Assignment 2

1.11. Is $4^{1536} - 9^{4824}$ divisible by 35?

Soln

* Let $N = 4^{1536} - 9^{4824}$ ------ (1)

* 35 is a Multiple of two prime Numbers 5 and 7. We need to check whether N value is disvisible by 5 and 7 seperately.

Step 1 - check N is divisible by 5:

$\rightarrow 4^2 \equiv 1 \mod 5$

$\rightarrow 4^{1536} = 4^{2 \cdot 768} = (4^2)^{768}$

$\rightarrow 4^{1536} = (1 \mod 5)^{768}$

$\cdot 1 \mod 5 = 1$

$\rightarrow 4^{1536} = (1)^{768}$

$= 1$ ---------- (2)

Therefore the value of 4^{1536} is 1

$\rightarrow 9^{4824} = 9^{2 \times 2412} = (9^2)^{2412}$

$\rightarrow 9^2 \equiv 1 \mod 5$

$\rightarrow 9^{4824} = (1 \mod 5)^{2412}$

$= (1)^{2412} = 1$ ---- (3)

$$N = 4^{1536} - 9^{4824}$$

$$= 1 - 1$$

$$= 0 \pmod 5$$

Therefore N is divisible by 5

Step 2 - Check N is divisible by 7:

$$4^3 = 64 \equiv 1 \bmod 7$$

$$\rightarrow 4^{1536} = 4^{3 \times 512} = (4^3)^{512}$$

$$\rightarrow 4^{1536} = (1 \bmod 7)^{512}$$

$$\rightarrow 4^{1536} = (1)^{512}$$

$$= 1 \quad \text{---------} \quad (4)$$

$$9^2 = 81 \equiv 4 \bmod 7$$

$$\rightarrow 9^{4824} = (9^2)^{2412}$$

$$\rightarrow 9^{4824} = (4 \bmod 7)^{2412}$$

$$\rightarrow 9^{4824} = (4)^{2412}$$

$$= (4^3)^{804}$$

$$4^3 \equiv 1 \bmod 7$$

$$= (1)^{804}$$

$$= 1$$

$$N = 4^{1536} - \bar{9}^{4824} = 1 - 1 = 0 \pmod 7$$

Therefore N is divisible by both 5 and 7, it is divisible by 35 also.

Assignment 2

1.11. Is $4^{1536} - 9^{4824}$ divisible by 35?

Soln

* Let $N = 4^{1536} - 9^{4824}$ ------ (1)

* 35 is a Multiple of two prime Numbers 5 and 7. We need to check whether N value is disvisible by 5 and 7 seperately.

Step 1 - Check N is divisible by 5:

$\rightarrow 4^2 \equiv 1 \mod 5$

$\rightarrow 4^{1536} = 4^{2 \cdot 768} = (4^2)^{768}$

$\rightarrow 4^{1536} = (1 \mod 5)^{768}$

$\cdot 1 \mod 5 = 1$

$\rightarrow 4^{1536} = (1)^{768}$

$= 1$ ---------- (2)

Therefore the value of 4^{1536} is 1

$\rightarrow 9^{4824} = 9^{2 \times 2412} = (9^2)^{2412}$

$\rightarrow 9^2 \equiv 1 \mod 5$

$\rightarrow 9^{4824} = (1 \mod 5)^{2412}$

$= (1)^{2412} = 1$ ---- (3)

$$N = 4^{1536} - 9^{4824}$$

$$= 1 - 1$$

$$= 0 \pmod 5$$

Therefore N is divisible by 5

Step 2 - Check N is divisible by 7 :

$$4^3 = 64 \equiv 1 \bmod 7$$

$$\rightarrow 4^{1536} = 4^{3 \times 512} = (4^3)^{512}$$

$$\rightarrow 4^{1536} = (1 \bmod 7)^{512}$$

$$\rightarrow 4^{1536} = (1)^{512}$$

$$= 1 \text{ ------ (4)}$$

$$9^2 = 81 \equiv 4 \bmod 7$$

$$\rightarrow 9^{4824} = (9^2)^{2412}$$

$$\rightarrow 9^{4824} = (4 \bmod 7)^{2412}$$

$$\rightarrow 9^{4824} = (4)^{2412}$$

$$= (4^3)^{804}$$

$$4^3 \equiv 1 \bmod 7$$

$$= (1)^{804}$$

$$= 1.$$

$$N = 4^{1536} - \overline{9}^{4824} = 1 - 1 = 0 \pmod 7$$

Therefore N is divisible by both 5 and 7, it is divisible by 35 also.

