Archit Agrawal
202052307

MA102 : Introduction to Discrete Mathematics

Tutorial 8

1. What time does a 12-hour clock read 45 hours before it reads 1 p.m.?

Let x be the time the clock reads 45 hours before 1 p.m.

$$\therefore \quad x + 45 \equiv 1 \pmod{12}$$
$$x + 44 \equiv 0 \pmod{12}$$
$$x \equiv 4 \bmod (12)$$

Now, to check if the time is a.m or p.m.
given time is 1 p.m.

$$\therefore \quad x + 45 \equiv 13 \bmod 24$$
$$x \equiv 16 \bmod 24$$

$\because$ x mod 24 is greater than 12
the time will be afternoon.

Hence, the time will be 4 p.m.

2. What is -101 mod 13?

$$-101 = 13 \times (-8) + 3$$
$$\therefore \quad -101 \equiv 3 \bmod 13$$

Hence, -101 mod 13 is 3.

Archit Agrawal
202052307

3. Find integers a, b, c, m which do not satisfy the following statement:

If $ac \equiv bc \mod m$ with $m \geq 2$, then $a \equiv b \pmod m$

$\because$ $ac \equiv bc \mod m$
$\Rightarrow m \mid (a-b)c$

and, $a \equiv b \pmod m$
$\Rightarrow m \mid (a-b)$

$\therefore$ for the statement to be false
$m \mid c$ and $m \nmid (a-b)$.

Let $m = 5$, $c = 20$, $a = 8$, $b = 4$

$\therefore$ $5 \mid 20$ and $5 \nmid (8-4)$

Hence required integers are $a = 8$, $b = 4$, $c = 20$ and $m = 5$.

4. Show that $2^{340} \equiv 1 \pmod{31}$

$\because$ $2^5 = 32 \equiv 1 \mod (31)$

$\because$ if $a \equiv b \mod n$, then $a^k \equiv b^k \mod n$ where $k \in \mathbb{N}$.

$\therefore$ $(32)^{68} \equiv 1^{68} \mod (31)$

Archit Agrawal
202052307

$$\therefore \left(2^5\right)^{68} \equiv 1 \bmod (31)$$

$$2^{340} \equiv 1 \bmod (31)$$

Hence, proved.

5. Find the last digit of 333^{555}.

We need to calculate $(333)^{555} \bmod 10$

$$\because (333)^{555} \bmod 10 = 3^{555} \bmod 10$$

$\therefore$ we need to calculate $3^{555} \bmod (10)$

$\because$ we know that $3^4 \equiv 1 \bmod (10)$

and $\because$ $555 = 4 \times 138 + 3$

$$\therefore 3^{555} \equiv 3^{552} \cdot 3^3 \pmod{10}$$

$$3^{555} \equiv 3^3 \pmod{10}$$

$$3^{555} \equiv 7 \pmod{10}$$

Hence, unit digit in $(333)^{555}$ is 7.

6. State and prove divisibility test of 3.

A number is divisible by 3 if the sum of its digits is divisible by 3.

Archit Agrawal
202052307

Proof:
Let N be ~~abcd~~, $a_n a_{n-1} a_{n-2} \cdots a_0$ where a_i are digits of N.

$\therefore N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10^1 + a_0 10^0$

$\because$ $10 \equiv 1 \bmod (3)$

$\therefore$ $10^i \equiv 1 \bmod (3)$ $\forall\, i \in \mathbb{N}$

$$N = a_n (10^n - 1) + a_{n-1}(10^{n-1} - 1) + \cdots + a_1 (10^1 - 1) + a_0 (10^0 - 1) + (a_n + a_{n-1} + \cdots + a_0)$$

~~$N = a_n (10^n$~~

$N \bmod 3 \equiv (a_n + a_{n-1} + \cdots + a_1 + a_0) \bmod (3)$

$\therefore$ K will be a multiple of 3 iff $a_n + a_{n-1} + a_{n-2} + \cdots + a_1 + a_0$ i.e. the sum of digits is divisible by 3.

