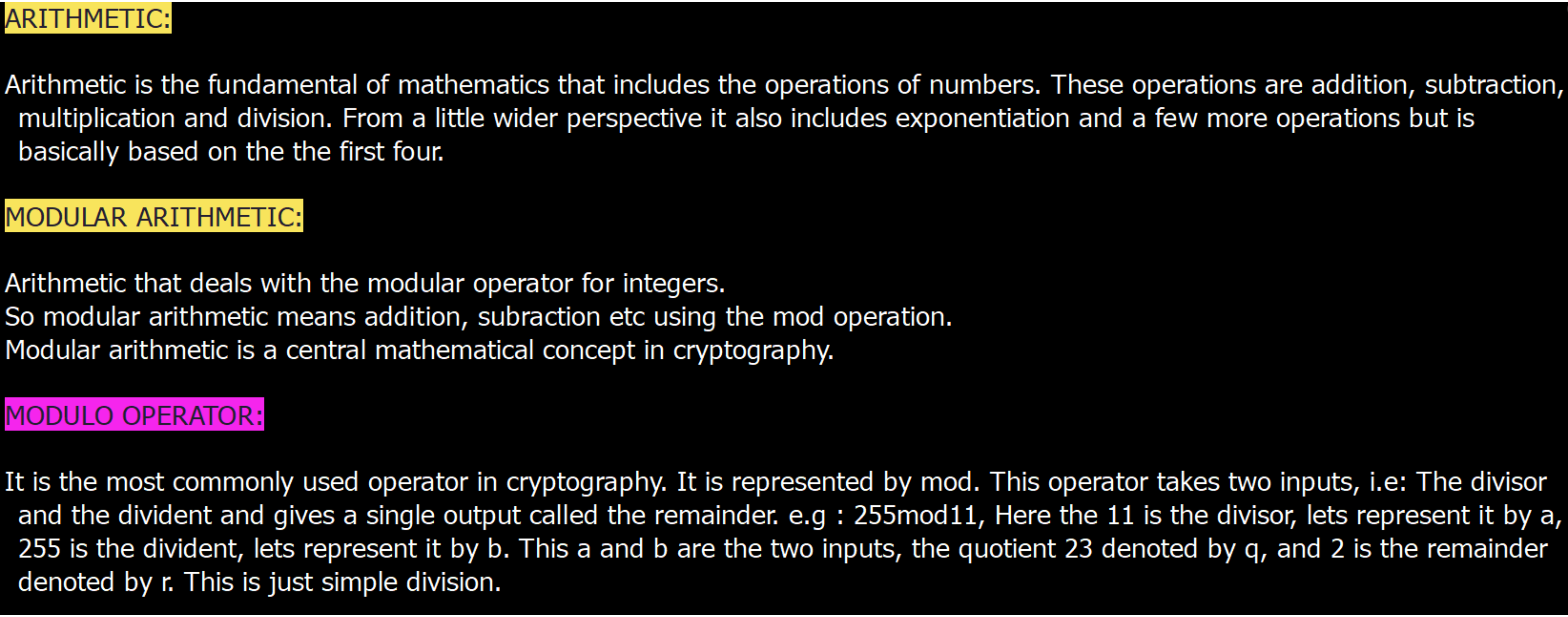
HAROON



ARITHMETIC:

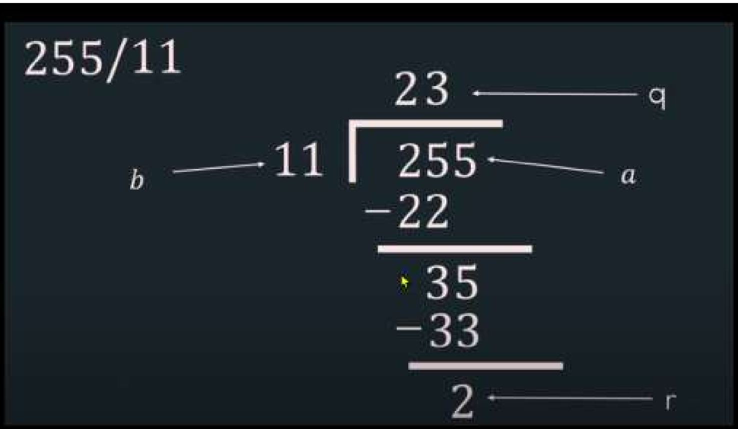
Arithmetic is the fundamental of mathematics that includes the operations of numbers. These operations are addition, subtraction, multiplication and division. From a little wider perspective it also includes exponentiation and a few more operations but is basically based on the the first four.

MODULAR ARITHMETIC:

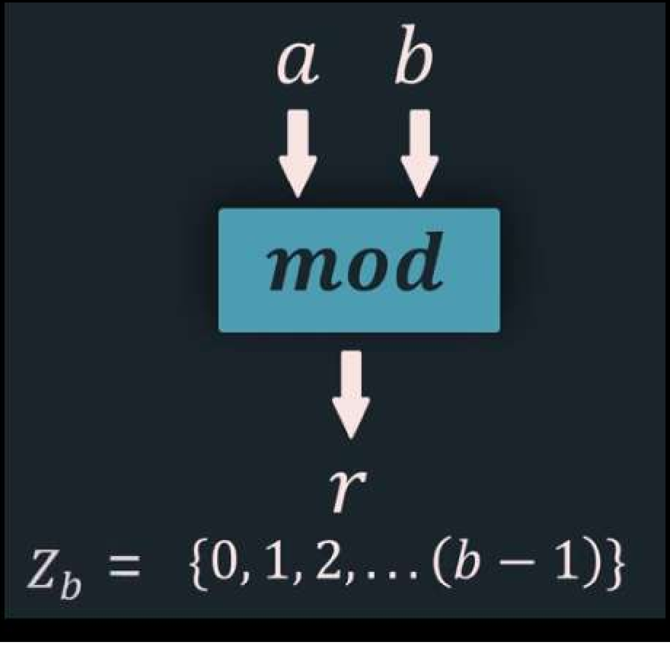
Arithmetic that deals with the modular operator for integers.
So modular arithmetic means addition, subraction etc using the mod operation.
Modular arithmetic is a central mathematical concept in cryptography.

MODULO OPERATOR:

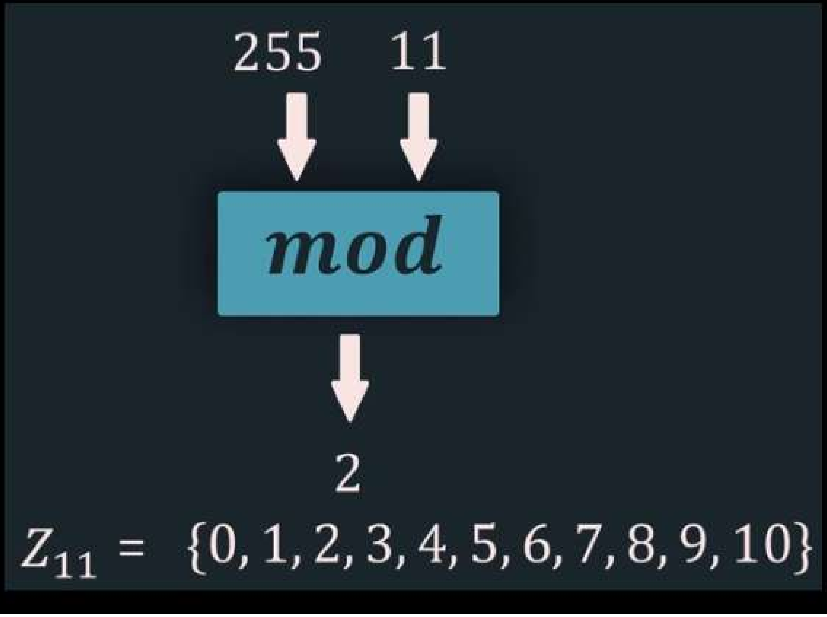
It is the most commonly used operator in cryptography. It is represented by mod. This operator takes two inputs, i.e: The divisor and the divident and gives a single output called the remainder. e.g : 255mod11, Here the 11 is the divisor, lets represent it by a, 255 is the divident, lets represent it by b. This a and b are the two inputs, the quotient 23 denoted by q, and 2 is the remainder denoted by r. This is just simple division.



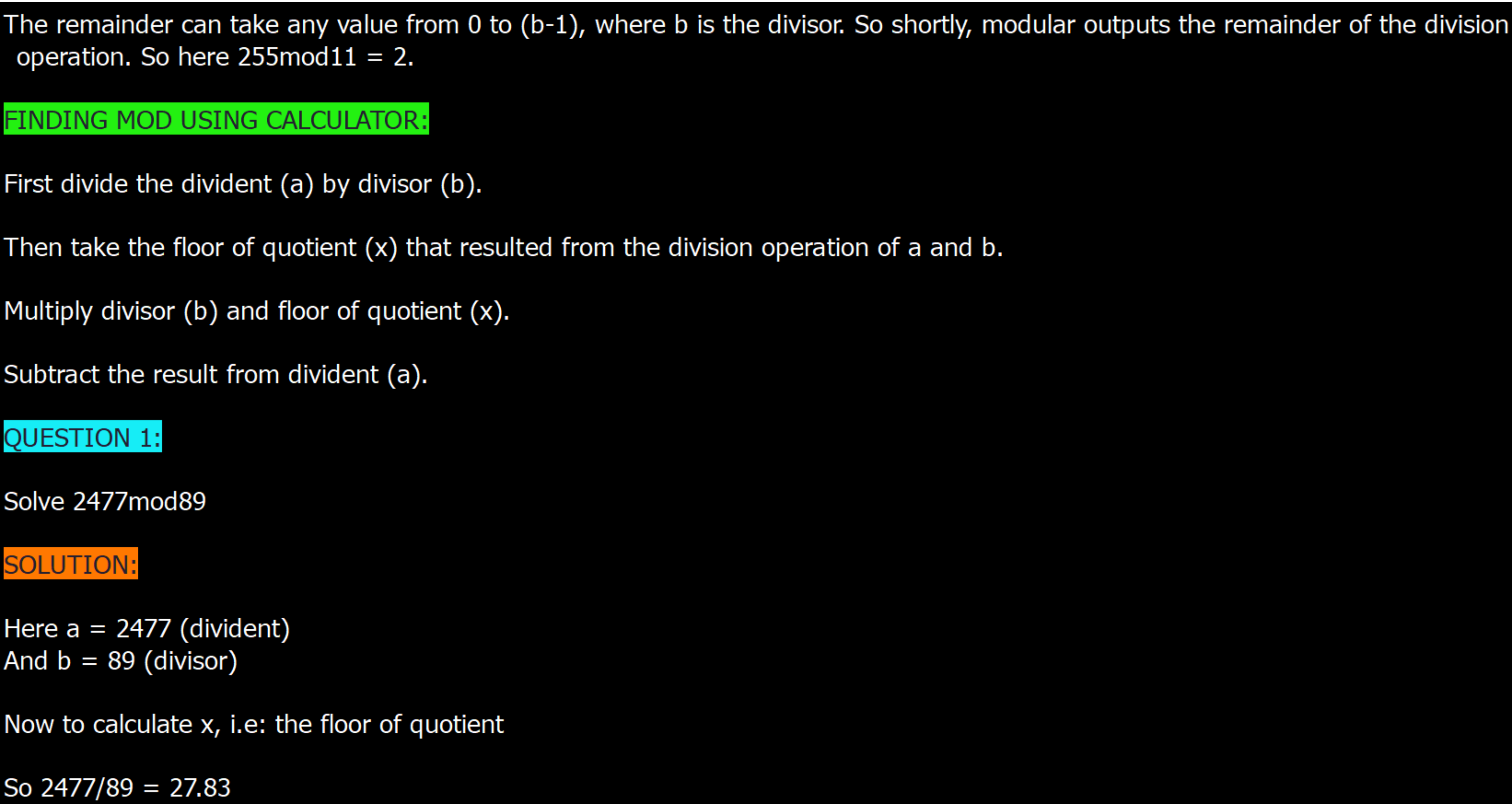
Here is how mod operator works:



$Z_b = \{0, 1, 2, \ldots (b-1)\}$



$Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$



The remainder can take any value from 0 to (b-1), where b is the divisor. So shortly, modular outputs the remainder of the division operation. So here 255mod11 = 2.

FINDING MOD USING CALCULATOR:

First divide the divident (a) by divisor (b).

Then take the floor of quotient (x) that resulted from the division operation of a and b.

Multiply divisor (b) and floor of quotient (x).

Subtract the result from divident (a).

QUESTION 1:

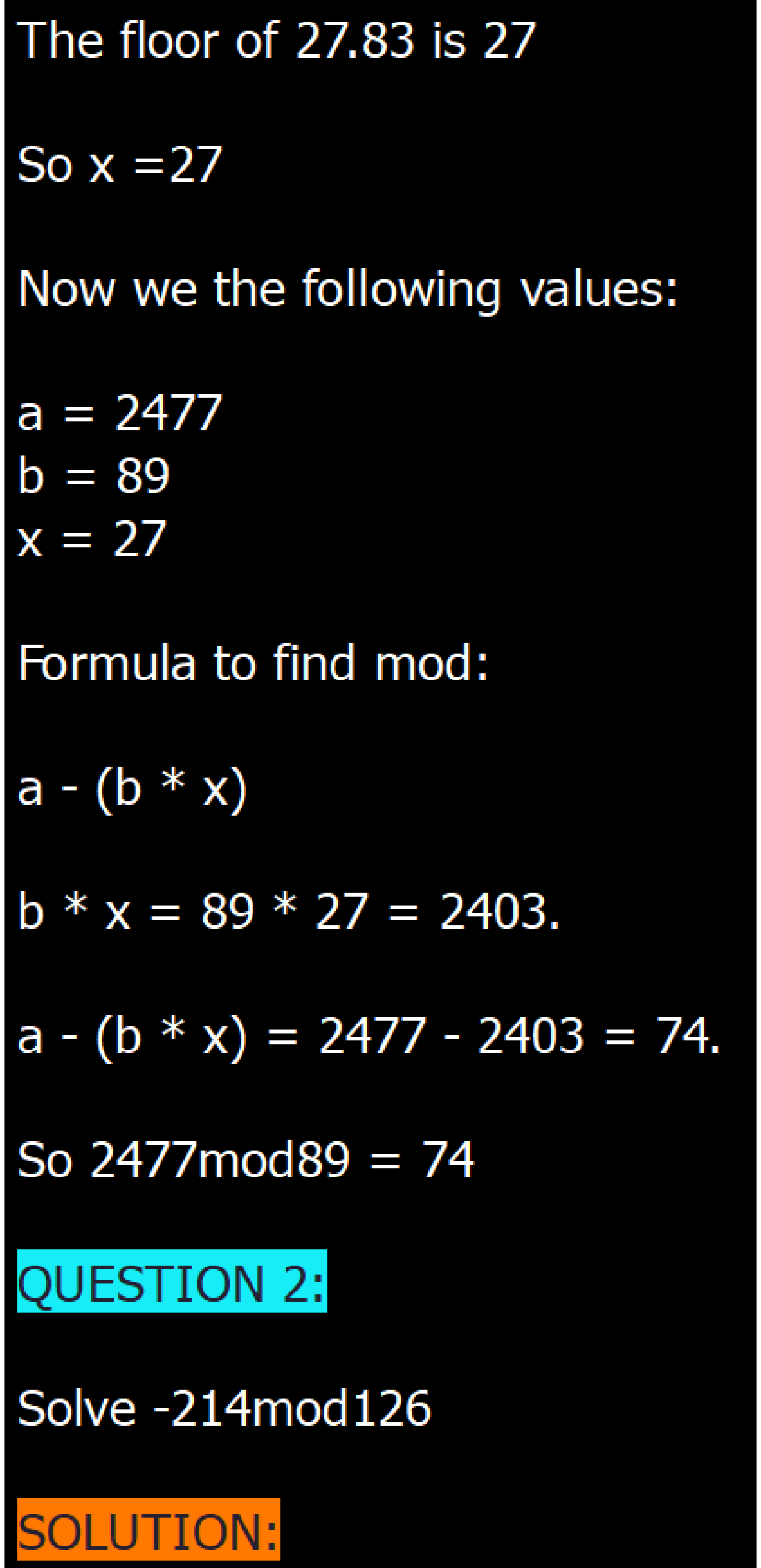
Solve 2477mod89

SOLUTION:

Here a = 2477 (divident)
And b = 89 (divisor)

Now to calculate x, i.e: the floor of quotient

So 2477/89 = 27.83



The floor of 27.83 is 27

So x =27

Now we the following values:

a = 2477
b = 89
x = 27

Formula to find mod:

a - (b * x)

b * x = 89 * 27 = 2403.

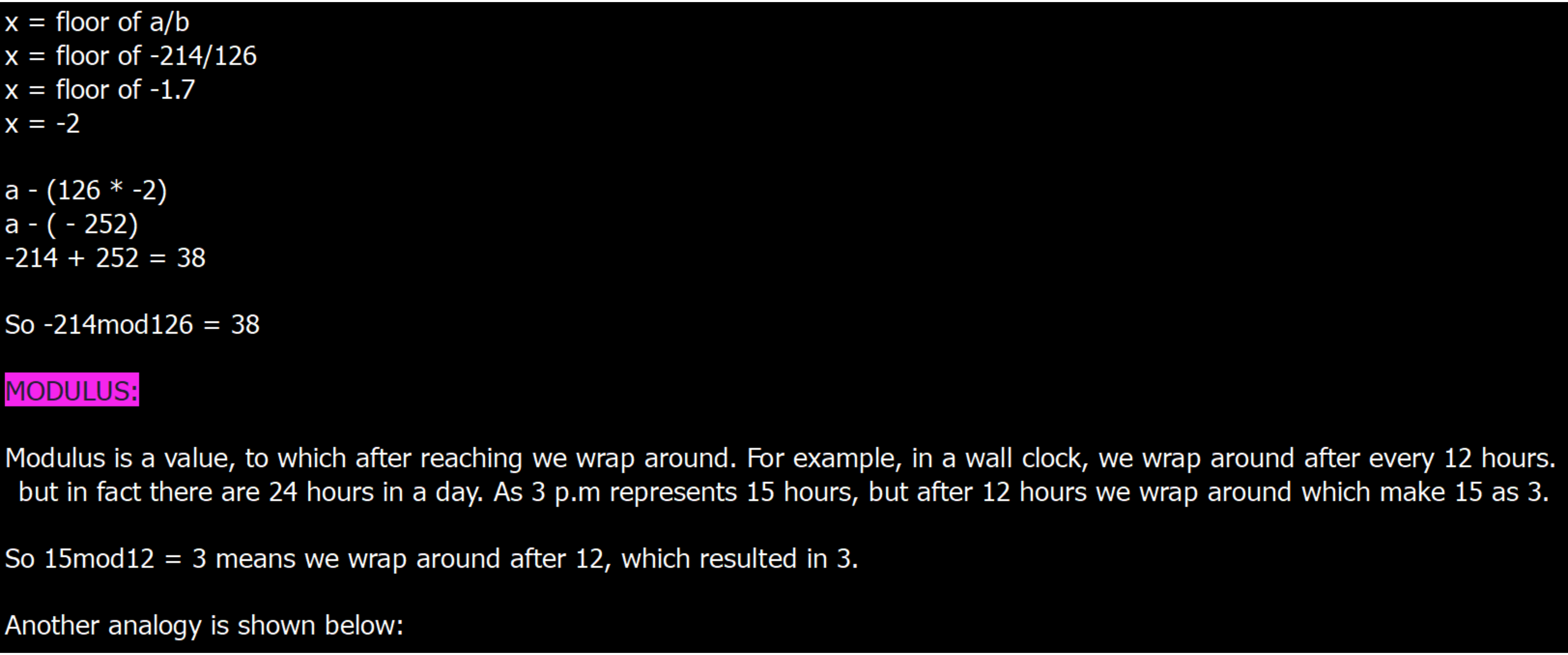
a - (b * x) = 2477 - 2403 = 74.