1.12) What is $2^{2^{2006}} \pmod 3$?

Solution

$2^{2^{2006}} \pmod 3$ ..... ?

$2^{2006} = 2^1 \cdot 2^{2005}$

Let $K = 2^{2005}$

$2^{2006} \pmod 3 = 2^{2^1 \cdot 2^{2005}} \pmod 3$

Apply K

$2^{2006} \pmod 3 = 2^{2^1 \cdot K} \pmod 3$

$= 2^{2K} \pmod 3$

$= 4^K \pmod 3$

$4 \equiv 1 \bmod 3$

$2^{2006} \pmod 3 = (1 \bmod 3)^K \bmod 3$

$= (1)^K \bmod 3$

1 the power of anything is "1" Therefore

$2^{2006} \pmod 3 = (1 \bmod 3)^K$

$= 1$

Therefore, the result $2^{2^{2006}} \pmod 3$ is "1"

1.13) Is the difference of $5^{30,000}$ and $6^{123,456}$ a multiple of 31?

Solution

* We can determine using Fermat's little theorem

$$a^{p-1} = 1 \pmod p \quad \text{..... (1)}$$

The value of p here is 31, which is prime number

$$a^{31-1} \equiv 1 \pmod{31}$$
$$a^{30} \equiv 1 \pmod{31} \text{ for all } 1 \le a < 31 \text{ ... (2)}$$

=> 30000 is multiple of 30.

$$5^{30} \pmod{31} = 1$$

Therefore $5^{30000} \pmod{31} = 1$.

=> to find the value of 6^{123456} the following steps can be performed.

$$123456 \pmod{30} = 6$$

6^{123456} can be rewrite as 6^6

Since $6^{30} \pmod{31} = 1$, then $6^{123456} \pmod{31} = 1$

The difference between 5^{30000} and 6^{123456} can be written as ~~&~~.

$$= 5^{30000} \pmod{31} - 6^{123456} \text{ is}$$
$$= 1 \pmod{31} - 1 \pmod{31}$$
$$= 0 \pmod{31}$$

Therefore the difference between 5^{30000} and 6^{123456} is multiple of 31.

2) a) find $d = \gcd(423, 128)$. Are they co-prime? Now find integers x, y such that $d = x \cdot 423 + y \cdot 128$.

Solution

1st step

	rem	q
gcd (423, 128) =	39	3
gcd (128, 39) =	11	3
gcd (39, 11) =	6	3
gcd (11, 6) =	5	1
gcd (6, 5) =	1	1
gcd (5, 1) =	0	5

gcd (423, 128) = 1.

Therefore they co-prime.

2nd step

x	y	rem(x, y) = x − qy
423	128	$39 = 423 - 3(128)$
128	39	$11 = 128 - 3(39)$
		$= 128 - 3(423 - 3(128))$
		$= 10(128) - 3(423)$
39	11	$6 = 39 - 3(11)$
		$= 423 - 3(128) - 3(10(128) - 3(423))$
		$= 10(423) - 33(128)$

11	6	$5 = 11 - 1(6)$
		$= 10(128) - 3(423) - 1(10(423) - 33(128))$
		$= 43(128) - 13(423)$
6	5	$1 = 6 - 1(5)$
		$= 10(423) - 33(128) - 1(43(128) - 13(423))$
		$= 23(423) - 76(128)$
5	1	0

Therefore $\gcd(423, 128) = 1 = 23(423) - 76(128)$

$X = 23$

$Y = -76$

//

b) Find $d = \gcd(588, 210)$. Are they co-prime? Now find Integers x, y such that $d = x \cdot 588 + y \cdot 210$.

Sol^n

1st step

	rem	q
$\gcd(588, 210) =$	168	2
$\gcd(210, 168) =$	42	1
$\gcd(168, 42) =$	0	4

$\Rightarrow$ They are not co-prime.