7. Find the multiplicative inverse of each non-zero element of Z_{11} to verify Z_{11} is a field.

In Z_{11}, we need to find b for every non-zero a, such that
$$ab \equiv 1 \bmod (11)$$

$1 \times b \equiv 1 \bmod (11)$, $b = 1$
$2 \times b \equiv 1 \bmod (11)$, $b = 6$
$3 \times b \equiv 1 \bmod (11)$, $b = 4$

Archit Agrawal
202052307

$4 \times b \equiv 1 \bmod 11$, $b = 3$

$5 \times b \equiv 1 \bmod 11$, $b = 9$

$6 \times b \equiv 1 \bmod 11$, $b = 2$

$7 \times b \equiv 1 \bmod 11$, $b = 8$

$8 \times b \equiv 1 \bmod 11$, $b = 7$

$9 \times b \equiv 1 \bmod 11$, $b = 5$

$10 \times b \equiv 1 \bmod 11$, $b = 10$

$\therefore$ the multiplicative inverses of (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) are

(1, 6, 4, 3, 9, 2, 8, 7, 5, 10) respectively.

8. Show that 1729 is a Carmichael number.

A composite number n that satisfies the congruence $b^{n-1} \equiv 1 \pmod n$ for all positive integers b with $\gcd(b, n) = 1$ is called a Carmichael number.

$\because$ $1729 = 7 \times 13 \times 19$

$\therefore$ 1729 is composite.

Now, if $\gcd(b, 1729) = 1$, then
$\gcd(b, 7) = \gcd(13, b) = \gcd(b, 19) = 1$

$\therefore$ using Fermat's Little theorem, we have,

$b^6 \equiv 1 \pmod 7$ — (I)

$b^{12} \equiv 1 \pmod{13}$ — (II)

$b^{18} \equiv 1 \pmod{19}$ — (III)

Archit Agrawal
202052307

$\because$ If $a \equiv b \pmod{n}$ then $a^K \equiv b^K \pmod{n}$
for $K \in N$.

$b^{1728} = (b^6)^{288} \equiv (1)^{288} \bmod (7)$ {from (I)}

$\Rightarrow b^{1728} \equiv 1 \bmod (7)$

from (II),
$b^{1728} = (b^{12})^{144} \equiv (1)^{144} \bmod (13)$

$\therefore b^{1728} \equiv 1 \bmod (13)$

from (III),
$b^{1728} = (b^{18})^{96} \equiv (1)^{96} \bmod (19)$

$\therefore b^{1728} \equiv 1 \bmod (19)$

If $m_1, m_2, \ldots, m_n$ are coprime integers greater than equal to 2 and

$a \equiv b \bmod (m_i)$, $1 \leq i \leq n$, then
$a \equiv b \pmod{m}$
where $m = m_1 \times m_2 \times \ldots \times m_n$

$\therefore b^{1728} \equiv 1 \bmod (7 \times 13 \times 19)$
$b^{1728} \equiv 1 \bmod (1729)$

Hence, 1729 is a Carmichael number.

Archit Agrawal
202052307

Date:
Page: 7

9. Find all integers x such that
$2x \equiv 3 \bmod 5$, $3x \equiv 4 \bmod 7$
and $x \equiv 5 \bmod 11$.

multiplicative inverse of 2 mod 5 is,

$$(2b-1) \% 5 = 0$$
at $b = 3$

$\therefore$ multiplicative inverse of 2 mod 5 is 3.

multiplicative inverse of 3 mod 7,

$$(3b-1) \% 7 = 0$$
at $b = 5$ the above equation holds

$\therefore$ multiplicative inverse of 3 mod 7 is 5.

$\therefore$ $2x \equiv 3 \bmod 5 \Rightarrow x \equiv 4 \pmod 5$
$\therefore$ $3x \equiv 4 \bmod 7 \Rightarrow x \equiv 6 \pmod 7$
and, $x \equiv 5 \pmod{11}$

$\therefore$ $a_1 = 4$, $a_2 = 6$ and $a_3 = 5$

By Chinese Remainder Theorem, since, 5, 7 and 11 are co-prime, a solution exists for the system.

$$m = 5 \times 7 \times 11 = 385$$

$$M_1 = \frac{m}{m_1} = 77, \quad M_2 = \frac{m}{m_2} = 55$$

Archit Agrawal
20205 2307

and $M_3 = \frac{m}{m_3} = 35$

now, inverses of 77 mod 5, 55 mod 7 and 35 mod 11 are $y_1 = -2$, $y_2 = -1$ and $y_3 = -5$.