So 2477mod89 = 74

QUESTION 2:

Solve -214mod126

SOLUTION:



x = floor of a/b
x = floor of -214/126
x = floor of -1.7
x = -2

a - (126 * -2)
a - (- 252)
-214 + 252 = 38

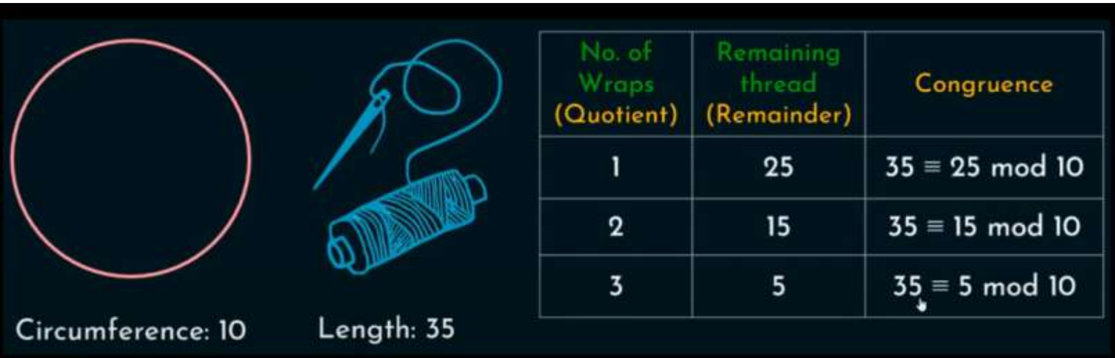
So -214mod126 = 38

MODULUS:

Modulus is a value, to which after reaching we wrap around. For example, in a wall clock, we wrap around after every 12 hours. but in fact there are 24 hours in a day. As 3 p.m represents 15 hours, but after 12 hours we wrap around which make 15 as 3.

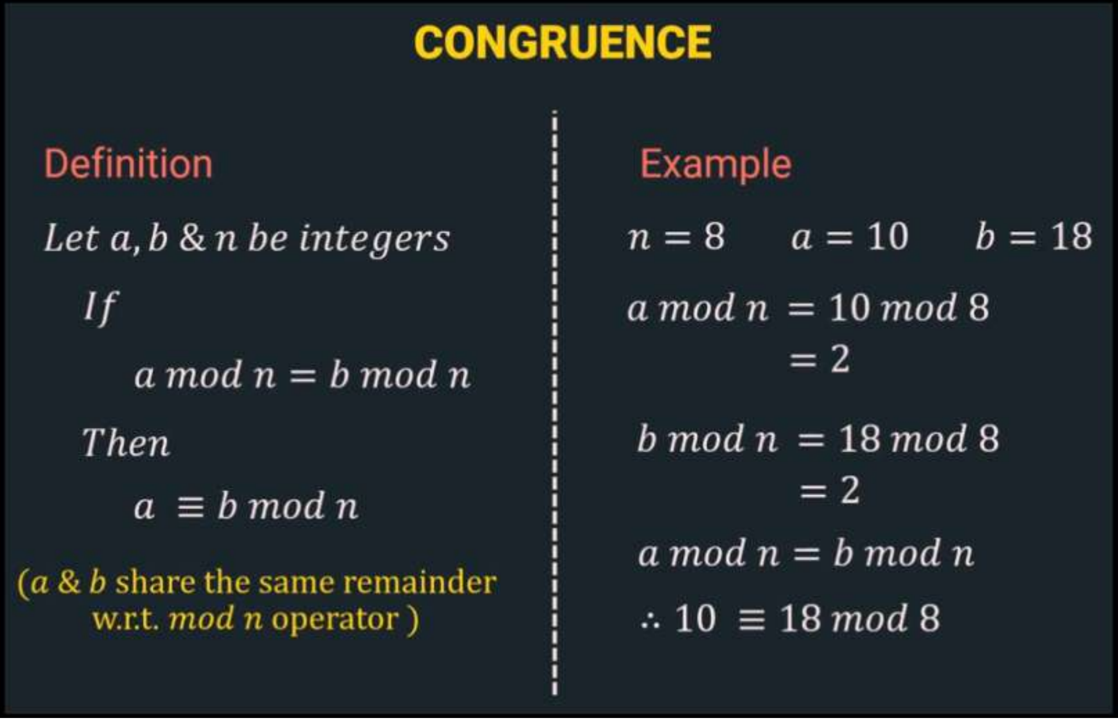
So 15mod12 = 3 means we wrap around after 12, which resulted in 3.

Another analogy is shown below:



No. of Wraps (Quotient)	Remaining thread (Remainder)	Congruence
1	25	35 ≡ 25 mod 10
2	15	35 ≡ 15 mod 10
3	5	35 ≡ 5 mod 10

CONGRUENCE:



CONGRUENCE

Definition

Let a, b & n be integers

If

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

Then

$$a \equiv b \bmod n$$

(a & b share the same remainder w.r.t. *mod n* operator)

Example

$n = 8 \quad a = 10 \quad b = 18$

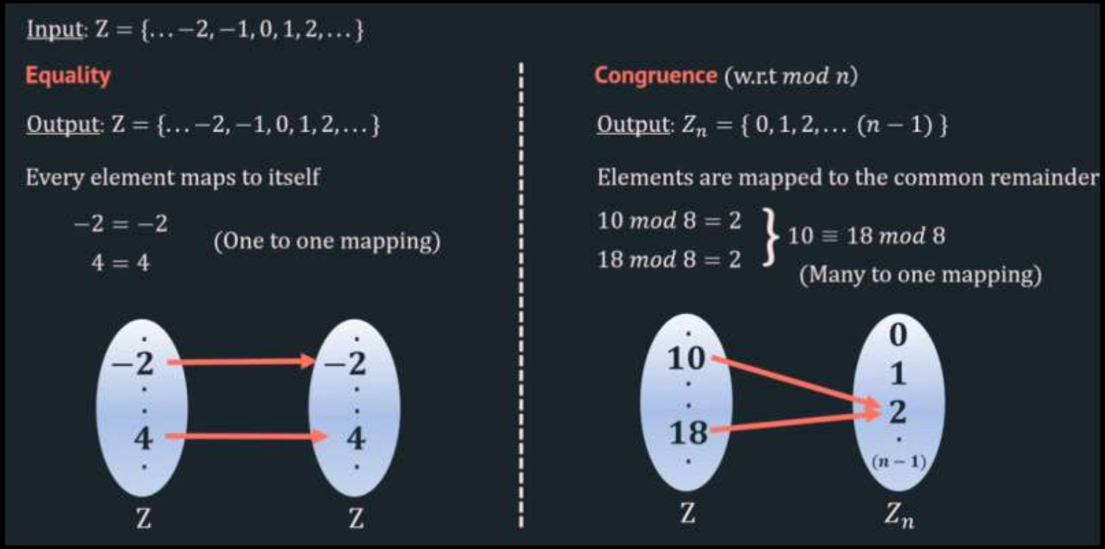
$$a \bmod n = 10 \bmod 8$$
$$= 2$$

$$b \bmod n = 18 \bmod 8$$
$$= 2$$

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

$$\therefore 10 \equiv 18 \bmod 8$$

CONGRUENCE VS EQUALITY:



Input: Z = $\{\ldots -2, -1, 0, 1, 2, \ldots\}$

Equality

Output: Z = $\{\ldots -2, -1, 0, 1, 2, \ldots\}$

Every element maps to itself

$-2 = -2$

$4 = 4$

(One to one mapping)

Congruence (w.r.t *mod n*)

Output: $Z_n = \{0, 1, 2, \ldots (n-1)\}$

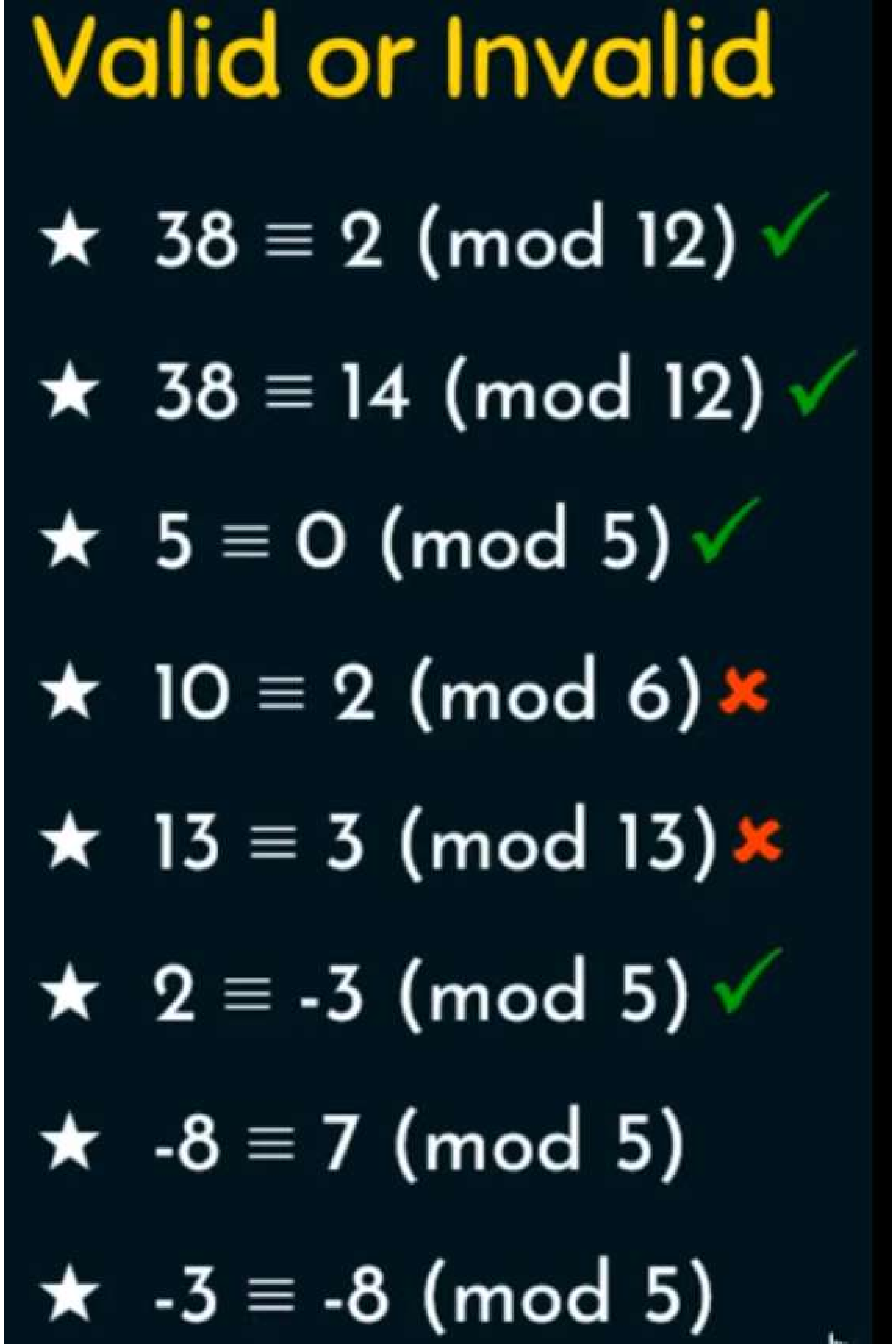
Elements are mapped to the common remainder

$$\left.\begin{array}{l}10 \; mod \; 8 = 2 \\ 18 \; mod \; 8 = 2\end{array}\right\} 10 \equiv 18 \; mod \; 8$$

(Many to one mapping)

The input of congruence is same as the equality.

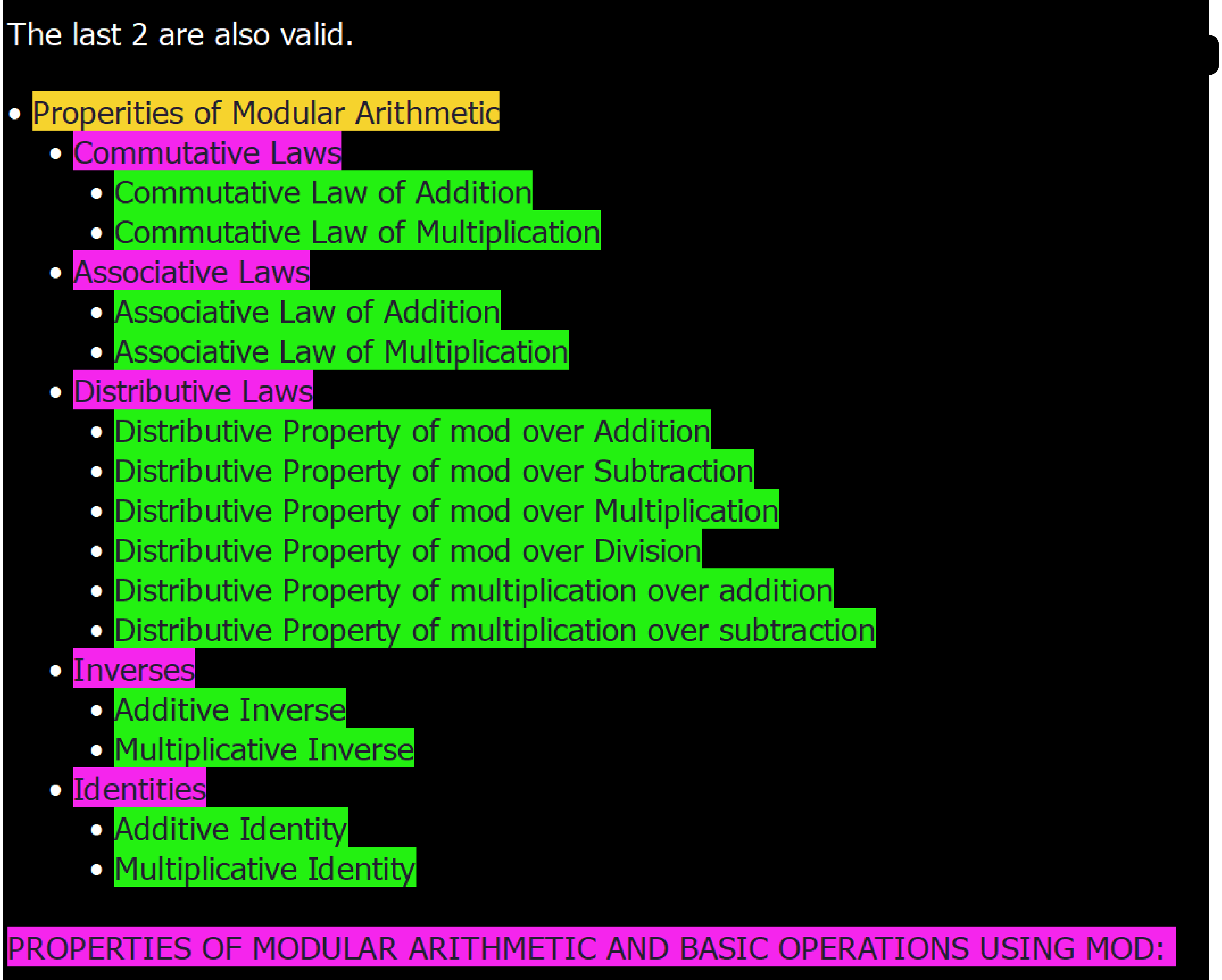
VALID AND INVALID MOD:



Valid or Invalid

- ★ $38 \equiv 2 \pmod{12}$ ✓
- ★ $38 \equiv 14 \pmod{12}$ ✓
- ★ $5 \equiv 0 \pmod{5}$ ✓
- ★ $10 \equiv 2 \pmod{6}$ ✗
- ★ $13 \equiv 3 \pmod{13}$ ✗
- ★ $2 \equiv -3 \pmod{5}$ ✓
- ★ $-8 \equiv 7 \pmod{5}$
- ★ $-3 \equiv -8 \pmod{5}$

ON

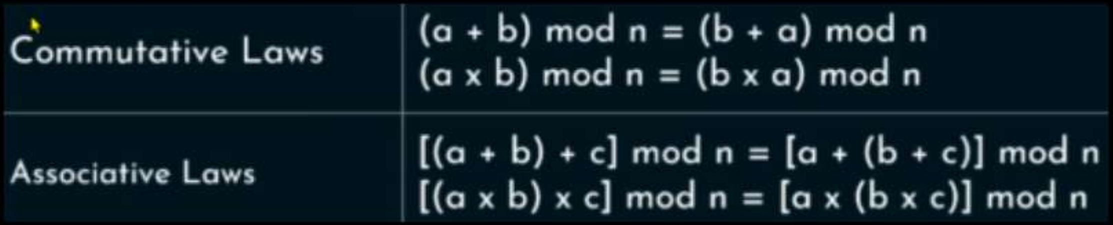


The last 2 are also valid.

- Properities of Modular Arithmetic
  - Commutative Laws
    - Commutative Law of Addition
    - Commutative Law of Multiplication
  - Associative Laws
    - Associative Law of Addition
    - Associative Law of Multiplication
  - Distributive Laws
    - Distributive Property of mod over Addition
    - Distributive Property of mod over Subtraction
    - Distributive Property of mod over Multiplication
    - Distributive Property of mod over Division
    - Distributive Property of multiplication over addition
    - Distributive Property of multiplication over subtraction
  - Inverses
    - Additive Inverse
    - Multiplicative Inverse
  - Identities
    - Additive Identity
    - Multiplicative Identity

PROPERTIES OF MODULAR ARITHMETIC AND BASIC OPERATIONS USING MOD:

1, 2. COMMUTATIVE AND ASSOCIATIVE PROPERTIES USING MODULAR OPERATIONS:



Commutative Laws	(a + b) mod n = (b + a) mod n (a x b) mod n = (b x a) mod n
Associative Laws	[(a + b) + c] mod n = [a + (b + c)] mod n [(a x b) x c] mod n = [a x (b x c)] mod n

3. DISTRIBUTIVE LAWS:

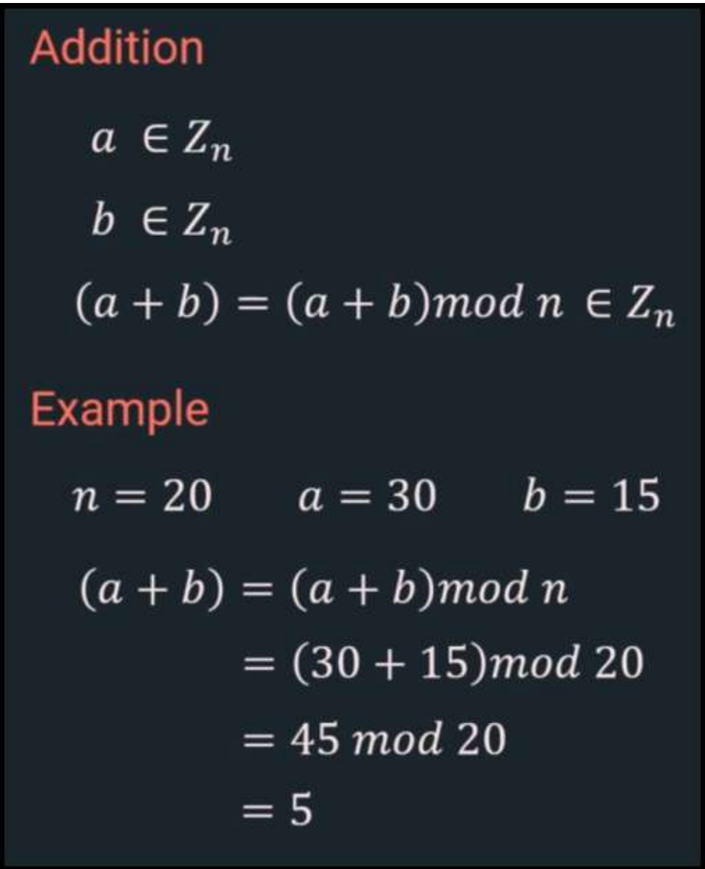
a. PERFORMING ADDITION AND THEN CHECKING DISTRIBUTIVE PROPERTY OF MOD OVER ADDITION HOLDS TRUE IN MOD OPERATION:

- ADDITION IN MODULAR ARITHMETIC:

Lets perform addition using modulo operator.

As in simple addition we use a + b for adding 2 integers, so in modular addition we apply mod with it for addition.