2nd step

X	Y	$\text{rem}(X,Y) = X - q \cdot Y$
588	210	$168 = 588 - 2(210)$
210	168	$42 = 210 - 1(168)$

$= 210 - 1(588 - 2(210))$

$= 3(210) - 1(588)$

Therefore $\gcd(588, 210) = 42 = 3(210) - 1(588)$

$42 = -1(588) - 3(210)$

$x = -1$

$y = 3$

c) Find $d = \gcd(420, 96)$. Are they co-prime? Now find integers x, y such that $d = x \cdot 420 + y \cdot 96$

Sol^n

Step 1 -

	rem	q
$\gcd(420, 96) =$	36	4
$\gcd(96, 36) =$	24	2
$\gcd(36, 24) =$	12	1
$\gcd(24, 12) =$	0	2

$\Rightarrow$ They are not co-prime.

Step 2

X	Y	$\text{rem}(X,Y) = X - qY$
420	96	$36 = 420 - 4(96)$
96	36	$24 = 96 - 2(36)$
		$24 = 96 - 2(420 - 4(96))$
		$= 9(96) - 2(420)$
36	24	$12 = 36 - 1(24)$
		$= 420 - 4(96) - 1(9(96) - 2(420))$
		$= 3(420) - 13(96)$
24	12	0

Therefore $\gcd(420, 96) = 12 = 3(420) - 13(96)$

$x = 3$

$y = -13$

d) Find $d = \gcd(33, 27)$. Are they co-prime? Now Find Integers x, y such that $d = x \cdot 33 + y \cdot 27$

Soln

Step 1

	Rem	q
$\gcd(33, 27) =$	6	1
$\gcd(27, 6) =$	3	4
$\gcd(6, 3) =$	0	2

They are not co-prime.

Step 2

X	Y	$\text{rem}(x, y) = X - q \cdot Y$
33	27	$6 = 33 - 1(27)$
27	6	$3 = 27 - 4(6)$
		$= 27 - 4(33 - 1(27))$
		$= 5(27) - 4(33)$
6	3	0

Therefore $\gcd(33, 27) = 3 = 5(27) - 4(33)$

$3 = -4(33) + 5(27)$

$X = -4$

$Y = 5$

(3) Find the multiplicative Inverse of all element in Z_{23}?

Sol^n

- The multiplicative Inverse of an Integer 'a' Modulo 'm' is an Integer 'b' s.t

$$a \cdot b \equiv 1 \pmod{m}$$

Now for $a = 1$ we need to find 'b' s.t

$$1 \cdot b \equiv 1 \mod 23$$

$$\Rightarrow b = 1$$

Multiplicative Inverse of 1 in Z_{23} is 1. Similarly

Multiplicative Inverse of 2 in Z_{23} is

$$2 \cdot b \equiv 1 \pmod{23}$$

$b = 12$, $2 \cdot 12 = 24 = 1 \mod 23$

Similarly, Multiplicative Inverse of all element are

element	Multiplicative Inverse
1	1
2	12
3	8
4	6
5	14
6	4
7	10
8	3

element	Multiplicative Inverse
9	18
10	7
11	21
12	2
13	16
14	5
15	20
16	13
17	19
18	9
19	17
20	15
21	11
22	22

Problem 1.17

Solution

-> Suppose x is an n bit number and time for a single Multiplication of a n bit number to m bit number is O(mn). Assume running time for multiplication $x \cdot x$ will be $O(n^2)$.

Recursive Method :

```
if Y=0
    return 1
if Y=1
    return x
```

temp = power $(x, \text{floor}(y/2))$

Suppose temp is p bits long

if Y is odd; b = temp x temp

return x x b

if Y is even :

return temp x temp

Time required to calculate x^Y recursively is as follows:

While calculating temp, power function is recursively called by breaking x^Y to two halves $(X^{Y/2}, X^{Y/2})$. Thus time Complexity, T(d) of solving this subproblem becomes $O(n/2)$.

- While calculating b, temp is multiplied by temp. size of b after multiplication can be maximum (n+2) bits. As 2 constant taking it as n, the running time T(b) of

Calculating b will be $\wedge^2$.

- To calculate $x \times b$, a multiplication operation is applied. Running time $T(n)$ to calculate it will be equal to $O(\wedge^2)$ time. Thus

$$T(\wedge) = T(d) + T(b) + T(n)$$

$$= O\left(\frac{\wedge}{2}\right) + O(\wedge^2) + O(\wedge^2)$$

Since, $\wedge$ is an integer, polynomially time taken to calculate the temp is less than $T(b)$ and $T(n)$.

Thus overall running time of this algorithm is $O(\wedge^2)$.