$\therefore \ x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$= 4 \times 77 \times -2 + 6 \times 55 \times (-1) + 3 \times 35 \times (-5)$

$x = -616 - 330 - 875$

$x = -1821 \Rightarrow \boxed{x \equiv 104 \text{ mod } 385}$ Answer

10. Use Fermat's Little Theorem to compute 5^{2021} mod 7, 5^{2021} mod 11, and 5^{2021} mod 13. Use Chinese Remainder Theorem to find 5^{2021} mod 1001.

5^{2021} mod 7

Since 5 and 7 are co-primes.
$\therefore$ Using Fermat's Little theorem, we have

$$5^6 \equiv 1 \text{ mod } (7)$$

$$\therefore \ 5^{2021} = 5^{336 \times 6} \times 5^5$$

$$5^{2021} = (5^6)^{336} \times 5^5$$

Archit Agrawal
202052307

$\therefore \quad 5^{2021} \pmod 7 \equiv 5^{336 \cdot 6} \cdot 5^5 \pmod 7$

$\equiv 1 \cdot 5^5 \pmod 7$

$\equiv 5^2 \cdot 5^3 \pmod 7$

$\equiv \left(5^2 \pmod 7 \times 5^3 \pmod 7\right) \bmod 7$

$\equiv (4 \times 6) \bmod 7$

$= 3$

Hence, $\quad 5^{2021} \pmod 7 = 3$.

$\underline{5^{2021} \bmod 11}$

Since 5 and 11 are co-primes, therefore using Fermat's Little theorem, we have

$5^{10} \equiv 1 \bmod (11)$

$\because \quad 2021 = 10 \times 202 + 1$

$\therefore \quad 5^{2021} = (5^{10})^{202} \cdot 5$

$\therefore \quad 5^{2021} \bmod (11) \equiv (5^{10})^{202} \cdot 5 \pmod{11}$

$\equiv 1 \cdot 5 \pmod{11}$

$= 5$

$\therefore \quad 5^{2021} \bmod (11) = 5$

Archit Agrawal
202052307

$5^{2021} \mod 13$

Since, 5 and 13 are co-prime, using Fermat's little theorem, we have,

$$5^{12} \equiv 1 \pmod{13}$$

$$\because \quad 2021 = 168 \times 12 + 5$$

$$\therefore \quad 5^{2021} = (5^{12})^{168} \cdot 5^{5}$$

$$\therefore \quad 5^{2021} \pmod{13} \equiv (5^{12})^{168} \cdot 5^{5} \pmod{13}$$

$$= 1 \cdot 5^{2} \cdot 5^{3} \pmod{13}$$

$$= ((25 \bmod 13) \cdot (125 \bmod 13)) \bmod 13$$

$$= (12 \times 8) \bmod 13$$

$$= 5$$

$$\therefore \quad 5^{2021} \bmod 13 = 5$$

Finding $5^{2021} \bmod (1001)$

Using Chinese Remainder Theorem,

$$\because \quad 1001 = 7 \times 11 \times 13$$

Let $x = 5^{2021}$, we have
(using earlier solved result)

$$x \equiv 3 \pmod{7}$$
$$x \equiv 5 \pmod{11}$$
$$x \equiv 5 \pmod{13}$$

Archit Agrawal
202052307

$\therefore$ $a_1 = 3$, $a_2 = 5$, $a_3 = 5$

and $M = 1001$

$\therefore$ $M_1 = \frac{M}{m_1} = 143$

$M_2 = \frac{M_1}{m_2} = 91$

$M_3 = \frac{M}{m_3} = 77$

Now, inverses of 143 (mod 7), 91 (mod 11) and 77 (mod 13) are 5, 4 and −1 respectively.

$\therefore$ $y_1 = 5$, $y_2 = 4$ and $y_3 = -1$.

$\therefore$ $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$= 3 \times 143 \times 5 + 5 \times 91 \times 4 + 5 \times 77 \times -1$

$= 2185 + 1820 - 385$

$= 3580$

$x = 3580 \equiv 577 \pmod{1001}$

$\therefore$ $x \equiv 577 \pmod{1001}$

$\therefore$ $\boxed{5^{2021} \pmod{1001} = 577}$ Ans