So a + b in normal mathematics is equal to a + b mod n in modular arithmetic



Addition

$$a \in Z_n$$

$$b \in Z_n$$

$$(a + b) = (a + b) mod\ n \in Z_n$$

Example

$$n = 20 \qquad a = 30 \qquad b = 15$$

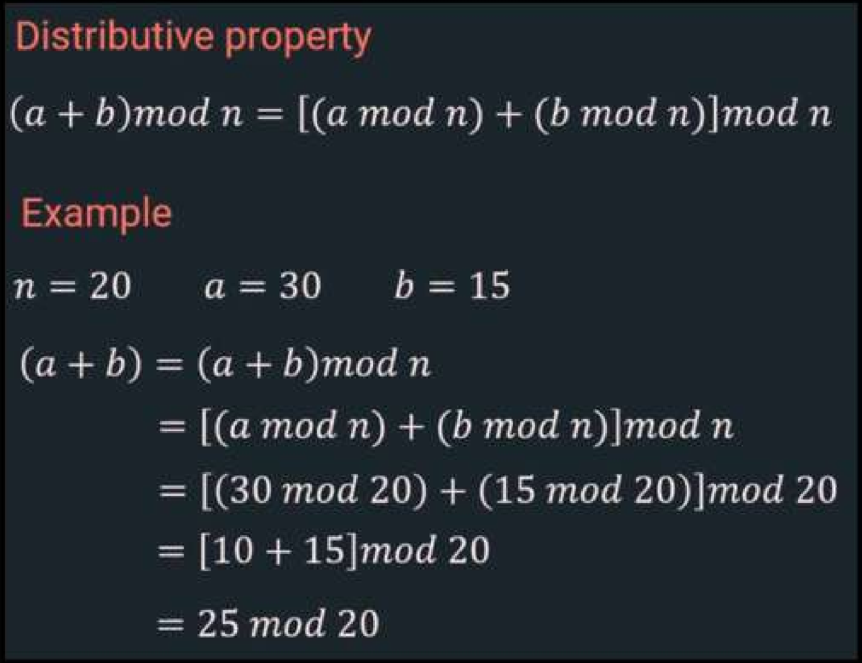
$$\begin{aligned}(a + b) &= (a + b) mod\ n \\ &= (30 + 15) mod\ 20 \\ &= 45\ mod\ 20 \\ &= 5\end{aligned}$$

We have learned how to add using mod, also we have find the value of left hand side of the distributive property of mod over addition.

- DISTRIBUTIVE PROPERTY OF MOD OVER ADDITION:

Lets understand the distributive property of mod operator in addition. Here we distribute the mod operator over the additon operation.

Example:



Distributive property

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

Example

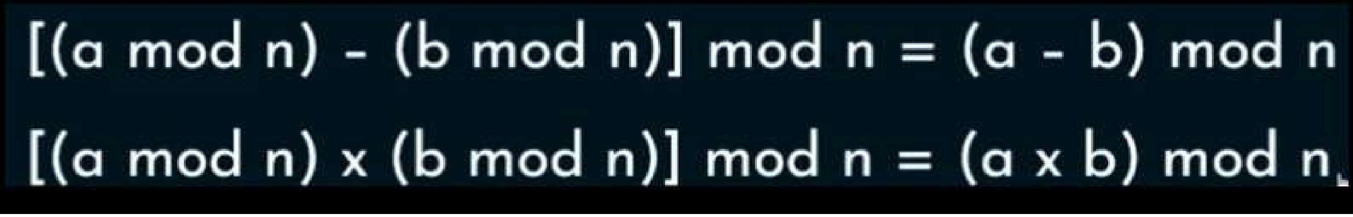
$n = 20 \qquad a = 30 \qquad b = 15$

$$\begin{aligned}(a+b) &= (a+b) mod\ n\\ &= [(a\ mod\ n) + (b\ mod\ n)] mod\ n\\ &= [(30\ mod\ 20) + (15\ mod\ 20)] mod\ 20\\ &= [10 + 15] mod\ 20\\ &= 25\ mod\ 20\end{aligned}$$

= 5

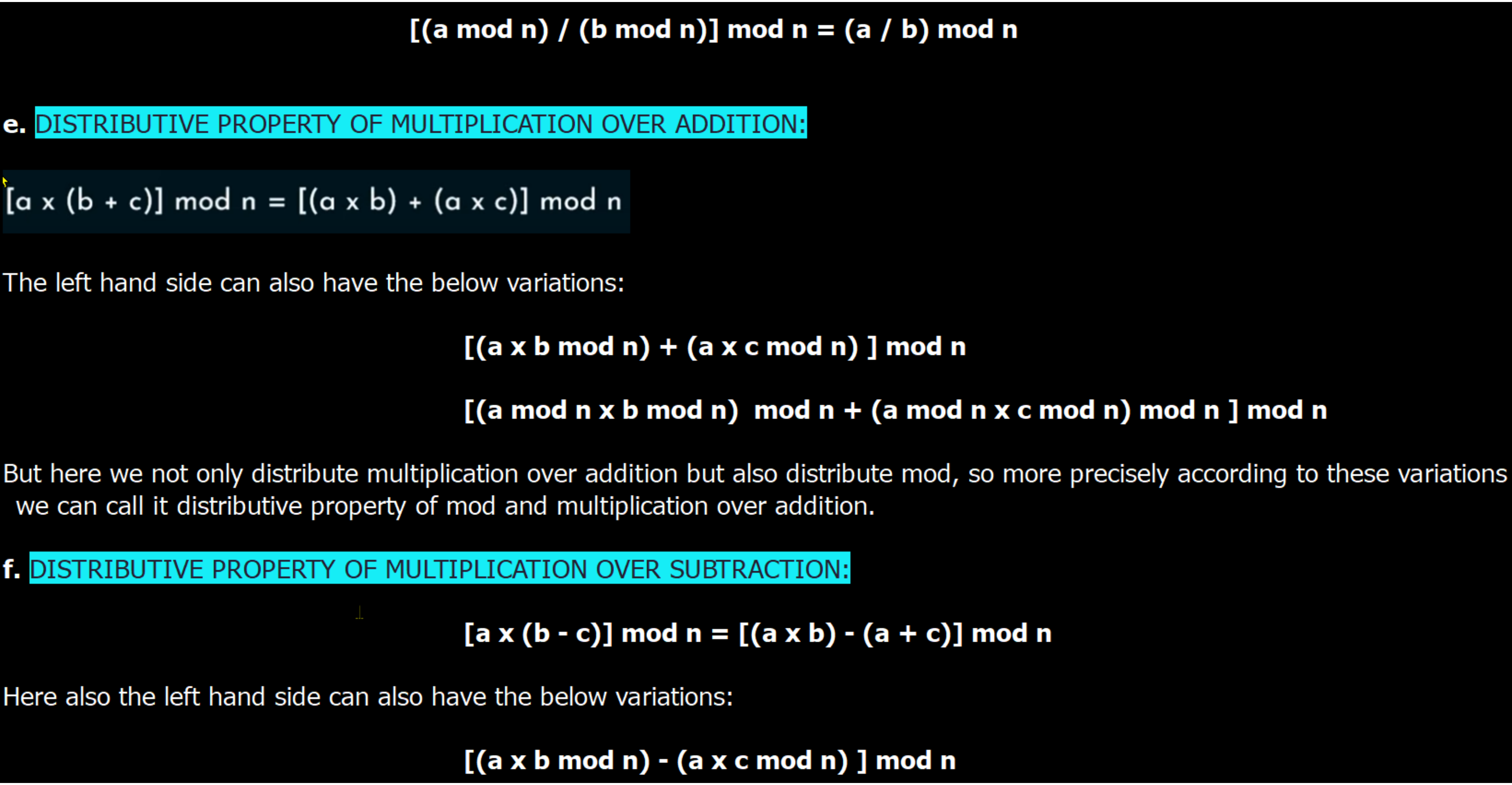
Hence the distributive property of mod over addition holds true.

b, c, d. DISTRIBUTIVE PROPERTY OF MOD OVER SUBTRACTION, DIVISION AND MULTIPLICATION:



[(a mod n) - (b mod n)] mod n = (a - b) mod n

[(a mod n) x (b mod n)] mod n = (a x b) mod n



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

e. DISTRIBUTIVE PROPERTY OF MULTIPLICATION OVER ADDITION:

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

The left hand side can also have the below variations:

$$[(a \times b \bmod n) + (a \times c \bmod n)\ ] \bmod n$$

$$[(a \bmod n \times b \bmod n)\ \ \bmod n + (a \bmod n \times c \bmod n) \bmod n\ ] \bmod n$$

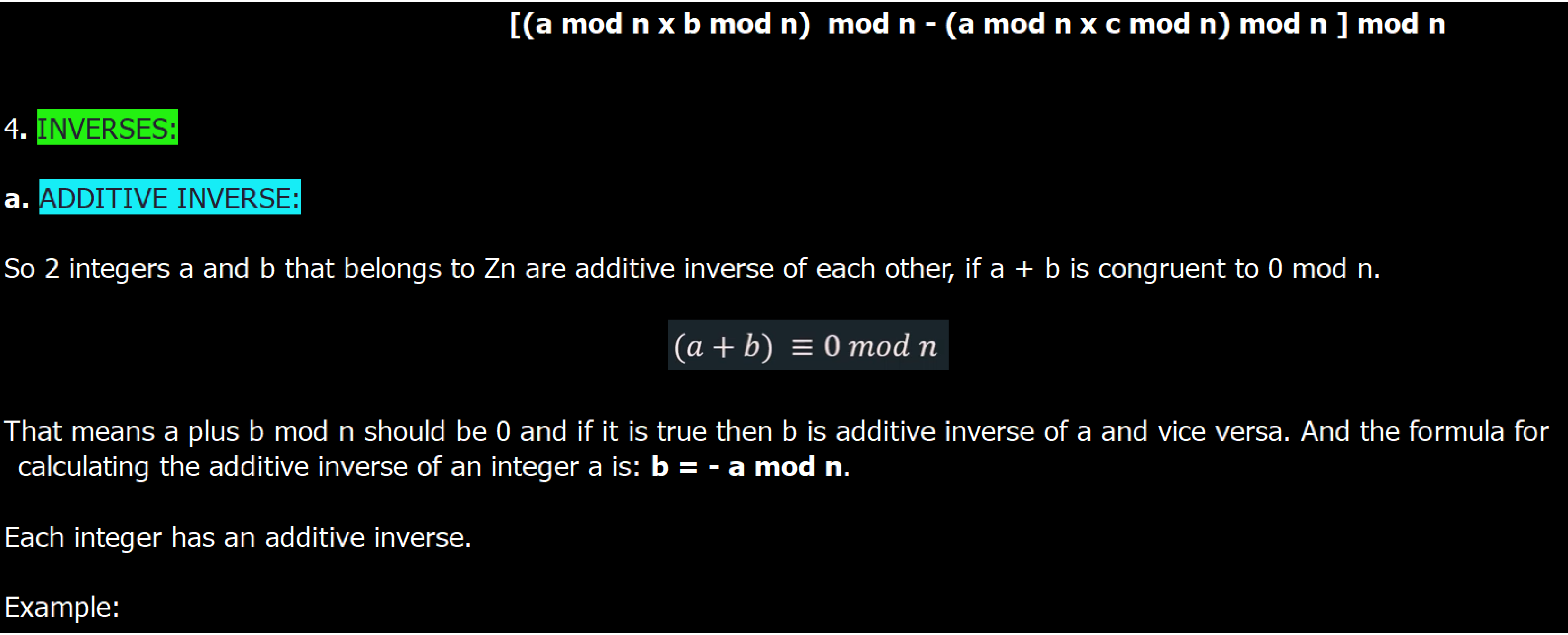
But here we not only distribute multiplication over addition but also distribute mod, so more precisely according to these variations we can call it distributive property of mod and multiplication over addition.

f. DISTRIBUTIVE PROPERTY OF MULTIPLICATION OVER SUBTRACTION:

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

Here also the left hand side can also have the below variations:

$$[(a \times b \bmod n) - (a \times c \bmod n)\ ] \bmod n$$



[(a mod n x b mod n) mod n - (a mod n x c mod n) mod n] mod n

4. INVERSES:

a. ADDITIVE INVERSE:

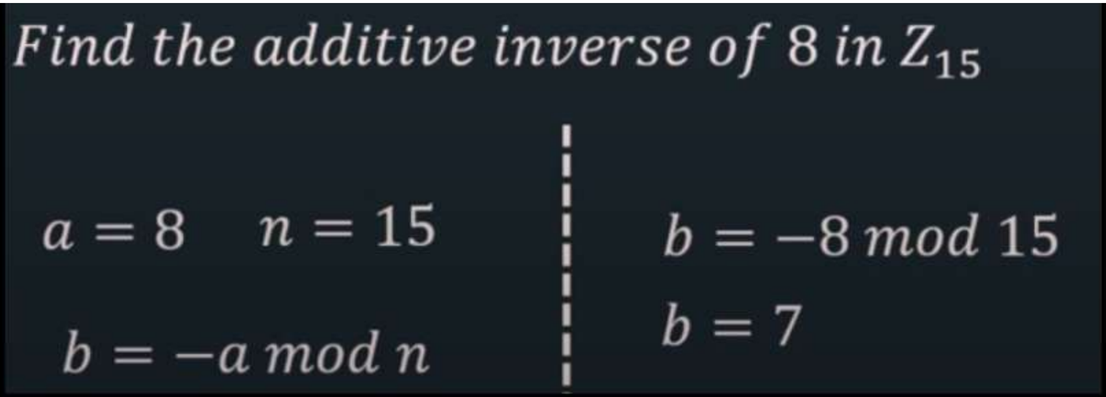
So 2 integers a and b that belongs to Zn are additive inverse of each other, if a + b is congruent to 0 mod n.

$$(a + b) \ \equiv 0 \, mod \, n$$

That means a plus b mod n should be 0 and if it is true then b is additive inverse of a and vice versa. And the formula for calculating the additive inverse of an integer a is: **b = - a mod n.**

Each integer has an additive inverse.

Example:



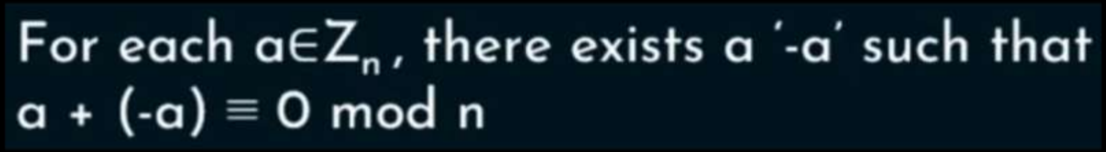
Find the additive inverse of 8 *in* Z_{15}

$a = 8 \quad n = 15$

$b = -a \bmod n$

$b = -8 \bmod 15$

$b = 7$

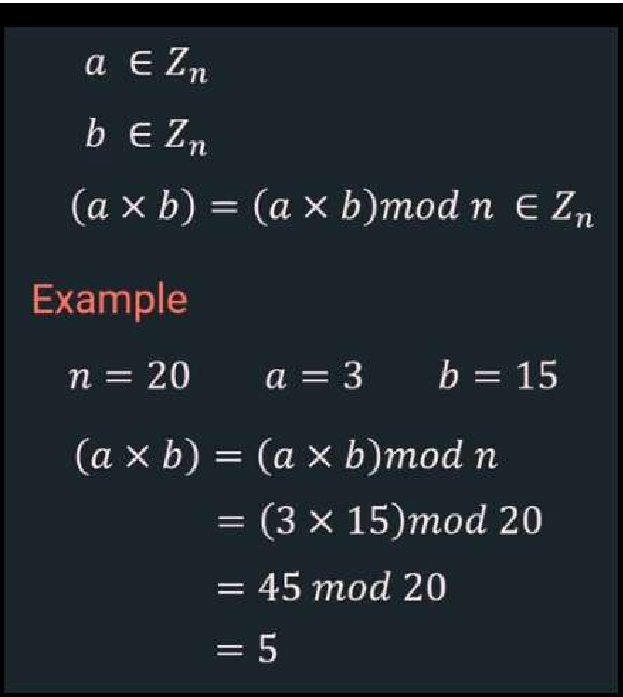


For each $a \in Z_n$, there exists a '-a' such that $a + (-a) \equiv 0 \bmod n$

Sometimes the above expression is used for defining addivtive inverse, so here -a is actually b. But here -a is used for understanding purpose because any positive integer has inverse as its negative integer in normal additive inverse.

b. FIRST PERFORMING MULTIPLICATION IN MOD OPERATIONS AND THEN PROVING THE ABOVE DISTRBUTIVE PROPERTY OF MOD OVER MULTIPLICATION:

- MULTIPLICATION (Basics of Modular Multiplication for Multiplicative Inverse):



$a \in Z_n$

$b \in Z_n$

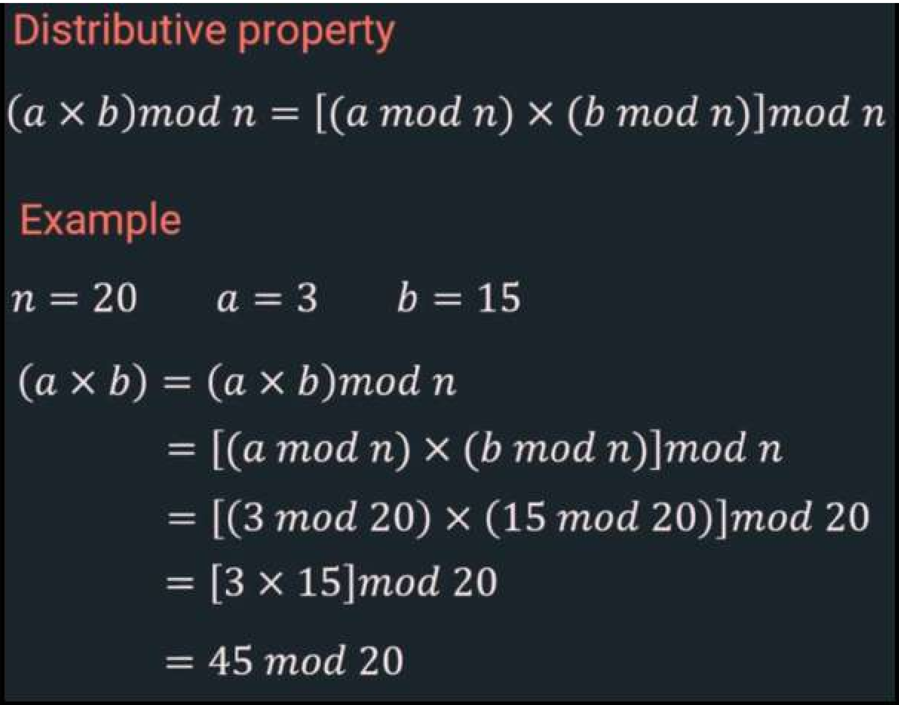
$(a \times b) = (a \times b) mod\ n \ \in Z_n$

Example

$n = 20 \qquad a = 3 \qquad b = 15$

$$\begin{aligned}(a \times b) &= (a \times b) mod\ n \\ &= (3 \times 15) mod\ 20 \\ &= 45\ mod\ 20 \\ &= 5\end{aligned}$$

DISTRIBUTIVE PROPERTY OF MOD OVER MULTIPLICATION:



Distributive property

$$(a \times b) mod\ n = [(a\ mod\ n) \times (b\ mod\ n)] mod\ n$$

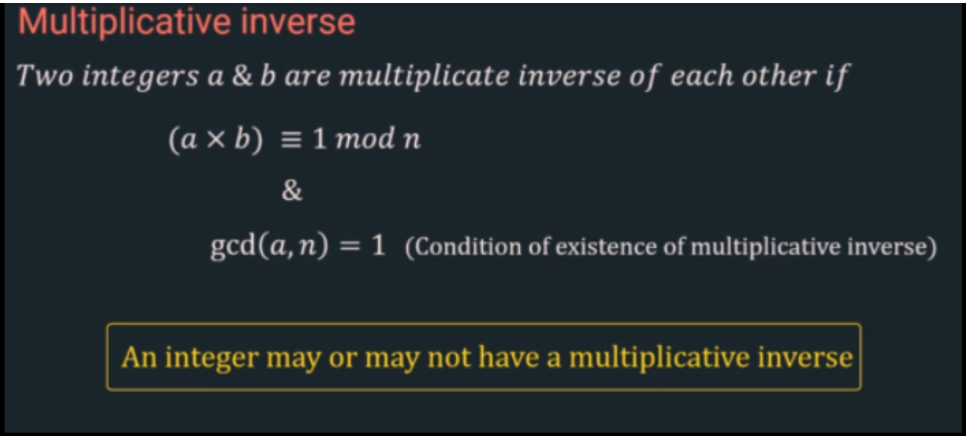
Example

$n = 20 \qquad a = 3 \qquad b = 15$

$$\begin{aligned}(a \times b) &= (a \times b) mod\ n \\ &= [(a\ mod\ n) \times (b\ mod\ n)] mod\ n \\ &= [(3\ mod\ 20) \times (15\ mod\ 20)] mod\ 20 \\ &= [3 \times 15] mod\ 20 \\ &= 45\ mod\ 20\end{aligned}$$

