod n$

eg $73 \equiv 4 \bmod 23$

$4 \equiv 73 \bmod 23$

3. $a \equiv b \pmod n$ and $b \equiv c \pmod n$ that imply $a \equiv c \pmod n$

Modular arithmetic exhibits the following properties

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

$a = 6, n = 10.$

Name : Semester / Section : Branch :

Roll No. : Subject : Invigilator Signature with Date :

Exponentiation

To find $11^7 \bmod 13$

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

$11^1 \bmod 13 = 11$

$11^2 \bmod 13 = 11^1 \times 11^1 \bmod 13$

$= 11 \times 11 \bmod 13$

$= 121 \bmod 13 = 4$

$11^4 \bmod 13 = 11^2 \times 11^2 \bmod 13$

$= 4 \times 4 \bmod 13$

$= 3$

$11^7 \bmod 13 = 3 \times 4 \times 11 \bmod 13$

$= 132 \bmod 13$

$= 2$

$\boxed{11^7 \bmod 13 = 2}$

Prime numbers :-

→ if 'N' is prime then the divisors are 1 and N.

→ All numbers have prime factors.

eg Number = 10

Prime factorization $= 2^1 \times 5^1$

prime numbers = 2, 5

Any integer $a > 1$ can be factored in a unique way as

$$a = P_1^{a_1} \times P_2^{a_2} \times \dots P_t^{at}$$

where $P_1 < P_2 < \dots < P_t$ are prime numbers and a_i is positive integer. This is known as the fundamental theorem of arithmetic

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

$91 = 7^1 \times 31^1$

eg Multiplication of two numbers is equivalent to adding the corresponding exponents

$K = 12 \times 18$

$= (2^2 \times 3) \times (2 \times 3^2)$

$= 216$

$K_2 = 2+1 = 3$

$K_3 = 1+2 = 3$

$\therefore 216 = 2^3 + 3^3$

$a = 3, n = 10.$

GCD of two positive integers can be determined easily if we express each integer as the product of primes.

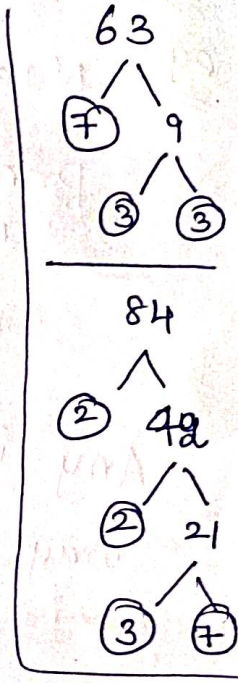
GCD using prime factorization

eg GCD (63, 84)

$63 = 3 \times 3 \times 7 \Rightarrow 3 \times 7 = 21$

$84 = 2 \times 2 \times 3 \times 7$

$\boxed{GCD(63, 84) = 21}$



Fermat's and Euler's theorems.

Fermat's theorem

Two theorems that play important roles in Public-key cryptography.

Fermat's theorem states

If p is prime and a is a positive integer not divisible by p then

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

(or)

$$\frac{a^p}{a} \equiv 1 \bmod p \Rightarrow \boxed{a^p \equiv a \bmod p}$$

$a = 5,\ P = 19$

eg 1

$5^{18} \bmod 19$

$a^{P-1} \equiv 1 \bmod P$

$5^{19-1} \bmod 19 = 1$

$5^{18} \bmod 19 = 1$

$a \equiv b \pmod n$

$\frac{a}{n} = b$ (remin

$a^P \equiv a \pmod P = a$

$a^{P-1} \equiv 1 \pmod P = 1$

eg 2

$5^{19} \bmod 19$

$a^P \equiv a \pmod P$

$5^{19} \bmod 19 = 5$

eg 3

$5^{20} \bmod 19$

$5^{19 \times 1 + 1} \bmod 19 \Rightarrow 5^{19} \cdot 5^1 \bmod 19$

$5^{19} \bmod 19 \cdot 5^1 \bmod 19$

$5 \times 5 = 25$

$5^{20} \bmod 19 = 25$

$25 \bmod 19 = 6$

$5^{20} \bmod 19 = 6$

eg 4 $P = 7$ and $a = 3$ verify Fermat's theorem by proving that $3^6 \equiv 1 \pmod 7$

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

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

$3^6 \equiv 1 \pmod 7 = 1$

$a = 3,\ n = 10.$

eg x^{86} congruent to 6 mod 29

$x^{86} \equiv 6 \mod 29$

$a \equiv b \mod n$

$a \bmod n = b \bmod n$

$x^{29 \times 2 + 28} \mod 29 = 6$

$(x^2)^{29} \cdot x^{28} \mod 29$

$a = x^2 \quad b = 29$

$x^2, x^{28} \mod 29$

$x^{30} \mod 29$

$x^{29} \cdot x^1 \mod 29$

$x^2 = 6 \mod 29$

$6 + 29 = 35$

$x^2 = 35$ ✗

$35 + 29 = 64$

$x^2 = 64$

$x = \pm 8$

$x = 8 \mod 29$

$x = -8 \mod 29$

$= 21 \mod 29$

eg

$x^{39} \equiv 3 \mod 13$

$(x^3)^{13} \mod 13 \equiv 3 \mod 13$

$x^3 \mod 13$

EULER'S THEOREM.