- MULTIPLICATIVE INVERSE:

Two integers a and b are multiplicative inverse of each other if a * b is congruent to 1 mod n and g.c.d of a and n is 1



Multiplicative inverse

Two integers a & b are multiplicate inverse of each other if

$$(a \times b) \equiv 1 \; mod \; n$$

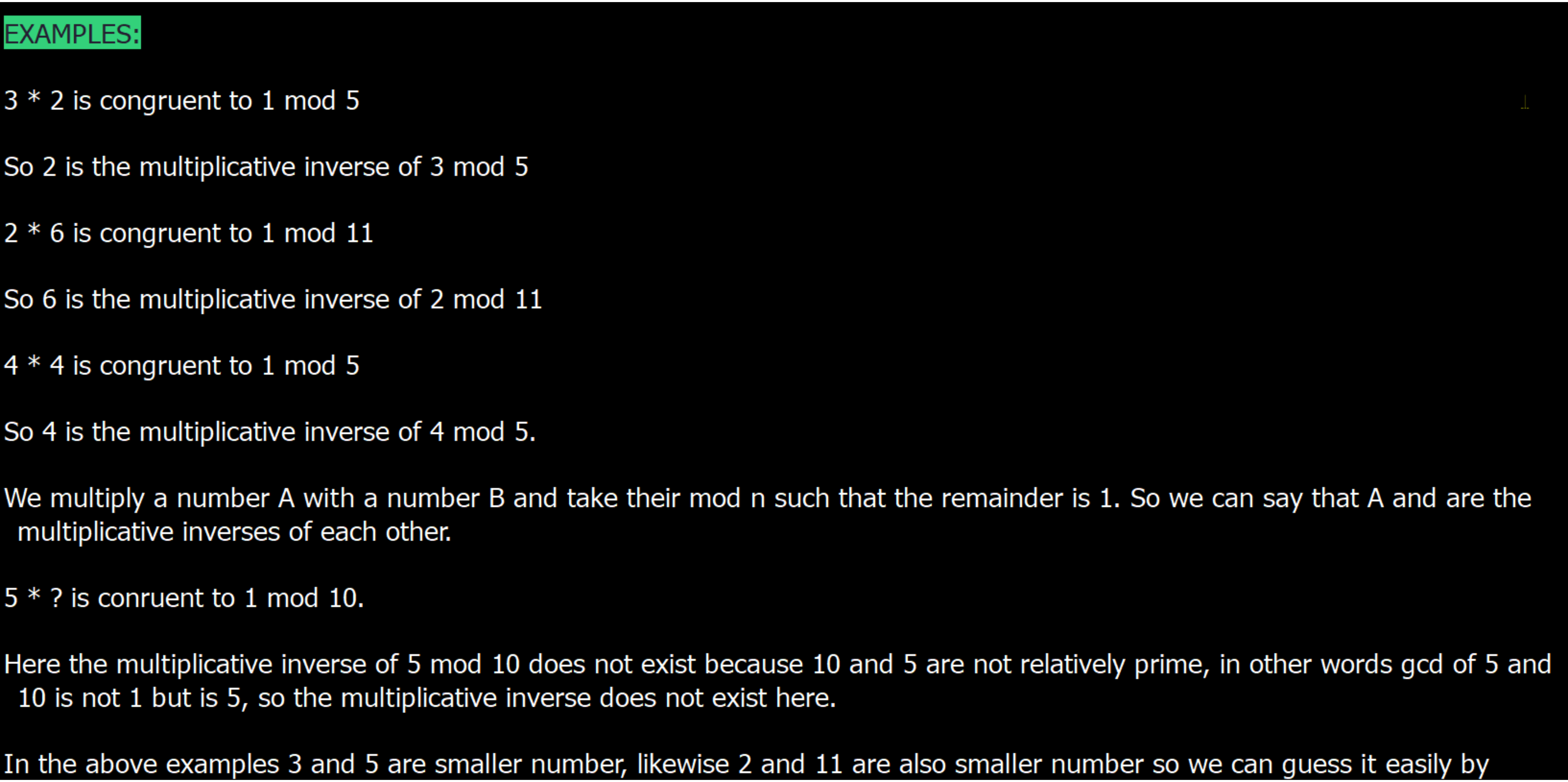
&

$$\gcd(a, n) = 1 \quad \text{(Condition of existence of multiplicative inverse)}$$

An integer may or may not have a multiplicative inverse

So here there are two conditions that must be satisfied. Also note that an integer may or may not have a multiplicative inverse with respect to mod, and how to know whether a multiplicative inverse of an integer a exist or not, and this is where the second condition comes and this condition is known as the condition of existence of multiplicative inverse so if this condition is not satisfied then multiplicative inverse for a does not exist with respect to mod n and if it is satisfied then it does exist. There is not a straight forward formula like that an additive inverse that gives us the multiplicative inverse of a number. To calculate the multiplicative inverse of a number there is an algorithm that is called as extended euclidean algorithm which is used to find it.

We can also write the above definition as a * 1/a is congruent to 1 mod n as we did in the additive inverse as -a, so we can either use a and -a or a and b in case of additive inverse, and a and a^-1 or a and b incase of multiplicative inverse, both mean the same. In case of normal integers, the 1/integer is the multiplicative inverse of that integer. For example, the multiplicative inverse of 5 is 1/5. Because when we multiply a number and its inverse it gives the result as 1, so we can say that these both are the multiplicative inverses of each other. But incase of multiplicative inverse of a number with respect to mod n, firsty will be checked if it exist or not and is different for a number with different mod number, for example the multiplcative inverse of 3 mod 5 and 3 mod 7 are different.



EXAMPLES:

3 * 2 is congruent to 1 mod 5

So 2 is the multiplicative inverse of 3 mod 5

2 * 6 is congruent to 1 mod 11

So 6 is the multiplicative inverse of 2 mod 11

4 * 4 is congruent to 1 mod 5

So 4 is the multiplicative inverse of 4 mod 5.

We multiply a number A with a number B and take their mod n such that the remainder is 1. So we can say that A and are the multiplicative inverses of each other.

5 * ? is conruent to 1 mod 10.

Here the multiplicative inverse of 5 mod 10 does not exist because 10 and 5 are not relatively prime, in other words gcd of 5 and 10 is not 1 but is 5, so the multiplicative inverse does not exist here.

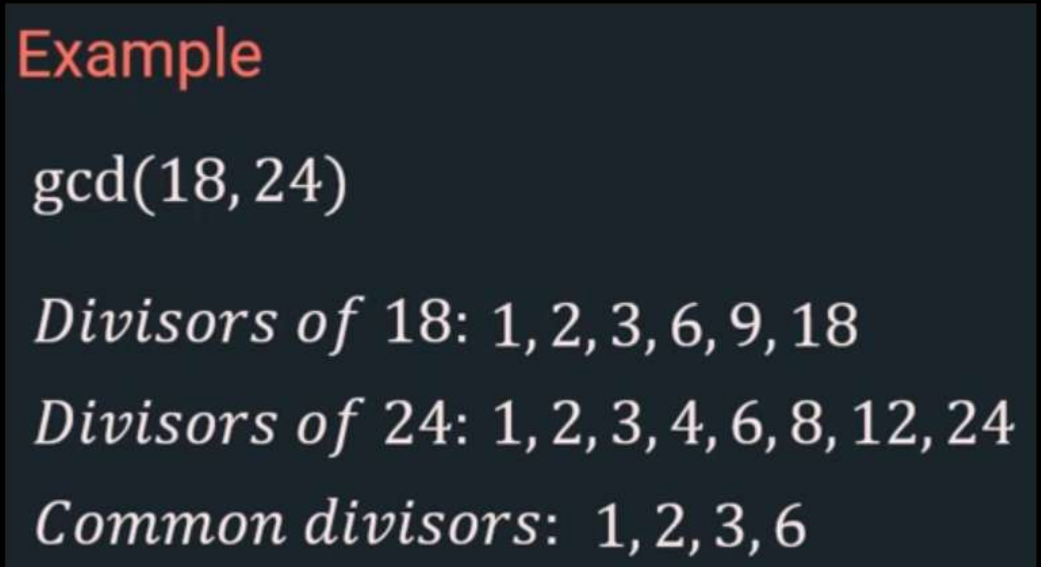
In the above examples 3 and 5 are smaller number, likewise 2 and 11 are also smaller number so we can guess it easily by starting from one and multiply it with 3 and 2 in 1st and 2nd example repectively untill we multiply a number that the remainder is zero, but for bigger numbers we use extended eucledian algorithm to find the multiplcative inverse of a number with respect to mod n.

ABSOLUTE VALUE OF A NUMBER:

The absolute value of a number or integer is the actual distance of the integer from zero, in a number line. Therefore, the absolute value is always a positive value and not a negative number.

GREATEST COMMON DIVISOR (G.C.D):

GCD of 2 integers is the largest integer that can divide both integers without a remainder or more precisely zero remainder



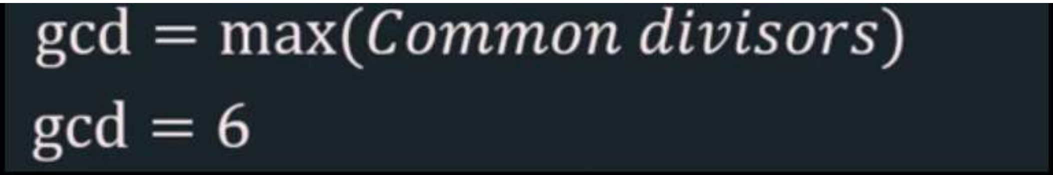
Example

$\gcd(18, 24)$

$Divisors\ of\ 18\colon 1, 2, 3, 6, 9, 18$

$Divisors\ of\ 24\colon 1, 2, 3, 4, 6, 8, 12, 24$

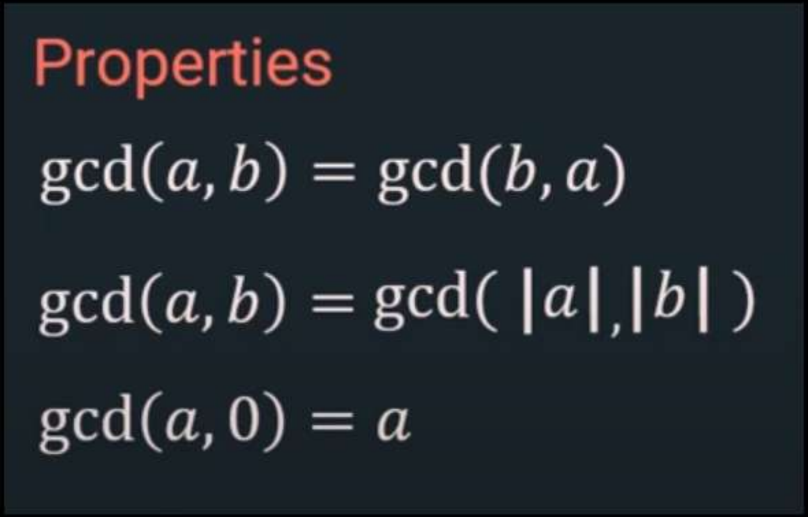
$Common\ divisors\colon\ 1, 2, 3, 6$



$$\gcd = \max(\mathit{Common\ divisors})$$

$$\gcd = 6$$

PROPERTIES OF GCD:



Properties

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

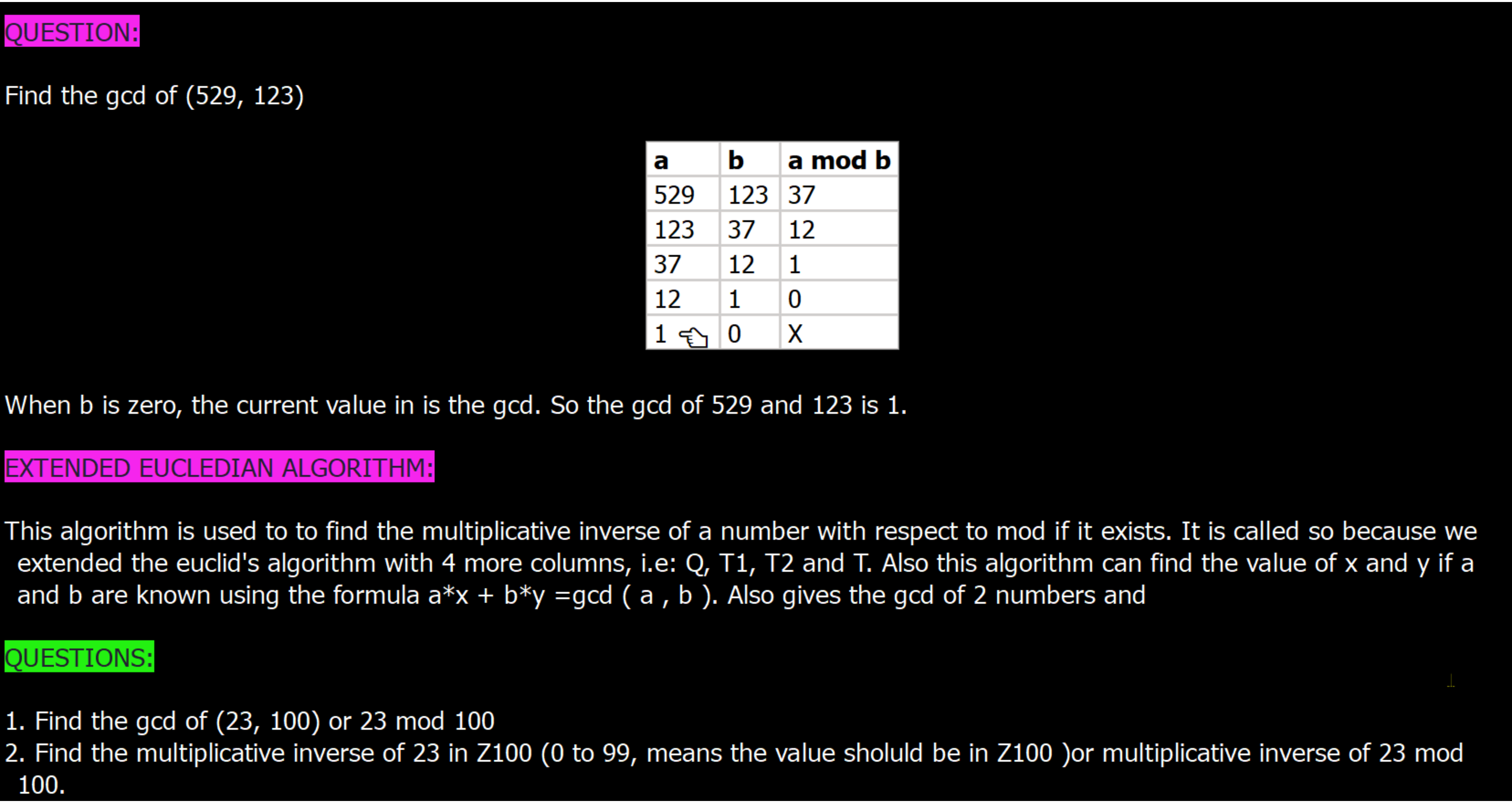
$$\gcd(a, b) = \gcd(\,|a|,|b|\,)$$

$$\gcd(a, 0) = a$$

If the numbers are big then finding every divisor is difficult therefore we have euclid's algorithm to find the gcd of 2 numbers.

EUCLIDEAN ALGORITHM:

Also called euclid's algorithm used for computing GCD (Greatest Common Divisor) also known as HCF (Highest Common Factor). Here we recursively replace a = b, and b = a mod b till the value of b is zero so the current value in a will be the gcd.



QUESTION:

Find the gcd of (529, 123)

a	b	a mod b
529	123	37
123	37	12
37	12	1
12	1	0
1 ☜	0	X

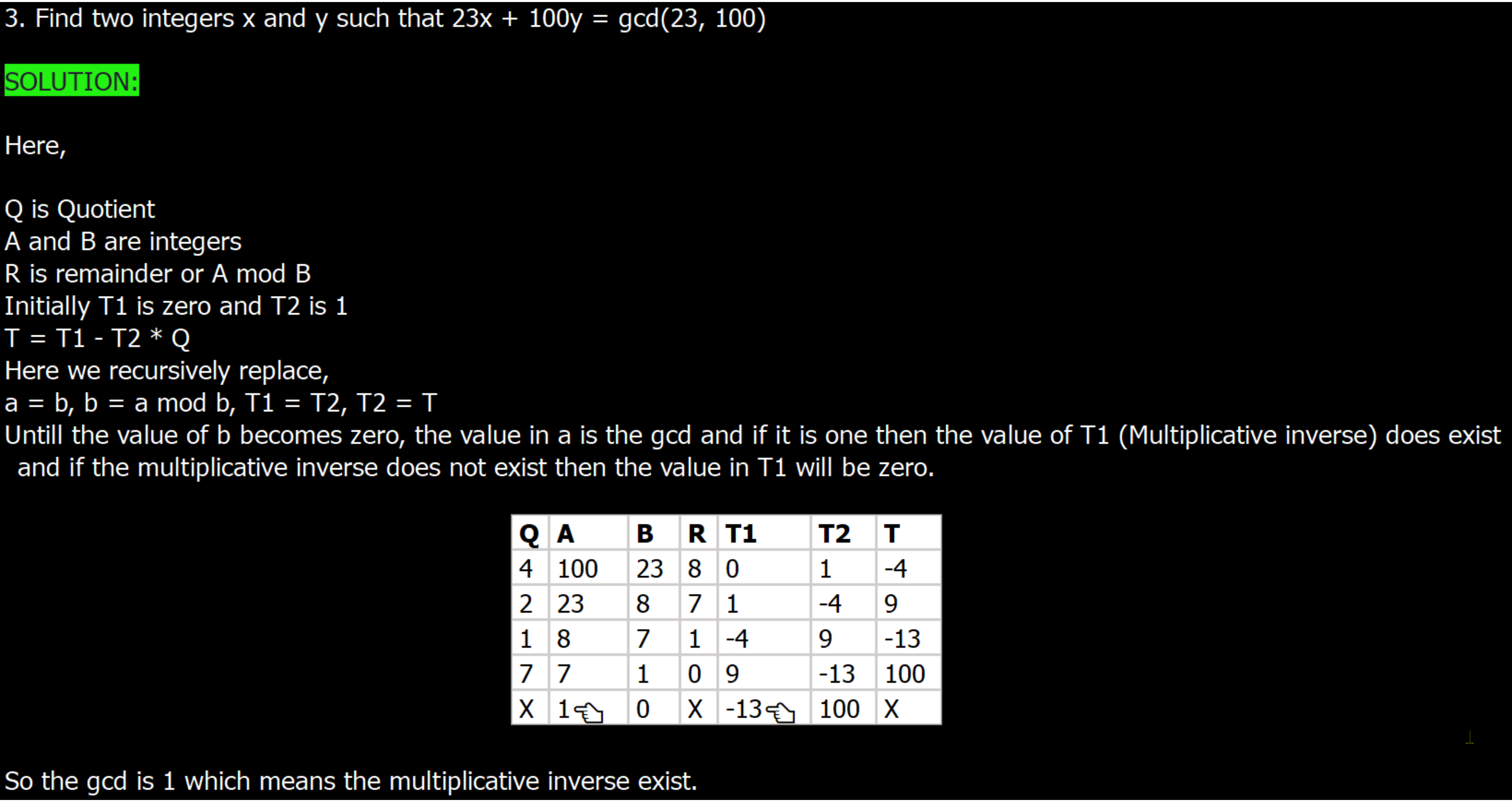
When b is zero, the current value in is the gcd. So the gcd of 529 and 123 is 1.

EXTENDED EUCLEDIAN ALGORITHM:

This algorithm is used to to find the multiplicative inverse of a number with respect to mod if it exists. It is called so because we extended the euclid's algorithm with 4 more columns, i.e: Q, T1, T2 and T. Also this algorithm can find the value of x and y if a and b are known using the formula a*x + b*y =gcd (a , b). Also gives the gcd of 2 numbers and

QUESTIONS:

1. Find the gcd of (23, 100) or 23 mod 100
2. Find the multiplicative inverse of 23 in Z100 (0 to 99, means the value sholuld be in Z100)or multiplicative inverse of 23 mod 100.



3. Find two integers x and y such that 23x + 100y = gcd(23, 100)

SOLUTION:

Here,

Q is Quotient
A and B are integers
R is remainder or A mod B
Initially T1 is zero and T2 is 1
T = T1 - T2 * Q
Here we recursively replace,
a = b, b = a mod b, T1 = T2, T2 = T
Untill the value of b becomes zero, the value in a is the gcd and if it is one then the value of T1 (Multiplicative inverse) does exist and if the multiplicative inverse does not exist then the value in T1 will be zero.

Q	A	B	R	T1	T2	T
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
X	1 ☜	0	X	-13 ☜	100	X

So the gcd is 1 which means the multiplicative inverse exist.

The multiplicative inverse of 23 mod 100 or 23 in Z100 is -13 or 87.
-13 is also the value of x.
To find the value of y, the formula is $23x + 100y = \gcd(23, 100)$
$23(-13) + 100y = 1$
$- 299 - 1 + 100y = 0$
$- 300 = -100y$
$y = 3$.

QUESTION:

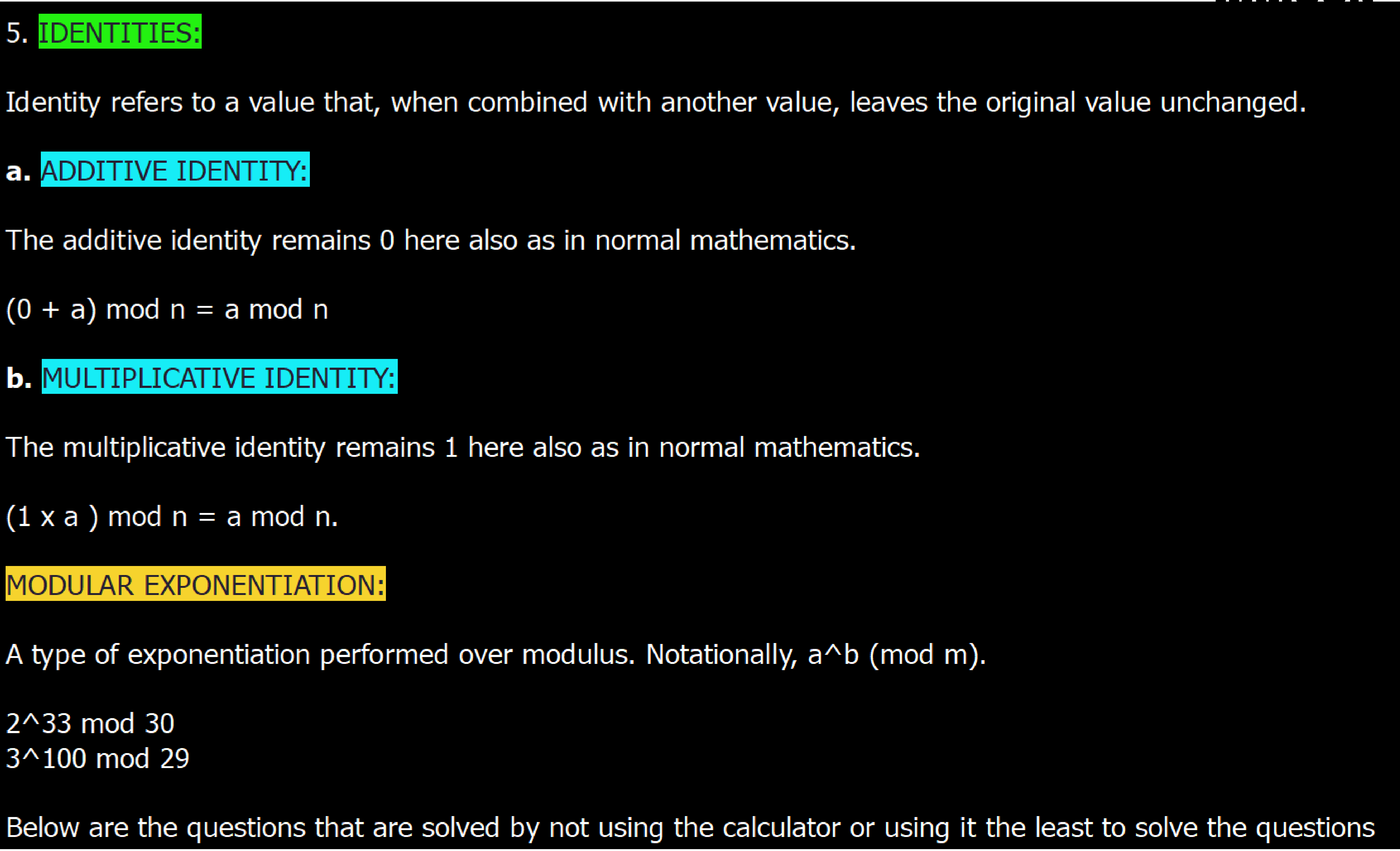
Find the multiplicative inverse of 10 mod 11

Q	A	B	R	T1	T2	T
1	11	10	1	0	1	-1
10	10	1	0	1	-1	11
X	1	0	X	-1	11	X

The multiplicative inverse of 10 mod 11 is -1 or 10 because -1 mod 11 is 10

Let's verify it,

10 * -1 is congruent to 1 mod 11
-10 is congruent to 1 mod 11.
10 * 10 mod 11 = 100 mod 11 .



5. IDENTITIES:

Identity refers to a value that, when combined with another value, leaves the original value unchanged.

a. ADDITIVE IDENTITY:

The additive identity remains 0 here also as in normal mathematics.

$(0 + a) \bmod n = a \bmod n$

b. MULTIPLICATIVE IDENTITY:

The multiplicative identity remains 1 here also as in normal mathematics.

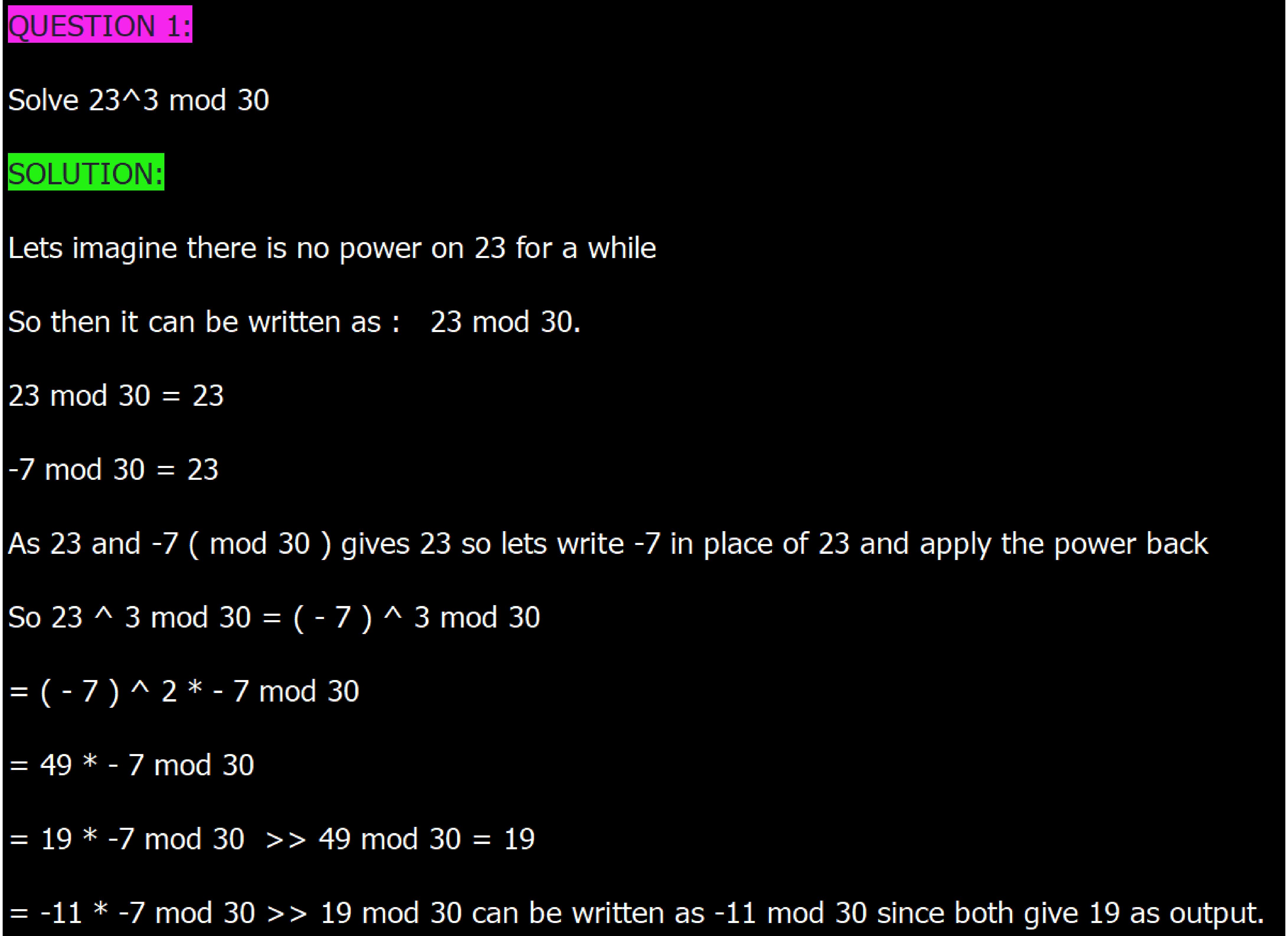
$(1 \times a) \bmod n = a \bmod n.$

MODULAR EXPONENTIATION:

A type of exponentiation performed over modulus. Notationally, a^b (mod m).

2^33 mod 30
3^100 mod 29

Below are the questions that are solved by not using the calculator or using it the least to solve the questions



QUESTION 1:

Solve 23^3 mod 30

SOLUTION:

Lets imagine there is no power on 23 for a while

So then it can be written as :   23 mod 30.

23 mod 30 = 23

-7 mod 30 = 23

As 23 and -7 (mod 30) gives 23 so lets write -7 in place of 23 and apply the power back

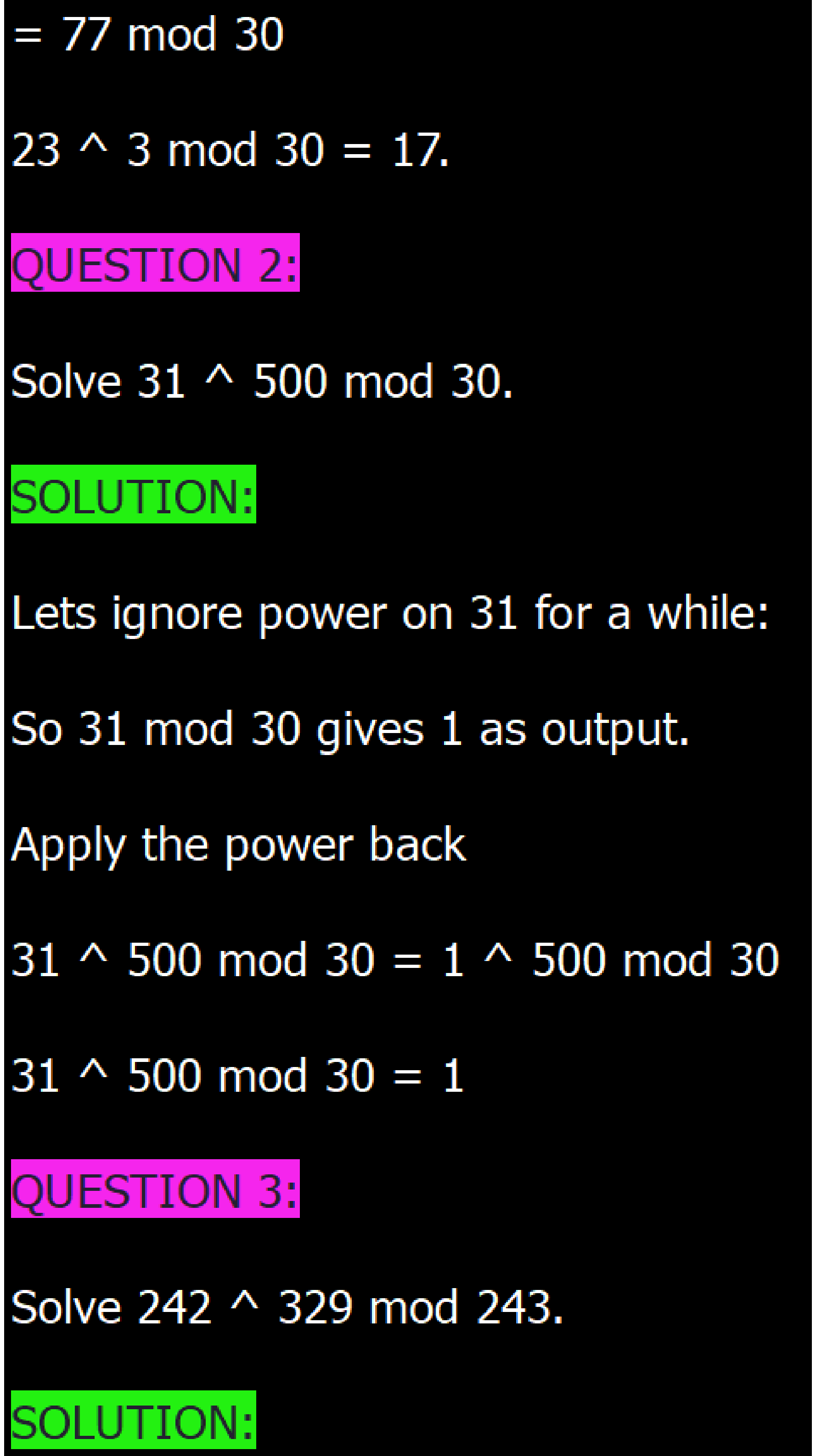
So 23 ^ 3 mod 30 = (- 7) ^ 3 mod 30

= (- 7) ^ 2 * - 7 mod 30

= 49 * - 7 mod 30

= 19 * -7 mod 30 >> 49 mod 30 = 19

= -11 * -7 mod 30 >> 19 mod 30 can be written as -11 mod 30 since both give 19 as output.



= 77 mod 30

23 ^ 3 mod 30 = 17.

QUESTION 2:

Solve 31 ^ 500 mod 30.

SOLUTION:

Lets ignore power on 31 for a while:

So 31 mod 30 gives 1 as output.

Apply the power back

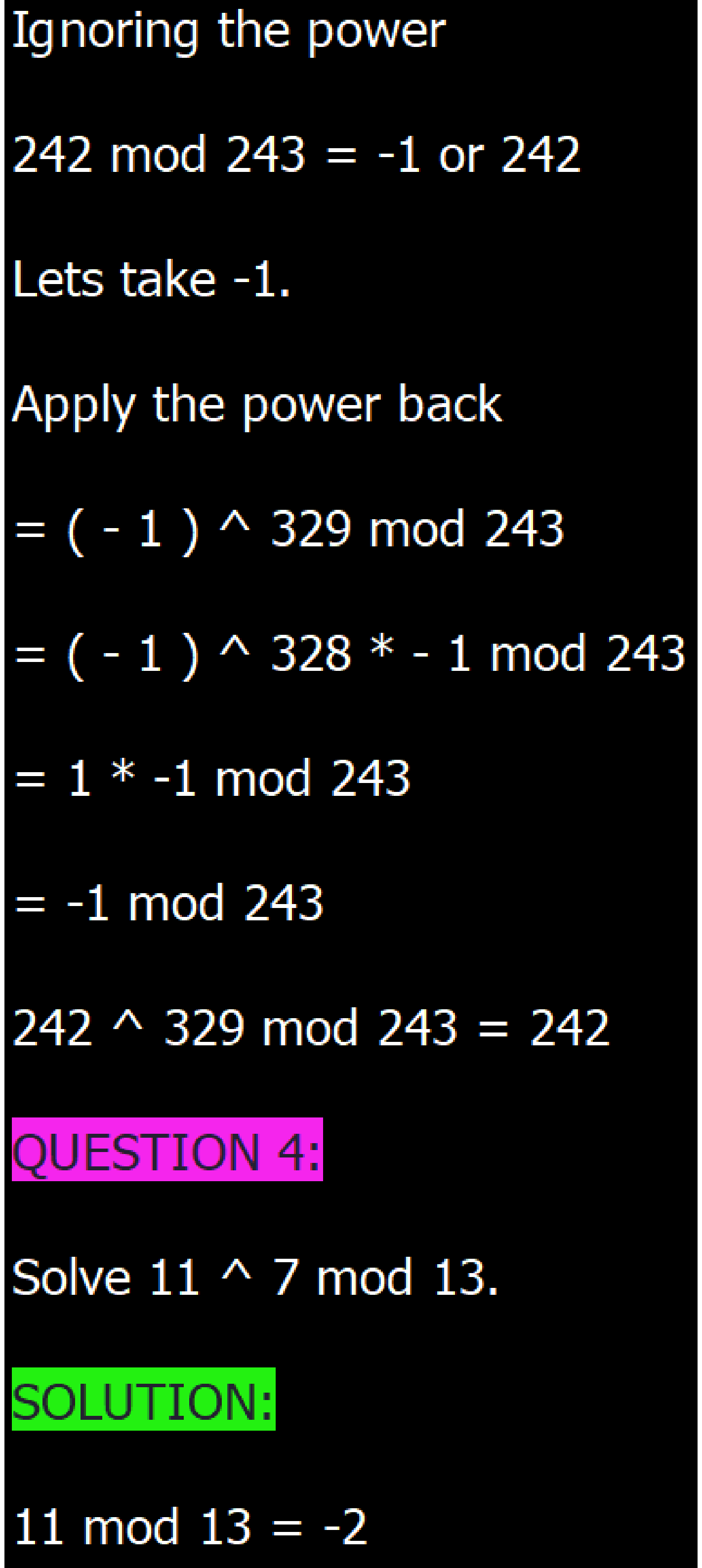
31 ^ 500 mod 30 = 1 ^ 500 mod 30

31 ^ 500 mod 30 = 1

QUESTION 3:

Solve 242 ^ 329 mod 243.

SOLUTION:



Ignoring the power

242 mod 243 = -1 or 242

Lets take -1.