For every positive integer 'a' and 'n' which are said to be relatively prime then

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

$\phi(n)$ = EULER'S totient function.

example:

Prove Euler's theorem hold true for $a = 3$ and $n = 10$

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

$$3^{\phi(10)} \equiv 1 \bmod 10$$

$$\phi(10) = 2 \times 5$$

$$\phi(2) \times \phi(5)$$

$$1 \times 4 = 4$$

$$3^4 \equiv 1 \bmod 10$$

$$81 \equiv 1 \bmod 10 = \frac{81}{10} = 1$$

Therefore Euler's theorem holds true for $a = 3, n = 10$.

Euler's totient function.

Case 1: if n is prime no

$n = 17 \quad \phi(n) = n-1$

$\phi(17) = 17-1 = 16$

Because 17 is prime, all of the positive integers from 1 through 16 are relatively prime to 17. Thus $\phi(17) = 16$.

case 2: $n = p \times q$

Where p, q are prime no's

$$\phi(n) = \phi(p \times q)$$
$$= \phi(p) \times \phi(q)$$
$$= (p-1) \times (q-1)$$

eg $n = 15$

$$\phi(15) = 5 \times 3$$
$$\phi(5) \times \phi(3)$$
$$(5-1) \times (3-1)$$
$$4 \times 2 = 8.$$

$$\boxed{\phi(15) = 8}$$

Case 3 $n = p^e$, p is prime no

$$\phi(n) = p^e - p^{e-1}$$

eg $n = 8$

$$\phi(8) = 2^3$$
$$= 2^3 - 2^{3-1} = 8 - 4 = 4$$

$\phi(21)$

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

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

$= 2 \times 6 = 12.$

Where the 12 integers are

$\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

Euler's theorem

Proof

Consider set of integers 'R'

$R = \{x_1, x_2 \cdots x_{\phi(n)}\}$, $< n$

$gcd(x_i, n) = 1$ $i = \phi(n)$

Multiply

$S = \{a x_1 \bmod n, a x_2 \bmod n \cdots a x_{\phi(n)} \bmod n\}$

$$\prod_{i=1}^{\phi(n)} a x_i \bmod n = \prod_{i=1}^{\phi(n)} x_i$$

represented as

$$\prod_{i=1}^{\phi(n)} a x_i \equiv \prod_{i=1}^{\phi(n)} x_i \bmod n$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i \equiv \prod_{i=1}^{\phi(n)} x_i \bmod n$$

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$

eg $a = 3, n = 13$

$3^{202} \bmod 13$

$$12 \overline{)202} \quad 16$$
12
82
72
10

202 multiples of 12

$\phi(n) = n-1$

$\phi(13) = 12$

$3^{12 \times 16 + 10} \bmod 13$

$(3^{12})^{16} \cdot 3^{10} \bmod 13$

$(1)^{16} \cdot 3^{10} \bmod 13$

$3^{10} \bmod 13$

$3^3 \cdot 3^3 \cdot 3^3 \cdot 3^1 \bmod 13 = 3.$

Testing for Primality:-

Primality testing determines whether a given number n is prime or not.

⇒ It is essential for generating secure keys in cryptographic system.

Miller - Rabin Test:- / Miller - Rabin algorithm

Algorithm:-

Step 1 : Find $n-1 = 2^k \times m$

Step 2 : Choose 'a' such that $1 < a < n-1$

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

$+1 \rightarrow$ composite

$-1 \rightarrow$ probably prime

eg

Is 561 prime

Solution

Given $n = 561$

Step 1: Fin $n-1 = 2^k \times m$

$560 = 2^4 \times 35$

So $k=4, m=35$

$560 \div 2^1 = 280$

$280 \div 2^2 = 140$

$140 \div 2^3 = 70$

$\frac{560}{2^1} = 280, \frac{560}{2^2} = 140$

$\frac{560}{2^3} = 70 \quad \frac{560}{2^4} = 35$

Step 2

Choosing $a=2$; $1<2<560$

Step 3

Compute $b_0 = a^m \pmod n$

$b_0 = 2^{35} \pmod{561}$

$= 263$

Is $b_0 = \pm 1 \pmod{561}$? NO

So calculate b_1

$b_1 = b_0^2 \pmod n$

$b_1 = 263^2 \pmod{561}$

$b_1 = 166$

Is $b_1 = \pm 1 \pmod{561}$? NO

$b_2 = b_1^2 \pmod n$

$b_2 = 166^2 \pmod{561}$

$b_2 = 67$

Is $b_2 = \pm 1 \pmod{561}$? NO

$b_3 = b_2^2 \pmod{561}$

$= 67^2 \pmod{561}$

$b_3 = 1 \rightarrow$ composite

561 is composite no