Apply the power back

= (- 1) ^ 329 mod 243

= (- 1) ^ 328 * - 1 mod 243

= 1 * -1 mod 243

= -1 mod 243

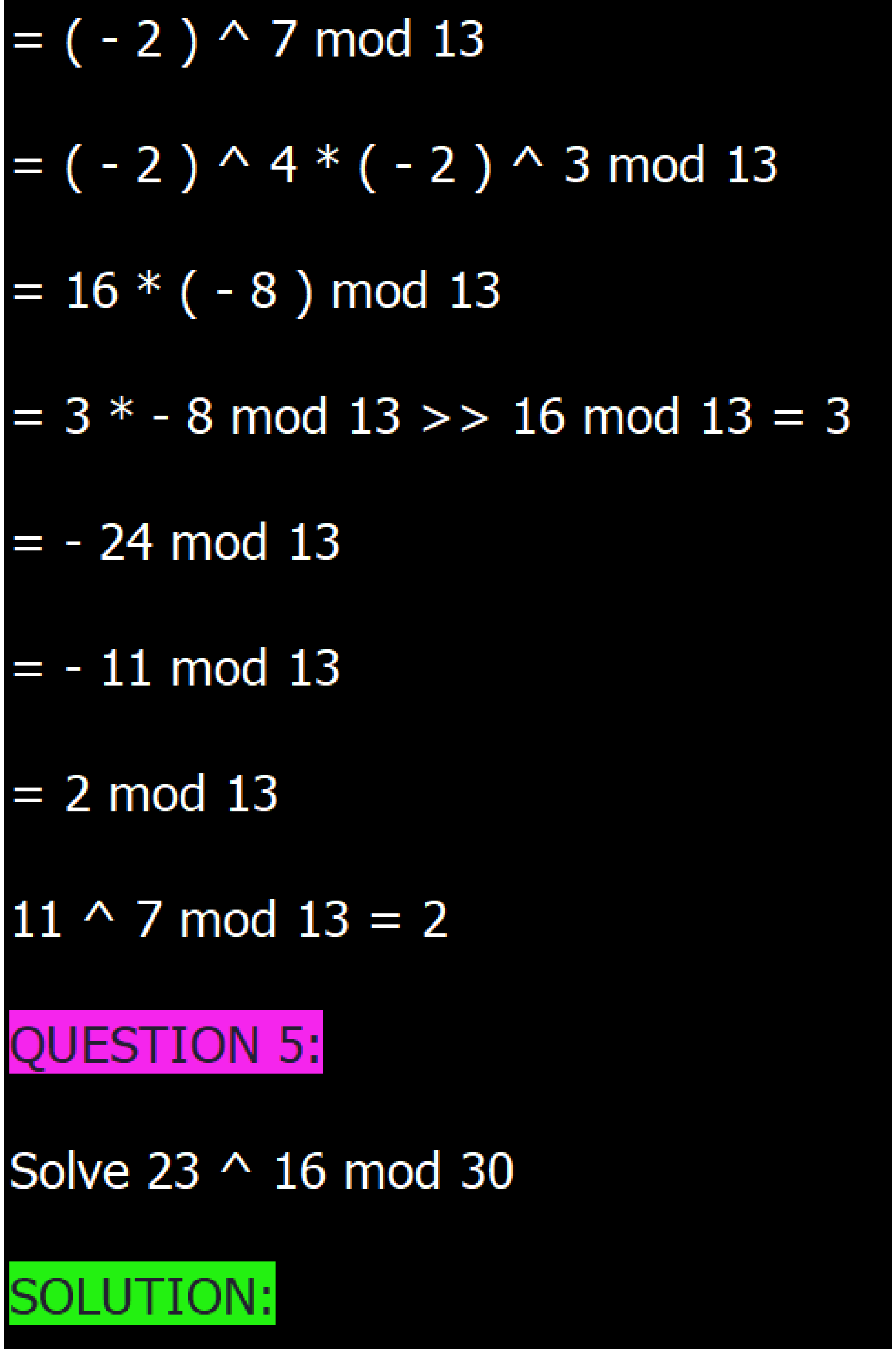
242 ^ 329 mod 243 = 242

QUESTION 4:

Solve 11 ^ 7 mod 13.

SOLUTION:

11 mod 13 = -2



= (- 2) ^ 7 mod 13

= (- 2) ^ 4 * (- 2) ^ 3 mod 13

= 16 * (- 8) mod 13

= 3 * - 8 mod 13 >> 16 mod 13 = 3

= - 24 mod 13

= - 11 mod 13

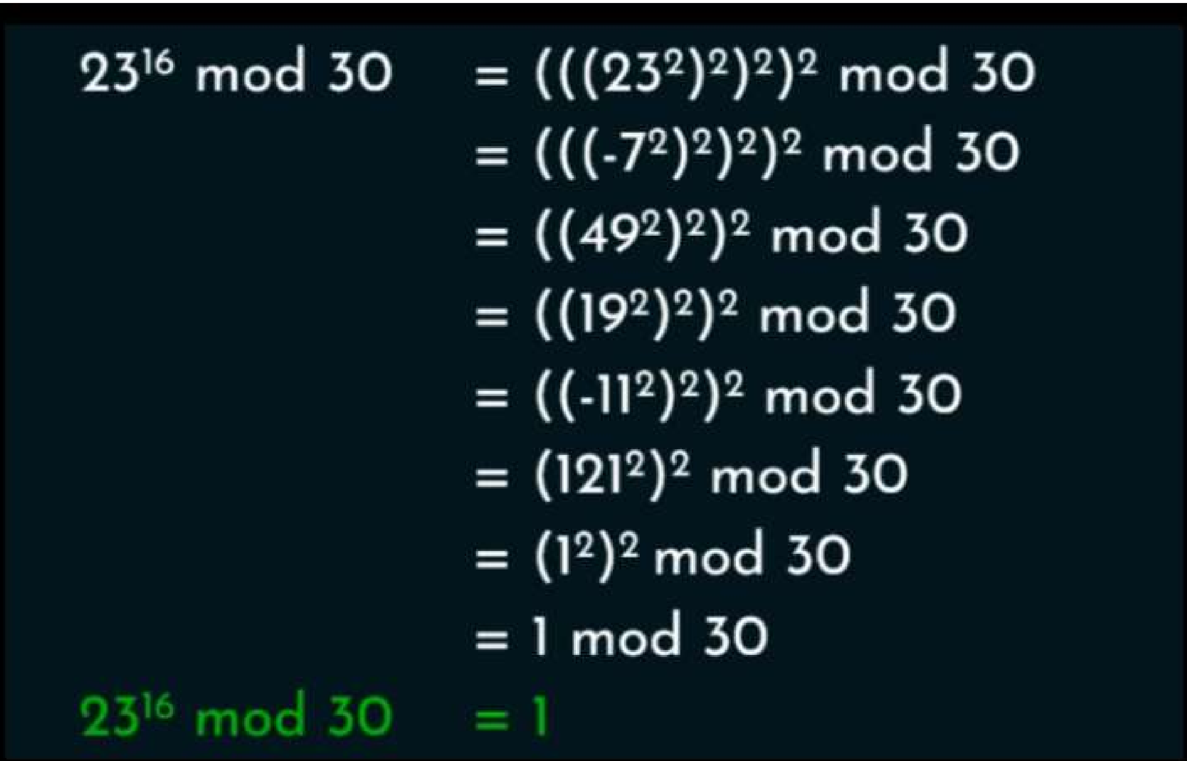
= 2 mod 13

11 ^ 7 mod 13 = 2

QUESTION 5:

Solve 23 ^ 16 mod 30

SOLUTION:

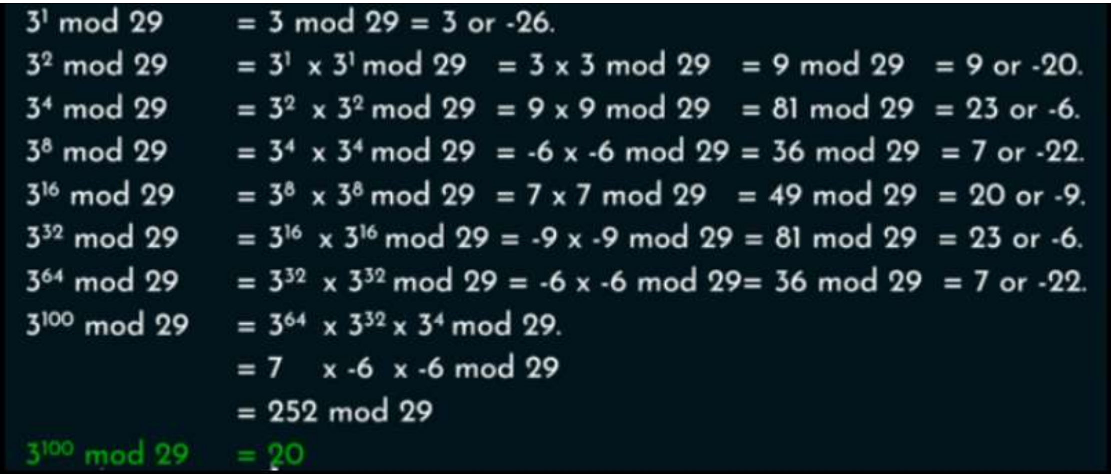


$$\begin{aligned}
23^{16} \bmod 30 &= (((23^2)^2)^2)^2 \bmod 30\\
&= (((-7^2)^2)^2)^2 \bmod 30\\
&= ((49^2)^2)^2 \bmod 30\\
&= ((19^2)^2)^2 \bmod 30\\
&= ((-11^2)^2)^2 \bmod 30\\
&= (121^2)^2 \bmod 30\\
&= (1^2)^2 \bmod 30\\
&= 1 \bmod 30\\
23^{16} \bmod 30 &= 1
\end{aligned}$$

QUESTION 6:

Solve 3 ^ 100 mod 29

SOLUTION:



3^{1} mod 29 = 3 mod 29 = 3 or -26.

3^{2} mod 29 = 3^{1} x 3^{1} mod 29 = 3 x 3 mod 29 = 9 mod 29 = 9 or -20.

3^{4} mod 29 = 3^{2} x 3^{2} mod 29 = 9 x 9 mod 29 = 81 mod 29 = 23 or -6.

3^{8} mod 29 = 3^{4} x 3^{4} mod 29 = -6 x -6 mod 29 = 36 mod 29 = 7 or -22.

3^{16} mod 29 = 3^{8} x 3^{8} mod 29 = 7 x 7 mod 29 = 49 mod 29 = 20 or -9.

3^{32} mod 29 = 3^{16} x 3^{16} mod 29 = -9 x -9 mod 29 = 81 mod 29 = 23 or -6.

3^{64} mod 29 = 3^{32} x 3^{32} mod 29 = -6 x -6 mod 29= 36 mod 29 = 7 or -22.

3^{100} mod 29 = 3^{64} x 3^{32} x 3^{4} mod 29.

= 7 x -6 x -6 mod 29

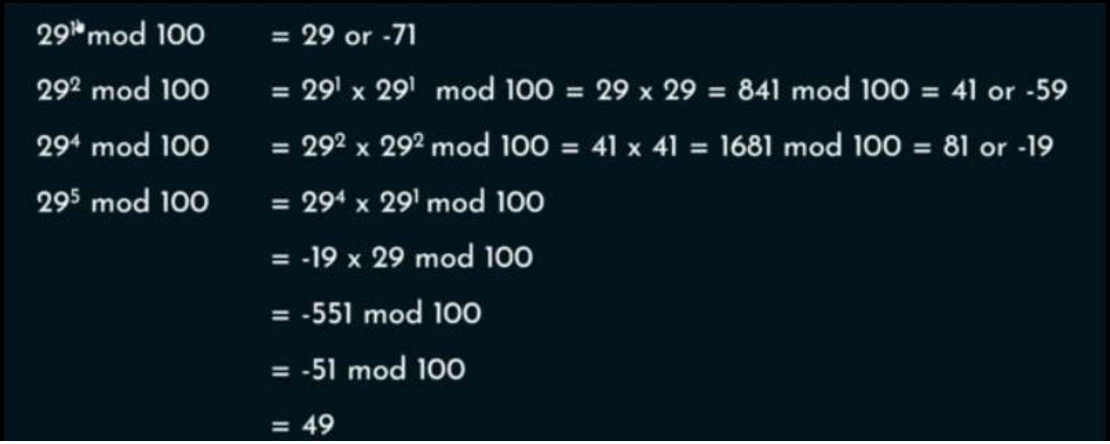
= 252 mod 29

3^{100} mod 29 = 20

QUESTION 7:

What are the last 2 digits of 29 ^ 5 ?

SOLUTION:



29^{1}mod 100 = 29 or -71

29^{2} mod 100 = 29^{1} x 29^{1} mod 100 = 29 x 29 = 841 mod 100 = 41 or -59

29^{4} mod 100 = 29^{2} x 29^{2} mod 100 = 41 x 41 = 1681 mod 100 = 81 or -19

29^{5} mod 100 = 29^{4} x 29^{1} mod 100

= -19 x 29 mod 100

= -551 mod 100

= -51 mod 100

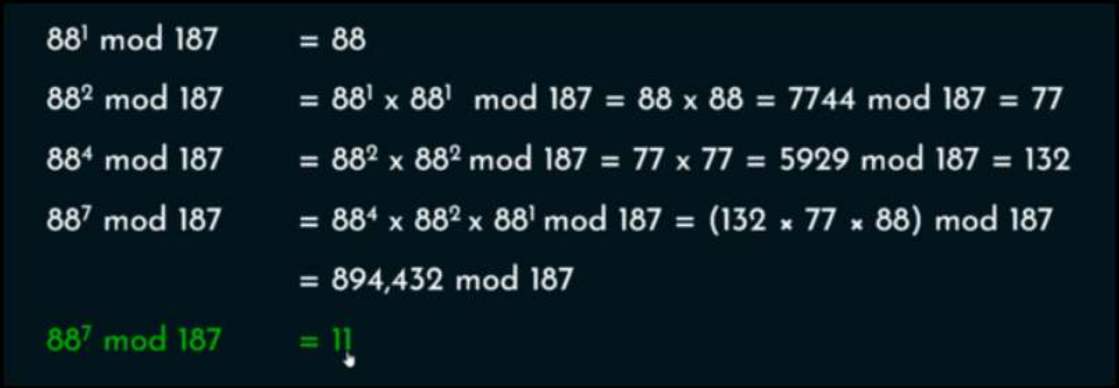
= 49

So the last 2 digits are 4 and 9.

QUESTION 8:

Solve 88 ^ 7 mod 187

SOLUTION:



$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 88^1 \times 88^1 \bmod 187 = 88 \times 88 = 7744 \bmod 187 = 77$

$88^4 \bmod 187 = 88^2 \times 88^2 \bmod 187 = 77 \times 77 = 5929 \bmod 187 = 132$

$88^7 \bmod 187 = 88^4 \times 88^2 \times 88^1 \bmod 187 = (132 \times 77 \times 88) \bmod 187$

$= 894{,}432 \bmod 187$

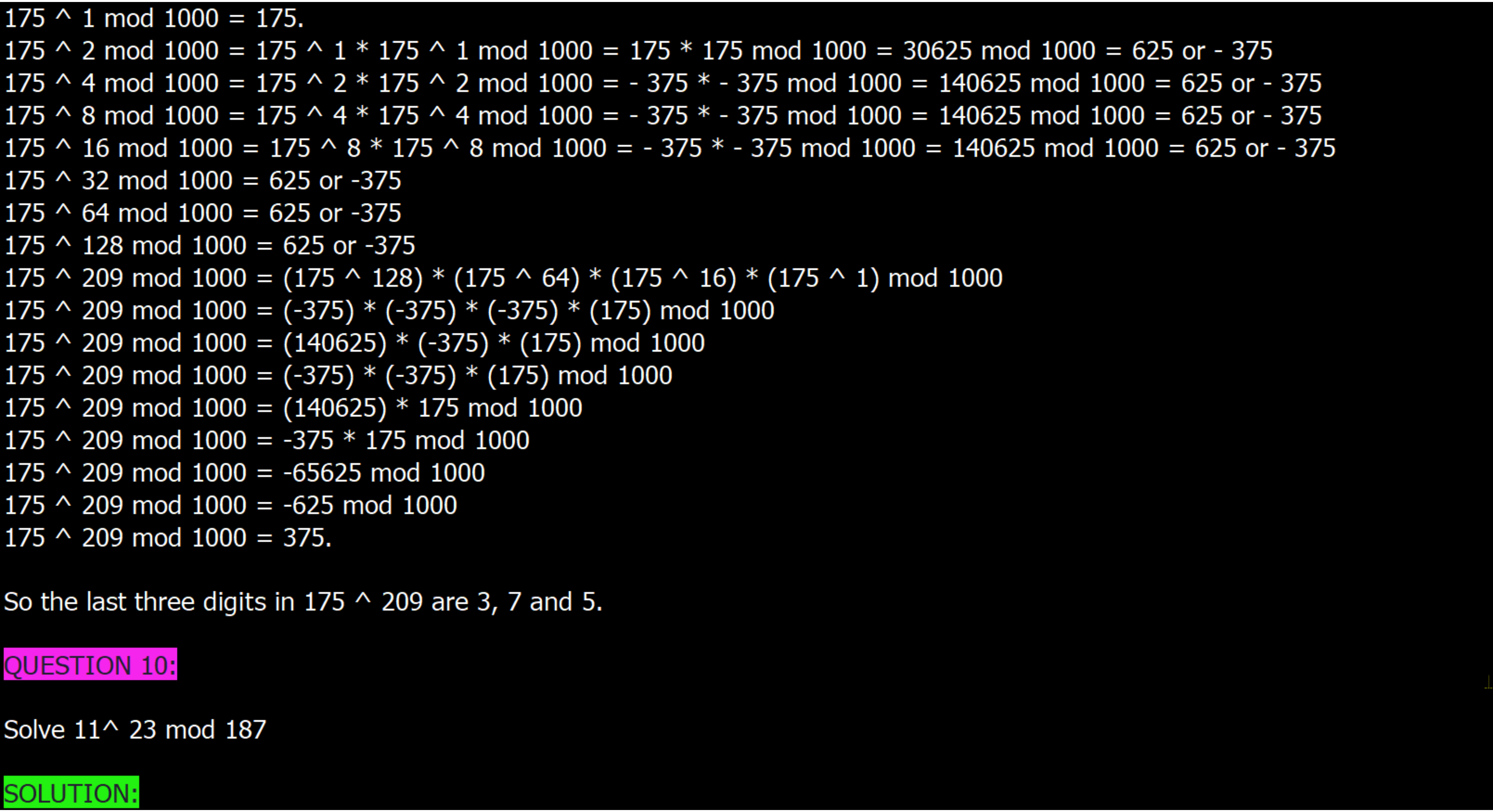
$88^7 \bmod 187 = 11$

QUESTION 9:

What are the last 3 digits of 175 ^ 209

SOLUTION:

175 ^ 209 mod 1000



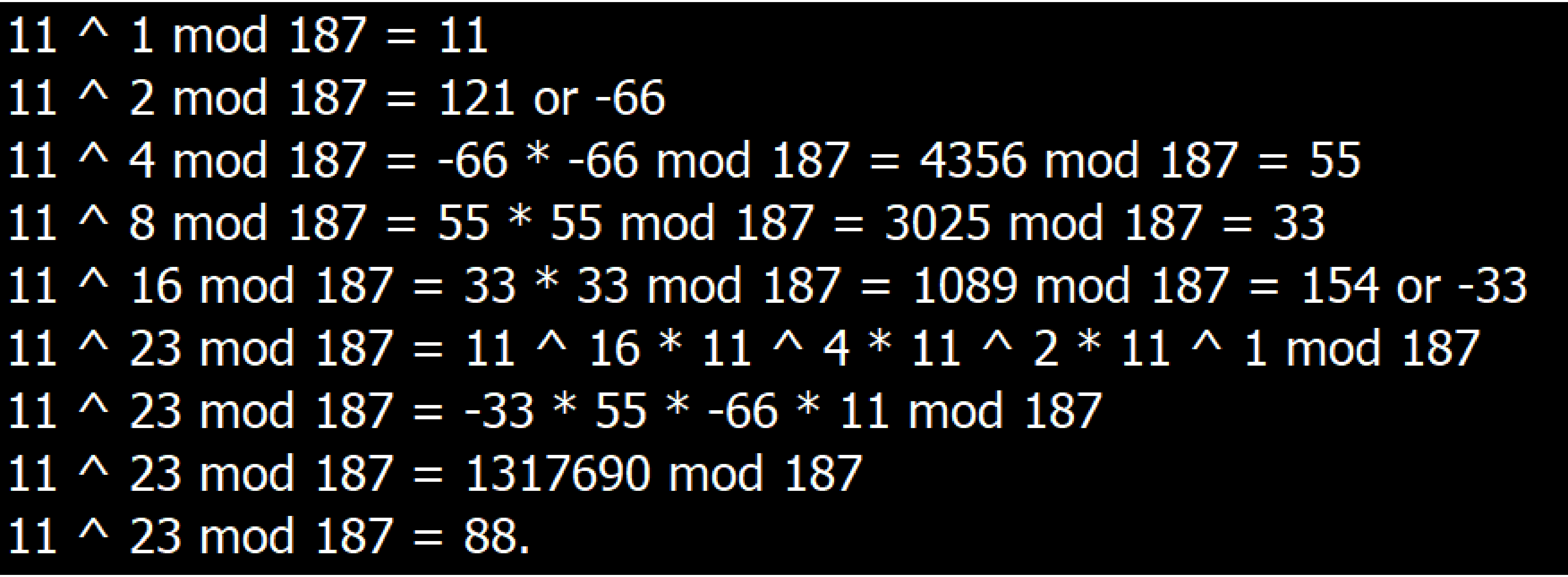
175 ^ 1 mod 1000 = 175.
175 ^ 2 mod 1000 = 175 ^ 1 * 175 ^ 1 mod 1000 = 175 * 175 mod 1000 = 30625 mod 1000 = 625 or - 375
175 ^ 4 mod 1000 = 175 ^ 2 * 175 ^ 2 mod 1000 = - 375 * - 375 mod 1000 = 140625 mod 1000 = 625 or - 375
175 ^ 8 mod 1000 = 175 ^ 4 * 175 ^ 4 mod 1000 = - 375 * - 375 mod 1000 = 140625 mod 1000 = 625 or - 375
175 ^ 16 mod 1000 = 175 ^ 8 * 175 ^ 8 mod 1000 = - 375 * - 375 mod 1000 = 140625 mod 1000 = 625 or - 375
175 ^ 32 mod 1000 = 625 or -375
175 ^ 64 mod 1000 = 625 or -375
175 ^ 128 mod 1000 = 625 or -375
175 ^ 209 mod 1000 = (175 ^ 128) * (175 ^ 64) * (175 ^ 16) * (175 ^ 1) mod 1000
175 ^ 209 mod 1000 = (-375) * (-375) * (-375) * (175) mod 1000
175 ^ 209 mod 1000 = (140625) * (-375) * (175) mod 1000
175 ^ 209 mod 1000 = (-375) * (-375) * (175) mod 1000
175 ^ 209 mod 1000 = (140625) * 175 mod 1000
175 ^ 209 mod 1000 = -375 * 175 mod 1000
175 ^ 209 mod 1000 = -65625 mod 1000
175 ^ 209 mod 1000 = -625 mod 1000
175 ^ 209 mod 1000 = 375.

So the last three digits in 175 ^ 209 are 3, 7 and 5.

QUESTION 10:

Solve 11^ 23 mod 187

SOLUTION:



11 ^ 1 mod 187 = 11

11 ^ 2 mod 187 = 121 or -66

11 ^ 4 mod 187 = -66 * -66 mod 187 = 4356 mod 187 = 55

11 ^ 8 mod 187 = 55 * 55 mod 187 = 3025 mod 187 = 33

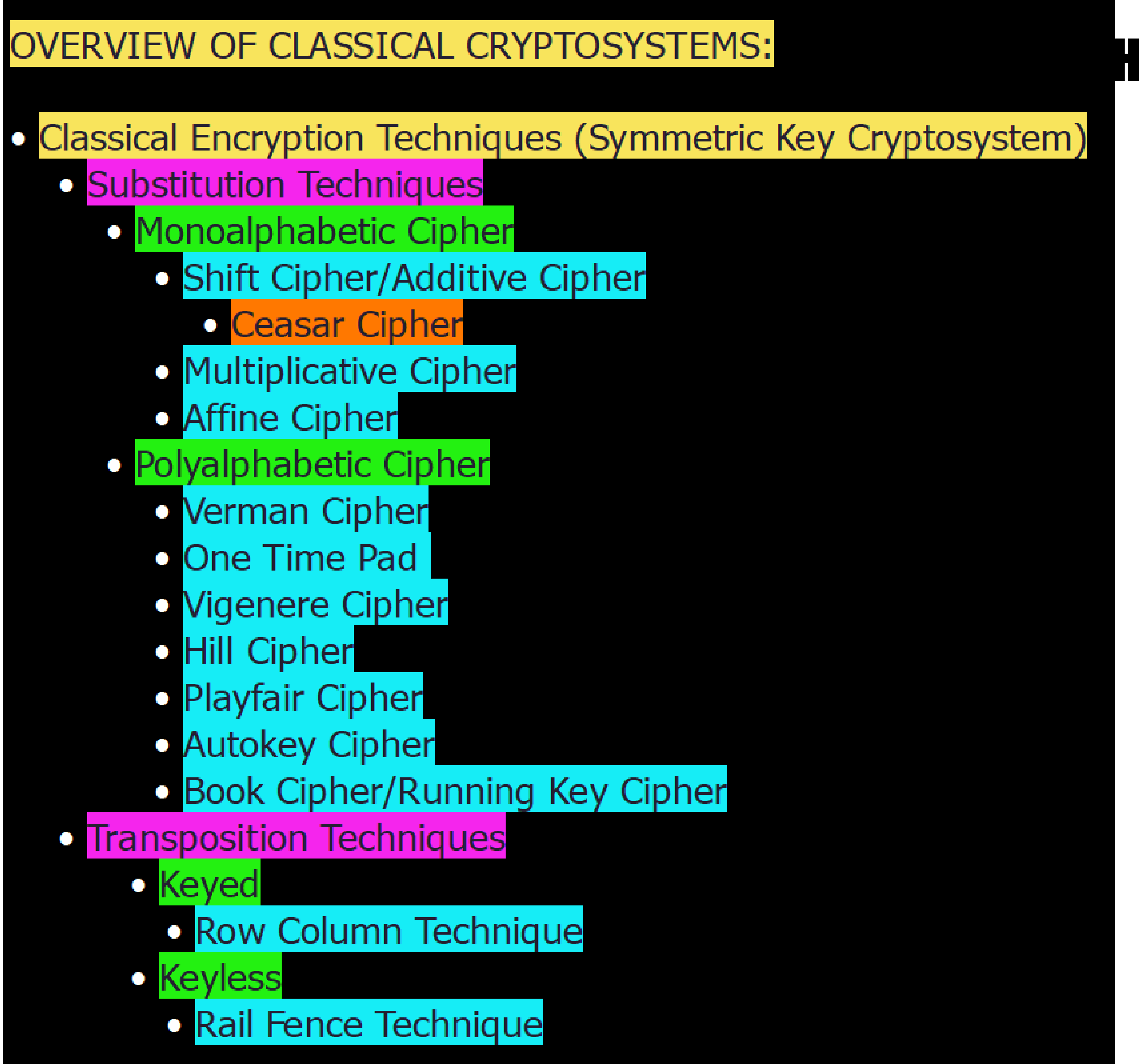
11 ^ 16 mod 187 = 33 * 33 mod 187 = 1089 mod 187 = 154 or -33

11 ^ 23 mod 187 = 11 ^ 16 * 11 ^ 4 * 11 ^ 2 * 11 ^ 1 mod 187

11 ^ 23 mod 187 = -33 * 55 * -66 * 11 mod 187

11 ^ 23 mod 187 = 1317690 mod 187

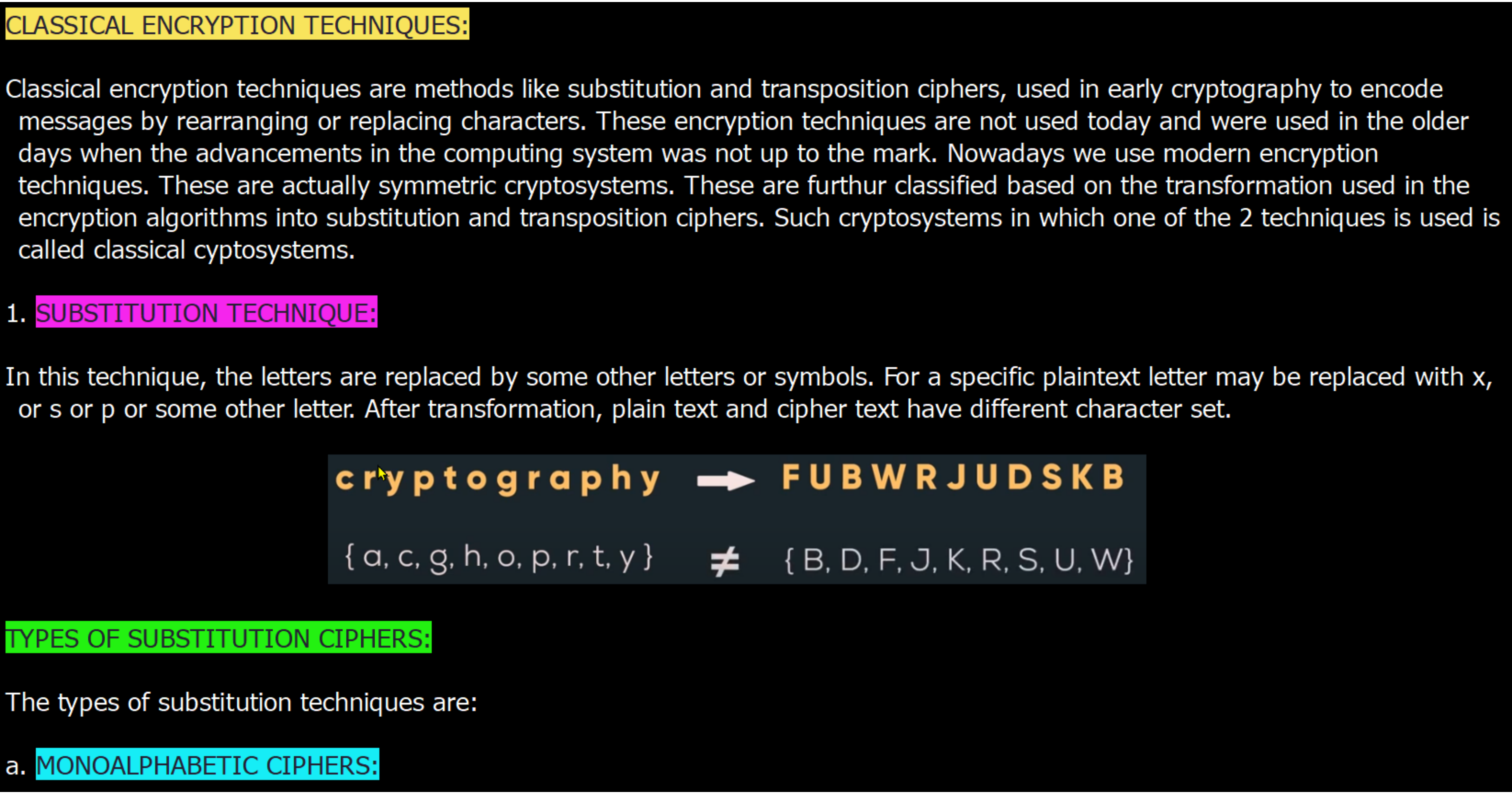
11 ^ 23 mod 187 = 88.



OVERVIEW OF CLASSICAL CRYPTOSYSTEMS:

- Classical Encryption Techniques (Symmetric Key Cryptosystem)
  - Substitution Techniques
    - Monoalphabetic Cipher
      - Shift Cipher/Additive Cipher
        - Ceasar Cipher
      - Multiplicative Cipher
      - Affine Cipher
    - Polyalphabetic Cipher
      - Verman Cipher
      - One Time Pad
      - Vigenere Cipher
      - Hill Cipher
      - Playfair Cipher
      - Autokey Cipher
      - Book Cipher/Running Key Cipher
  - Transposition Techniques
    - Keyed
      - Row Column Technique
    - Keyless
      - Rail Fence Technique

HAROON



CLASSICAL ENCRYPTION TECHNIQUES:

Classical encryption techniques are methods like substitution and transposition ciphers, used in early cryptography to encode messages by rearranging or replacing characters. These encryption techniques are not used today and were used in the older days when the advancements in the computing system was not up to the mark. Nowadays we use modern encryption techniques. These are actually symmetric cryptosystems. These are furthur classified based on the transformation used in the encryption algorithms into substitution and transposition ciphers. Such cryptosystems in which one of the 2 techniques is used is called classical cyptosystems.

1. SUBSTITUTION TECHNIQUE:

In this technique, the letters are replaced by some other letters or symbols. For a specific plaintext letter may be replaced with x, or s or p or some other letter. After transformation, plain text and cipher text have different character set.

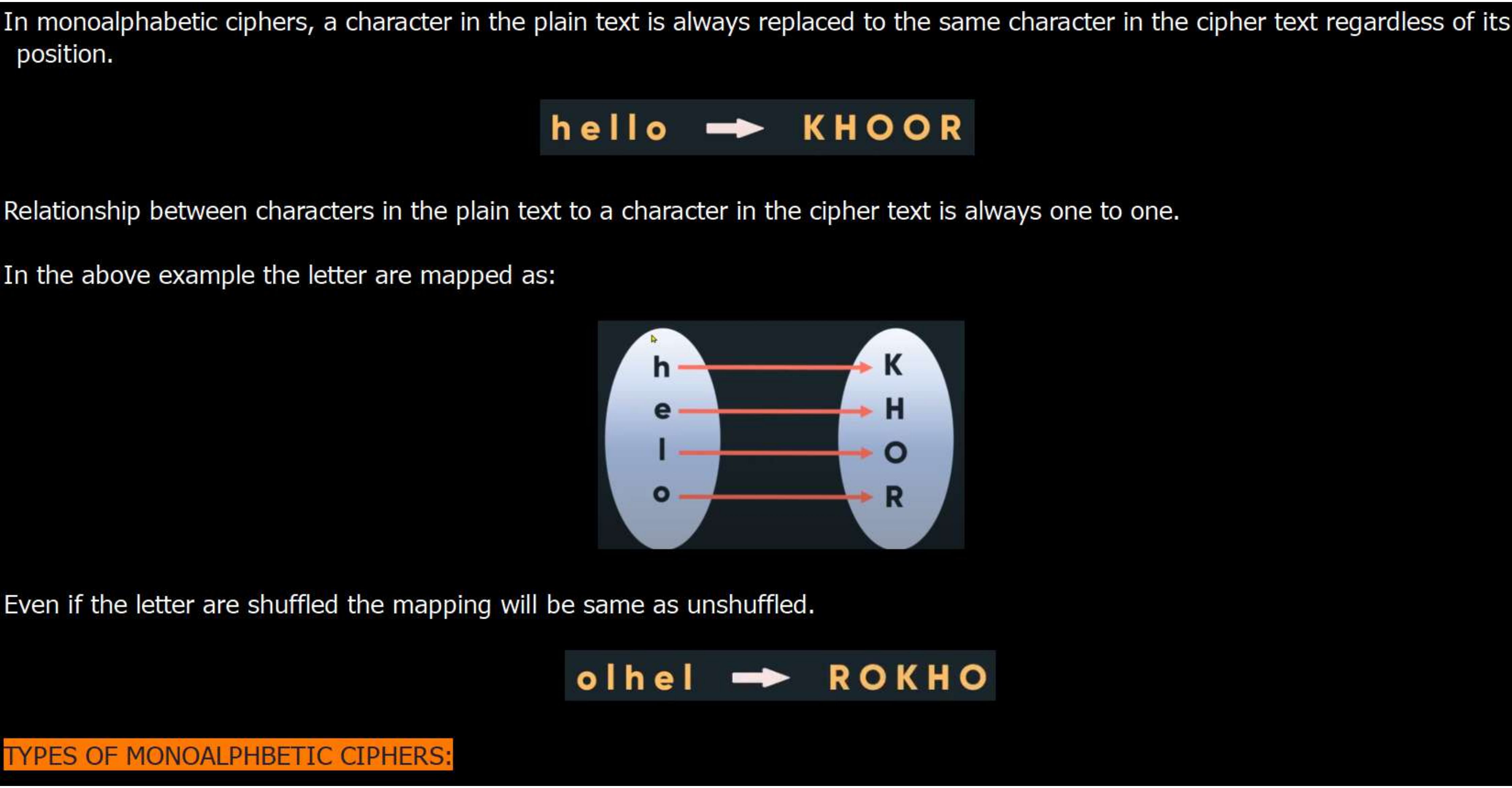
cryptography → FUBWRJUDSKB

{ a, c, g, h, o, p, r, t, y } ≠ { B, D, F, J, K, R, S, U, W}

TYPES OF SUBSTITUTION CIPHERS:

The types of substitution techniques are:

a. MONOALPHABETIC CIPHERS:



In monoalphabetic ciphers, a character in the plain text is always replaced to the same character in the cipher text regardless of its position.

hello → KHOOR

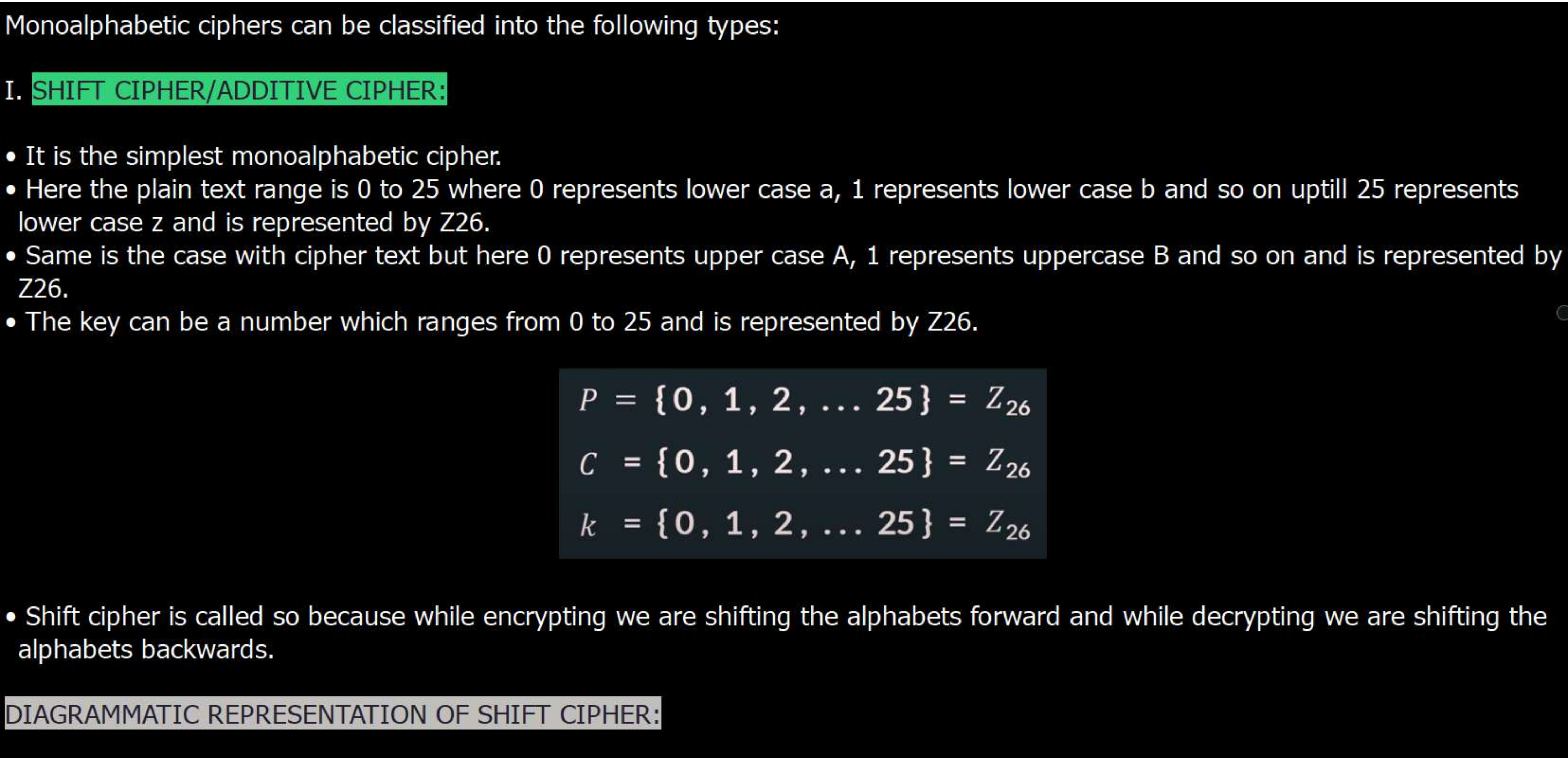
Relationship between characters in the plain text to a character in the cipher text is always one to one.

In the above example the letter are mapped as:

Even if the letter are shuffled the mapping will be same as unshuffled.

olhel → ROKHO

TYPES OF MONOALPHBETIC CIPHERS:



Monoalphabetic ciphers can be classified into the following types:

I. SHIFT CIPHER/ADDITIVE CIPHER:

- It is the simplest monoalphabetic cipher.
- Here the plain text range is 0 to 25 where 0 represents lower case a, 1 represents lower case b and so on uptill 25 represents lower case z and is represented by Z26.
- Same is the case with cipher text but here 0 represents upper case A, 1 represents uppercase B and so on and is represented by Z26.
- The key can be a number which ranges from 0 to 25 and is represented by Z26.

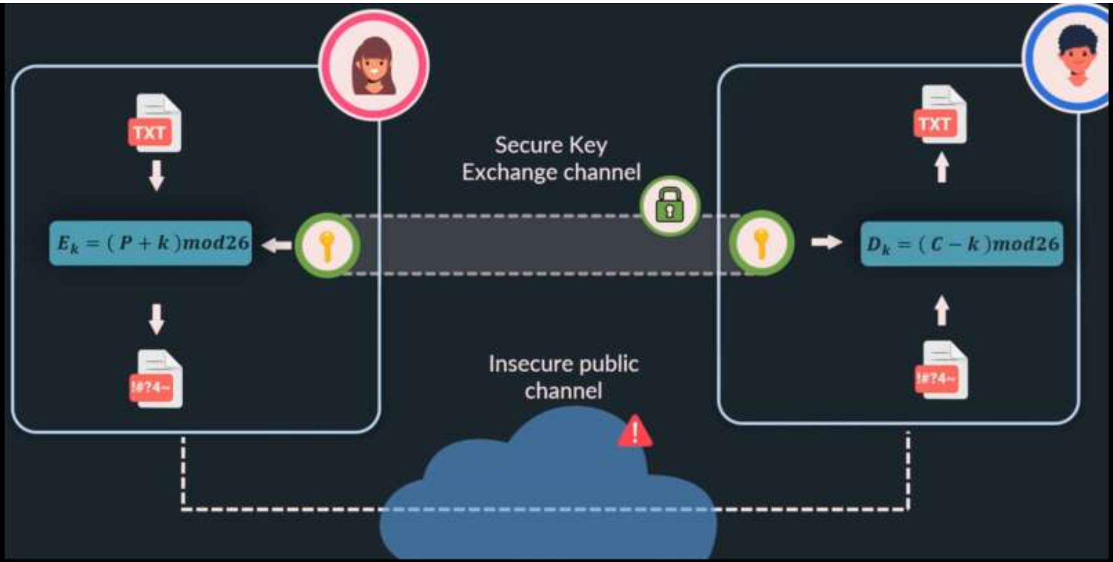
$$P = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$C = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$k = \{0, 1, 2, \ldots 25\} = Z_{26}$$

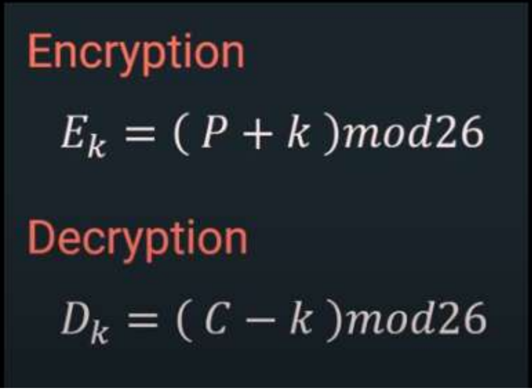
- Shift cipher is called so because while encrypting we are shifting the alphabets forward and while decrypting we are shifting the alphabets backwards.

DIAGRAMMATIC REPRESENTATION OF SHIFT CIPHER:



ENCRYPTION AND DECRYPTION OF SHIFT CIPHER:

The formula for encrypting and decrypting the plain text using shift cipher are as follows:



Encryption

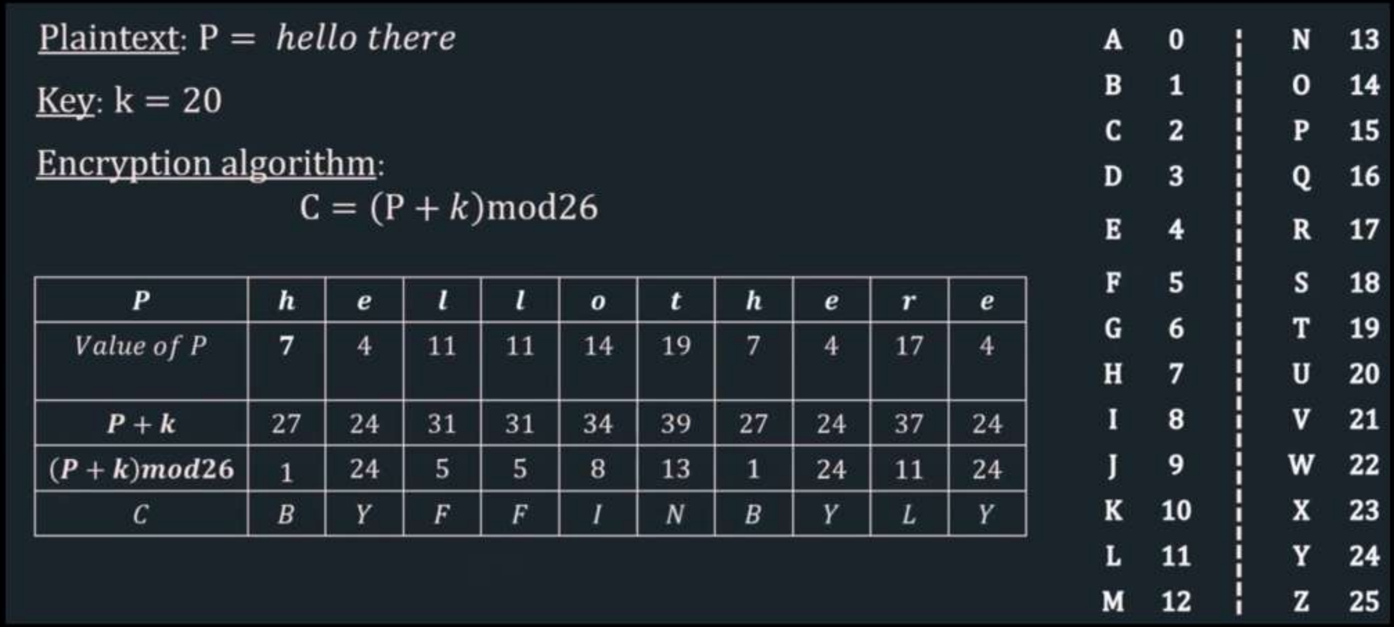
$$E_k = (P + k)mod26$$

Decryption

$$D_k = (C - k)mod26$$

QUESTION 1:

Encrypt the message "hello there" using shift cipher/ additive cipher using the key 20.



Plaintext: P = *hello there*

Key: k = 20

Encryption algorithm:

$$C = (P + k)\text{mod}26$$

P	h	e	l	l	o	t	h	e	r	e
Value of P	7	4	11	11	14	19	7	4	17	4
$P + k$	27	24	31	31	34	39	27	24	37	24
$(P + k)mod26$	1	24	5	5	8	13	1	24	11	24
C	B	Y	F	F	I	N	B	Y	L	Y

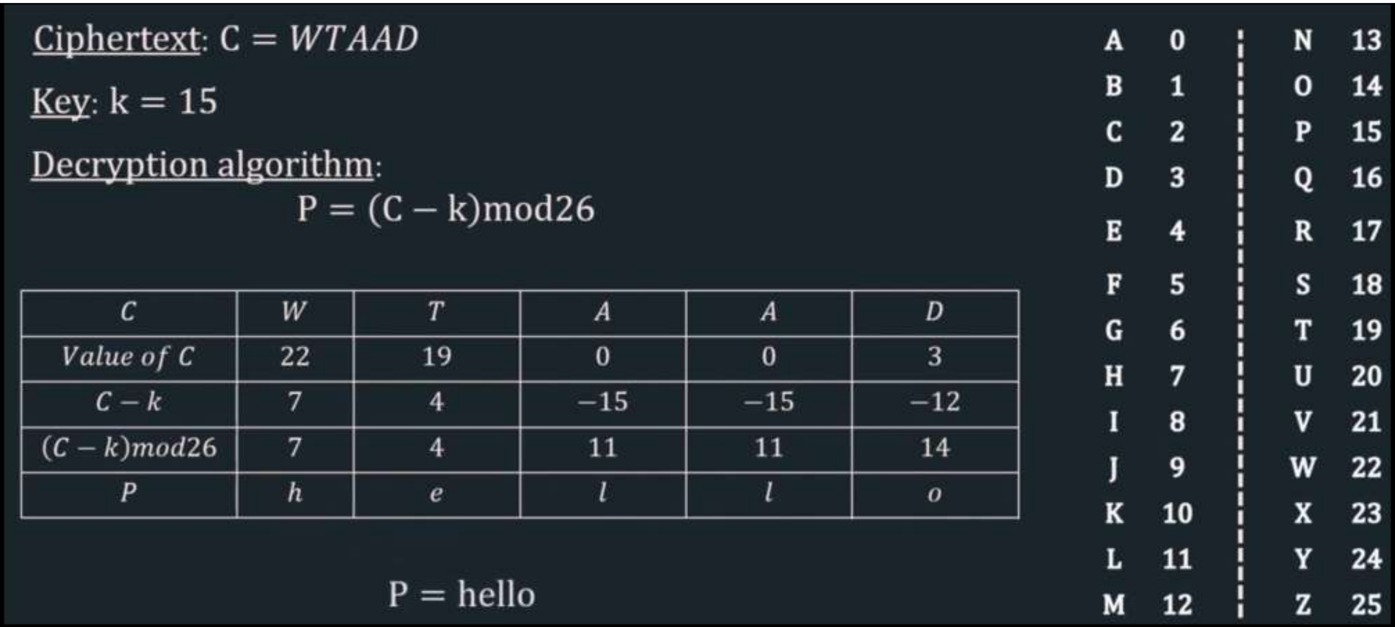
A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

So the cipher text is "BYFFI NBYLY".

The spaces are included on the ciphertext according to the plain text.

QUESTION 2:

Decrypt the ciphertext "WTAAD" using additive cipher with the key value 15.



Ciphertext: C = $WTAAD$

Key: k = 15

Decryption algorithm:

$$P = (C - k)\bmod 26$$

C	W	T	A	A	D
$Value\ of\ C$	22	19	0	0	3
$C-k$	7	4	−15	−15	−12
$(C-k)mod26$	7	4	11	11	14
P	h	e	l	l	o

P = hello

A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

So the plain text is "hello".

CRYPTANALYSIS OF SHIFT CIPHER:

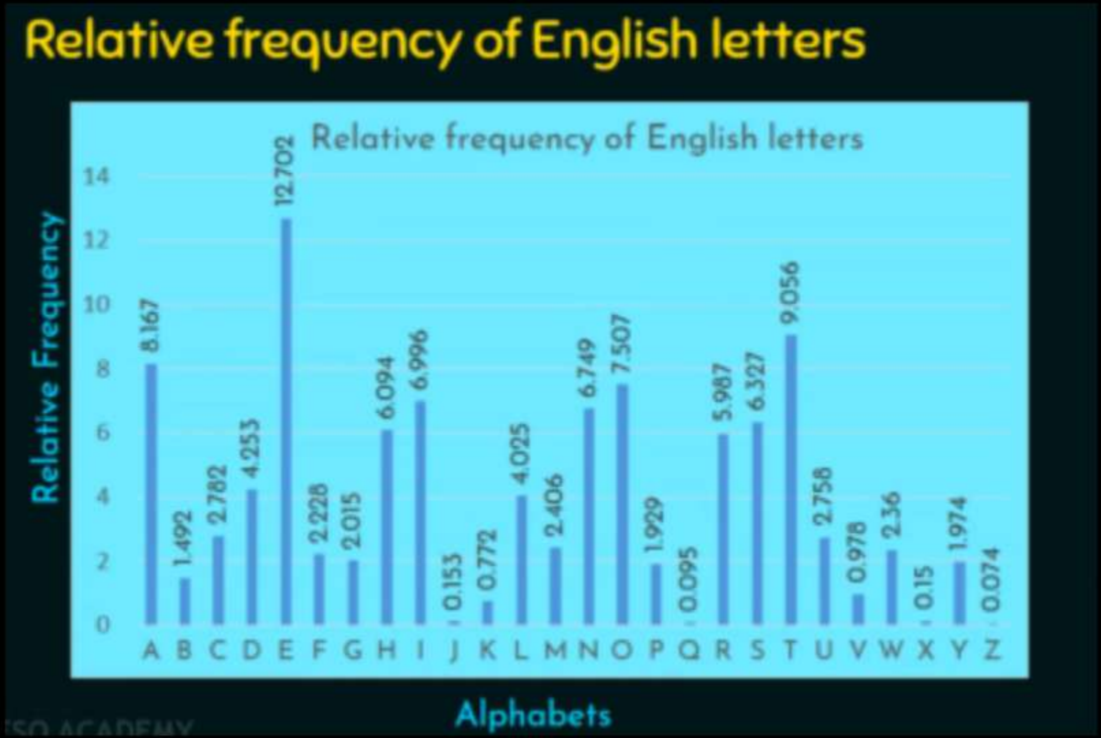
Shift cipher is vulnerable to attacks like brute force and statistical attack.

BRUTE FORCE ATTACK:

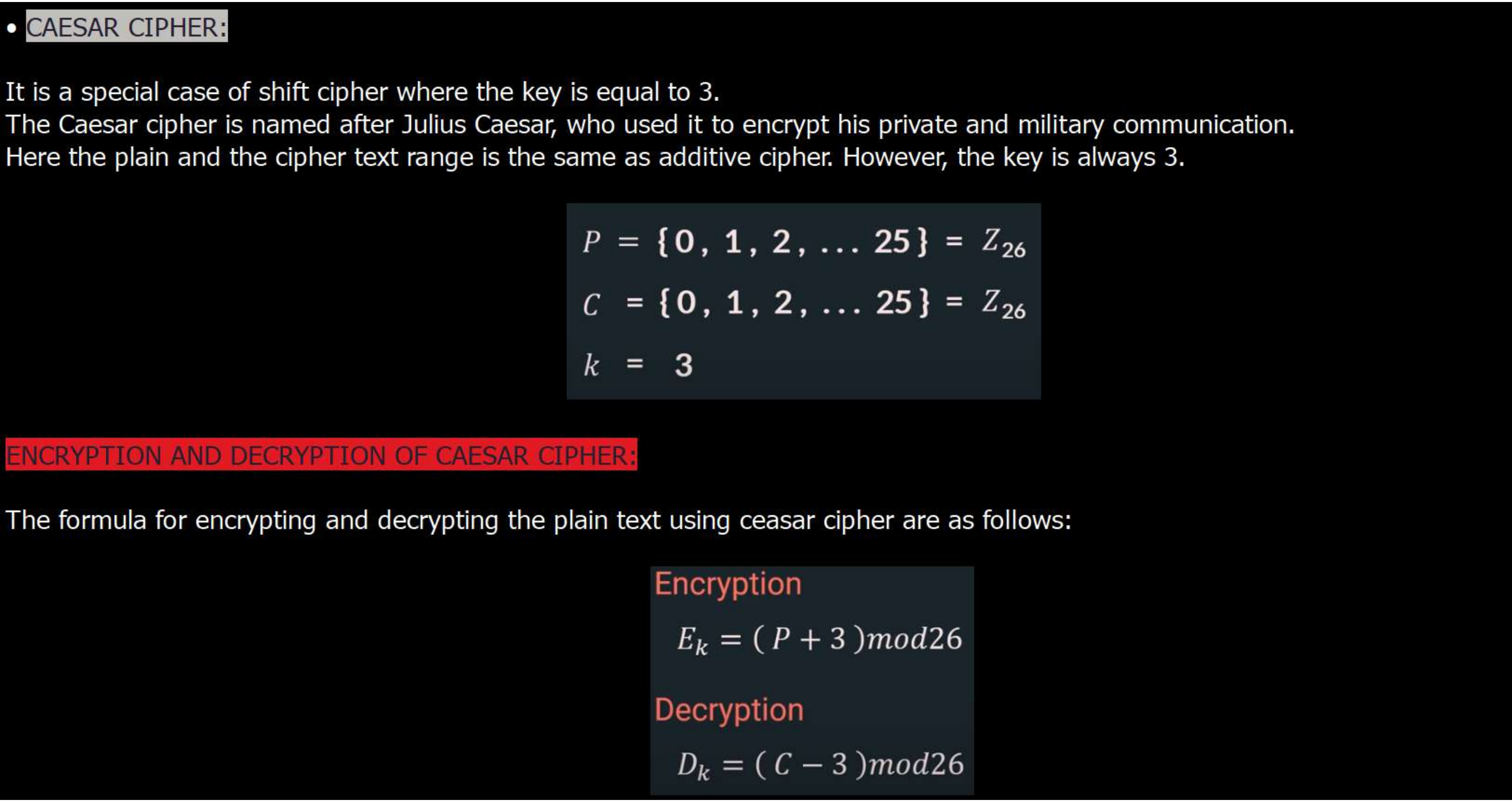
As we know that the key space is 0 to 25. So attacker can try all the 26 keys and easily find the plain text.

STATISTICAL ATTACK:

Attackers here uses the frequency of occurence of the cahracter in the english language. i.e: replacing the frequent letter in the ciphertext with "E" as so on.



We can decide the numbering by ourself. its not necessary that A is always denoted by 0 and so is the case with other letter but in sequence. We can start our counting by assigning A as 1, B as 2, even in the key as well.



- CAESAR CIPHER:

It is a special case of shift cipher where the key is equal to 3.
The Caesar cipher is named after Julius Caesar, who used it to encrypt his private and military communication.
Here the plain and the cipher text range is the same as additive cipher. However, the key is always 3.

$$P = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$C = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$k = 3$$

ENCRYPTION AND DECRYPTION OF CAESAR CIPHER:

The formula for encrypting and decrypting the plain text using ceasar cipher are as follows:

Encryption

$$E_k = (P + 3) mod 26$$

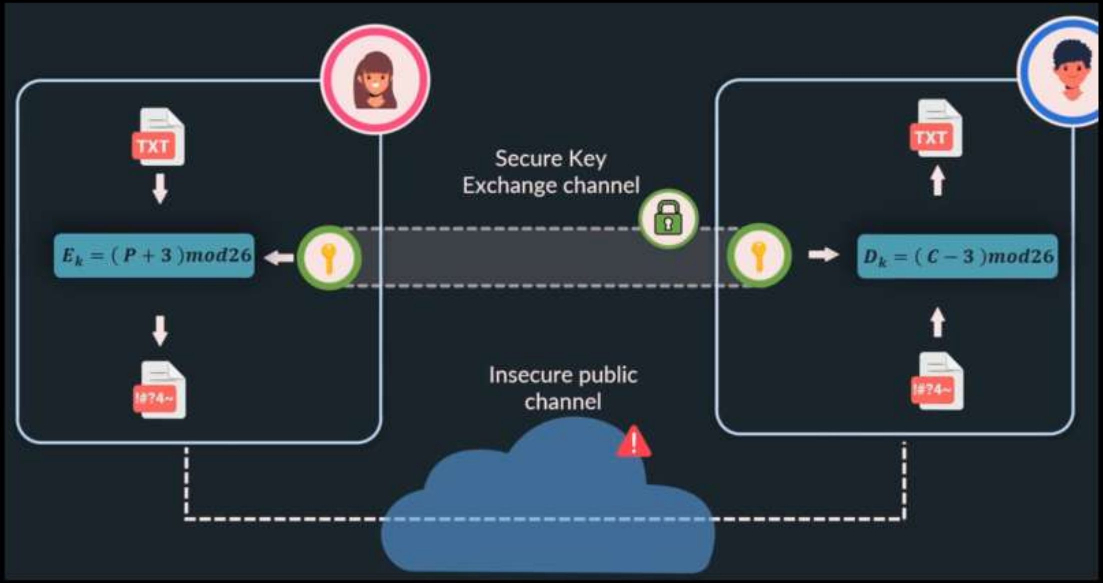
Decryption

$$D_k = (C - 3) mod 26$$

If we are encrypting a letter say z, then if mod26 is not present we will not be able to encrypt that because the range finishes at z.

DIAGRAMMATIC REPRESENTATION OF CAESAR CIPHER:

Below is the diagrammatic representation of caesar cipher



QUESTION 1:

Encrypt "haroon" using ceasar cipher.

SOLUTION: