Various Problem and Solution

Question 1. Show that $n(n+1)(2n+1)$ is divisible by 6.

Solution. One of the two consecutive integers n and $n+1$ is divisible by 2 and one of the other consecutive integer $2n$, $2n+1$ and $2n+2$ is divisible by 2.
Hence, the product $\quad 2n(2n+1)(2n+2)$

$$= 4n(2n+1)(2n+1) \text{ is divisible by 2 and 3.}$$

Since 4 is divisible by 2 and 2 is prime to 3, so $n(n+1)(2n+1)$ is divisible by 6.

Question 2. Show that $n^5 - n$ is divisible by 30.

Solution. Let n be even.
Then n^5 is even and $n^5 - n$ is also even and which is divisible by 2.
If n is odd, then $n^5 - n$ is even and hence divisible by 2.
Now, $n^5 - n = n(n^4 - 1)$
But, $n^4 - 1 = n^{5-1} - 1$
By Fermat's theorem $\quad n^{5-1} - 1$ is divisible by 5
i.e., $n^4 - 1$ is divisible by 5
$n(n^4 - 1)$ is divisible by 5
$n^5 - n$ is divisible by 5
Again n can be written any one of the form $3m$, $3m+1$ and $3m+2$.
When $n = 3m$, $3m\left\{(3m)^4 - 1\right\}$ which is divisible by 3.
When $n = 3m+1$,

$$\begin{aligned}
&(3m+1)\left\{(3m+1)^4 - 1\right\}\\
=&(3m+1)\left\{81m^4 + 108m^3 + 54m^2 + 12m + 1 - 1\right\}\\
=&3m(3m+1)(27m^3 + 36m^2 + 18m + 4) \quad \text{which is divisible by 3}
\end{aligned}$$

When $n = 3m+2$,

$$\begin{aligned}
&(3m+2)\left\{(3m+2)^4 - 1\right\}\\
=&(3m+2)\left\{81m^4 + 216m^3 + 216m^2 + 96m + 16 - 1\right\}\\
=&3(3m+2)(27m^4 + 72m^3 + 72m^2 + 32m + 5) \quad \text{which is divisible by 3}
\end{aligned}$$

Hence, $n^5 - n$ is divisible by the product of $2, 3, 5$
i.e., $n^5 - n$ is divisible by 30.

$$(a+b+c)^2 = a^2 + b^2 + c^2 + 2ab + 2bc + 2ca$$
$$(a+b)^4 = a^4 + b^4 + 6a^2b^2 + 4a^3b + 4ab^3$$

Question 3. If n is an integer then prove that one of n, $n+2$, $n+4$ is divisible by 3.

Solution. Given the number n, $n+2$, $n+4$ when n is an integer, then n must be any one of the form $3m,\ 3m+2,\ 3m+4$.
If $n = 3m$, the first integer is divisible by 3.
If $n = 3m+2$, then $n+4 = 3m+2+4 = 3(m+2)$ which is divisible by 3.
If $n = 3m+4$, then $n+2 = 3m+4+2 = 3(m+2)$ which is divisible by 3.
Hence, if n is an integer then one of n, $n+2$ and $n+4$ is divisible by 3.

Question 4. Prove that, $3^{2n+1} + 2^{n+2}$ is divisible by 7.

Solution. Let $T = 3^{2n+1} + 2^{n+2}$
For $n = 0$, $T = 3 + 4 = 7$ which is divisible by 7.
For $n = 1$, $T = 27 + 8 = 35$ which is divisible by 7.
For $n = 3$, $T = 259$ which is divisible by 7.
Suppose, for $n = 3$, $T = 3^{2r+1} + 2^{r+2} = 7q$ which is divisible by 7.
Thus, for $n = r+1$,

$$\begin{aligned}
T =& 3^{2(r+1)+2} + 2^{(r+1)+2} \\
=& 9 \cdot 3^{2r+1} + 2 \cdot 2^{r+2} \\
=& 9\left(3^{2r+1} + 2^{r+2}\right) - 7 \cdot 2^{r+2} \\
=& 7 \cdot 9q - 7 \cdot 2^{r+2} \\
=& 7\left(9q - 2^{r+2}\right) \text{ which is divisible by 7}
\end{aligned}$$

Hence, $3^{2n+1} + 2^{n+2}$ is divisible by 7.

Question 5. Show that $2^n + 1$ or $2^n - 1$ is divisible by 3 according as n is odd or even.

Solution. We know that the product $P = (2^n + 1)(2^n - 1) = 2^{2n} - 1$ is divisible by 3 for all n.
For $n = 0$, $P = 2 \cdot 0 = 0$ is divisible by 3.
For $n = 1$, $P = 3 \cdot 1 = 3$ is divisible by 3.
For $n = 2$, $P = 5 \cdot (4 - 1) = 15$ is divisible by 3.
Suppose, for $n = r$, $P = (2^r + 1)(2^r - 1)$ is divisible by 3. i.e., $(2^r + 1)(2^r - 1) = 3q$ where q is an integer.
Then for $n = r+1$,

$$\begin{aligned}
P =& \left(2^{r+1} + 1\right)\left(2^{r+1} - 1\right) \\
=& 2^{2(r+1)} - 1 \\
=& 4\left(2^{2r} - 1\right) + 3 \\
=& 4 \cdot 3q + 3 \\
=& 3(4q + 1) \text{ which is divisible by 3}
\end{aligned}$$

Question 6. Compute $\varphi(210)$, $\varphi(2187)$, $\varphi(2000)$, $\varphi(1026)$, $\varphi(13912)$, $\varphi(1981)$, $\varphi(1350)$.

Solution.

$$\begin{aligned}
\varphi(210) &= \varphi(2 \cdot 5 \cdot 3 \cdot 7) \\
&= \varphi(2)\ \varphi(5)\ \varphi(3)\ \varphi(7) \\
&= 1 \cdot 4 \cdot 2 \cdot 6 \\
&= 48
\end{aligned}$$

$$\begin{aligned}\varphi(2187) &= \varphi(3\cdot 3\cdot 3\cdot 3\cdot 3\cdot 3\cdot 3)\\ &= \varphi\left(3^7\right)\\ &= 3^7\left(1-\frac{1}{3}\right)\\ &= 1458\end{aligned}$$

$$\begin{aligned}\varphi(2000) &= \varphi(2\cdot 1000)\\ &= \varphi\left(2\cdot 5\cdot 200\right)\\ &= \varphi\left(2\cdot 5\cdot 5\cdot 4\cdot 2\cdot 5\right)\\ &= \varphi\left(2^4\cdot 5^3\right)\\ &= \varphi\left(2^4\right)\ \varphi\left(5^3\right)\\ &= \left(2^4-2^3\right)\ \left(5^3-5^2\right)\\ &= 8\cdot 100\\ &= 800\end{aligned}$$

$$\begin{aligned}\varphi(1026) &= \varphi(2\cdot 3\cdot 3\cdot 3\cdot 19)\\ &= \varphi\left(2\right)\ \varphi\left(3^3\right)\ \varphi(19)\\ &= 1\left(3^3-3^2\right)\ (18)\\ &= 324\end{aligned}$$

$$\begin{aligned}\varphi(13912) &= \varphi(2\cdot 2\cdot 2\cdot 37\cdot 47)\\ &= \varphi\left(8\right)\ \varphi\left(37\right)\ \varphi(47)\\ &= (8-4)\ (36)\ (46)\\ &= 6624\end{aligned}$$

$$\begin{aligned}\varphi(1981) &= \varphi(7\cdot 283)\\ &= \varphi\left(7\right)\ \varphi\left(283\right)\\ &= 7\cdot 282\\ &= 1974\end{aligned}$$

Question 7. Show that the sum of the integers less than n and prime to it is $\frac{1}{2}n\varphi(n)$ if $n \geq 2$.

Solution. Let x be an integer less than n and prime to it, then $n-x$ is also an integer less than n and prime to it.

Define the integer by $1, p, q, r, \ldots, (n-1)$ and their sum by S. Then

$$S = 1 + p + q + r + \cdots + (n-p) + (n-q) + (n-r) + (n-1)$$

which is the series consisting of $\varphi(n)$ terms.
Rearranging, we have

$$\begin{aligned} S =&(n-1)+(n-r)+(n-q)+(n-p)+\cdots+r+q+p+1 \\ \therefore 2S =&n+n+n+n+\dots \text{ upto } \varphi(n) \text{ terms} = n\varphi(n) \\ \therefore S =&\frac{1}{2}n\varphi(n) \end{aligned}$$

Question 8. Show that the following congruence holds for all integer values of n.

(i) $2^{2n}-1 \equiv 0 \pmod 3$

(ii) $2^{3n}-1 \equiv 0 \pmod 7$

(iii) $2^{4n}-1 \equiv 0 \pmod{15}$

Solution. We show that $T = 2^{2n}-1$ is divisible by 3.
For $n=1$, $T = 4-1 = 3$ which is divisible by 3.
For $n=2$, $T = 16-1 = 15$ which is divisible by 3.
For $n=3$, $T = 64-1 = 63$ which is divisible by 3.

Let for $n=r$, $t = 2^{2r}-1 = 3q$ which is divisible by 3.
Now for $n = r+1$,

$$\begin{aligned} T &= 2^{2(r+1)}-1 \\ &= 4\cdot 2^{2r}-1 \\ &= 4\left(2^{2r}-1\right)+3 \\ &= 3\,(4q+1) \text{ which is divisible by 3} \end{aligned}$$

Hence, $2^{2n}-1 \equiv 0 \pmod 3$.

Question 9. Prove that if a is an integer, then $6 \mid a(a^2+11)$.

Proof. Let a is an even integer, then for any integer values of n, we can write $a = 2n$.
So,

$$\begin{aligned} &2n\left\{(2n)^2+11\right\} \\ =&2n\left\{4n^2-1+12\right\} \\ =&2n(2n+1)(2n-1)+24n \\ =&(2n-1)(2n)(2n+1)+24n \end{aligned}$$

Since, $(2n-1)(2n)(2n+1)$ is the multiple of three consecutive integers and hence is divisible by $3! = 6$ and 24 is evidently divisible by 6.

Hence, $a(a^2+11)$ is divisible by 6 for all even values of a.

Again, let a is odd integer, then for any integer values of n, we write $a = 2n + 1$.
So,

$$\begin{aligned}
&(2n+1)\left\{(2n+1)^2+11\right\}\\
=&(2n+1)\left\{(2n+1)^2-1^2+12\right\}\\
=&(2n+1)\left\{(2n+2)(2n+1-1)\right\}+12(2n+1)\\
=&2n(2n+1)(2n+2)+12(2n+1)
\end{aligned}$$

Since, $2n(2n+1)(2n+2)$ is the product of three consecutive integers and hence is divisible by $3! = 6$, again $12(2n+1)$ is divisible by 6.

Thus, $a(a^2 + 11)$ is divisible by 6. □

Question 10. Prove that if a is an odd integer, then 24 divides $a(a^2 - 1)$ i.e., $24 \mid a(a^2 - 1)$.

Solution. Let a is an odd integer, then $a - 1$ and $a + 1$ are two even integers, hence one of them is divisible by 2 and the other by 4.

Again, $a - 1$ a, $a + 1$ are three consecutive numbers and hence one of them is divisible by 3.

Thus, the product $a(a^2 - 1)$ is divisible by $2 \cdot 3 \cdot 4$ i.e., $a(a^2 - 1)$ is divisible by 24.

Question 11. If a and b are odd integers then show that $8 \mid (a^2 - b^2)$.

Solution. Here $a^2 - b^2 = (a - b)(a + b)$
Since a and b are odd integers here, so $a - b$ and $a + b$ are two even numbers. Hence, one of them is divisible by 2 and the other is by 5.
Hence, the product $(a - b)(a + b)$ is divisible by product of 2 and 4 i.e., by 8.

Question 12. Show that $n^4 + 4$ is composite for all $n > 1$.

Solution. Suppose, $f(n) = n^4 + 4$

$$\begin{aligned}
&= (n^2+2)^2 - 4n^2\\
&= (n^2+2n+2)(n^2-2n+2)
\end{aligned}$$

If $n = 1$, $f(1) = 5$ which is not composite.
But when $n > 1$ then $f(n)$ is a product of two factors and hence is a composite number.

Question 13. Show that $n^4 + n^2 + 1$ is composite for all $n > 1$.

Solution. Let, $f(n) = n^4 + n^2 + 1$

$$\begin{aligned}
&= (n^2+1)^2 - n^2\\
&= (n^2+n+1)(n^2-n+1)
\end{aligned}$$

If $n = 1$, $f(1) = 3$ which is not composite.
Thus, when $n > 1$ then $f(n)$ is a product of two factors and hence is a composite number.

Question 14. Show that $n^4 + n^2 + 1$ is composite for all $n > 1$.

Question 15. If $(a, 7) = 1$, then prove that $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

Solution. Since $(a, 7) = 1$ and 7 is a prime so by Fermat's theorem,

$$\begin{aligned} &a^{7-1} \equiv 1 \pmod 7 \\ \Rightarrow\ &a^6 - 1 \equiv 0 \pmod 7 \\ \Rightarrow\ &(a^3)^2 - 1 \equiv 0 \pmod 7 \\ \Rightarrow\ &(a^3+1)(a^3-1) \equiv 0 \pmod 7 \end{aligned}$$

Hence, $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

Question 16. If $(a, p) = 1$, $(b, p) = 1$ then show that $a^p \equiv b^p \pmod p$ implies that $a \equiv b \pmod p$.

Solution. Since,

$$\begin{aligned} &(a, p) = 1 \qquad \text{and} \qquad (b, p) = 1 \\ \Rightarrow\ &a^{p-1} \equiv 1 \pmod p \qquad \text{and} \qquad b^{p-1} \equiv 1 \pmod p \\ \Rightarrow\ &a^p \equiv a \pmod p \qquad \text{and} \qquad b^p \equiv b \pmod p \\ \therefore\ &a^p - b^p \equiv a - b \pmod p \end{aligned} \tag{1}$$

Again,

$$a^p \equiv b^p \pmod p \quad \Rightarrow \quad a^p - b^p \equiv 0 \pmod p$$

Hence, (1) implies that $a \equiv b \pmod p$.

Question 17. If $(a, p) = 1$, $(b, p) = 1$ then show that $a^p \equiv b^p \pmod p$ implies that $a \equiv b \pmod{p^2}$.

Solution. Since,

$$\begin{aligned} &(a, p) = 1 \qquad \text{and} \qquad (b, p) = 1 \\ \Rightarrow\ &(a, p^2) = 1 \qquad \text{and} \qquad (b, p^2) = 1 \\ \Rightarrow\ &a^{p^2-1} \equiv 1 \pmod{p^2} \qquad \text{and} \qquad b^{p^2-1} \equiv 1 \pmod{p^2} \\ \Rightarrow\ &a^{p^2} \equiv a \pmod{p^2} \qquad \text{and} \qquad b^{p^2} \equiv b \pmod{p^2} \\ \Rightarrow\ &\left(a^{p^2}\right)^p \equiv a^p \pmod{p^2} \qquad \text{and} \qquad \left(b^{p^2}\right)^p \equiv b \pmod{p^2} \\ \therefore\ &a^p - b^p \equiv \left(a^{p^2}\right)^p - \left(b^{p^2}\right)^p \pmod{p^2} \end{aligned}$$

Again, $a^p \equiv b^p \pmod p$

We have, $\quad (a^p)^{p^2} \equiv (b^p)^{p^2} \pmod{p^2}$

$\Rightarrow a^p \equiv b^p \pmod{p^2}$

$\Rightarrow a \equiv b \pmod{p^2}$

Question 18. If p is a prime of the form $4n+1$, then show that $28! + 233 \equiv 0 \pmod{899}$ i.e., $28! + 233$ is divisible by 899.

Solution. Here, $899 = 29 \cdot 31$

$233 = 8 \cdot 29 + 1$

$233 = 3 \cdot 7 + 16$

$$\therefore\ 233 \equiv 1 \pmod{29} \tag{2}$$

and

$$\therefore\ 233 \equiv 16 \pmod{31} \tag{3}$$

Now, by using Wilson's theorem we have,

$$\begin{aligned}
&(29-1)! + 1 \equiv 0 \pmod{29}\\
\Rightarrow\ &28! + 1 \equiv 0 \pmod{29} \qquad (4)
\end{aligned}$$

Combining (2) and (4),

$$28! + 233 \equiv 0 \pmod{29} \tag{5}$$

Again by using Wilson's theorem,

$$\begin{aligned}
&(31-1)! + 1 \equiv 0 \pmod{31}\\
\Rightarrow\ &30 \cdot 29 \cdot 28! + 1 \equiv 0 \pmod{31}\\
\Rightarrow\ &-1 \cdot -2 \cdot 28! + 1 \equiv 0 \pmod{31}\\
\Rightarrow\ &2 \cdot 28! + 1 + 31 \equiv 0 \pmod{31}\\
\Rightarrow\ &28! + 16 \equiv 0 \pmod{31} \qquad (6)
\end{aligned}$$

Combining (3) and (6),

$$28! + 233 \equiv 0 \pmod{29 \cdot 31} \quad \Rightarrow \quad 28! + 233 \equiv 0 \pmod{899}$$

Question 19. Prove that $18! + 1 \equiv 0 \pmod{437}$ i.e., $18! + 1$ is divisible by 437.

Solution. Here $437 = 19 \cdot 23$
Thus, using Wilson's theorem,

$$\begin{aligned}
&(19-1)! + 1 \equiv 0 \pmod{19}\\
\Rightarrow\ &18! + 1 \equiv 0 \pmod{19} \qquad (7)
\end{aligned}$$

$$\begin{aligned}
&(23-1)! + 1 \equiv 0 \pmod{23}\\
\Rightarrow\ &22! + 1 \equiv 0 \pmod{23}\\
\Rightarrow\ &22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! + 1 \equiv 0 \pmod{23}\\
\Rightarrow\ &-1 \cdot -2 \cdot -3 \cdot -4 \cdot 18! + 1 \equiv 0 \pmod{23}\\
\Rightarrow\ &24 \cdot 18! + 1 \equiv 0 \pmod{23}\\
\Rightarrow\ &(23+1) \cdot 18! + 1 \equiv 0 \pmod{23}\\
\Rightarrow\ &23 \cdot 18! + 18! + 1 \equiv 0 \pmod{23} \qquad (8)
\end{aligned}$$

Now, from (7) and (8) we have $18! + 1 \equiv 0 \pmod{19 \cdot 23}$ i.e., $18! + 1 \equiv 0 \pmod{437}$.

Question 20. If p is a prime of the form $4n+1$, then $(2n)!$ is a solution of the congruence $x^2 \equiv -1 \pmod{p}$.

Solution. If p is a prime, then by Wilson's theorem,
We have,

$$(p-1)! + 1 \equiv 0 \pmod{p} \tag{9}$$

Putting $p = 4n + 1$ in (9), we get,

$$\begin{aligned}
&(4n)! + 1 \equiv 0 \pmod{p} \\
&\Rightarrow 4n \cdot (4n-1) \cdot (4n-2) \ldots (2n+1) \cdot (2n)! + 1 \equiv 0 \pmod{p}
\end{aligned} \tag{10}$$

Now, $p = 4n + 1$

$$\begin{aligned}
\therefore\ & 4n + 1 \equiv 0 \pmod{p} \\
\Rightarrow\ & 4n \equiv -1 \pmod{p} \\
\Rightarrow\ & 4n - 1 \equiv -2 \pmod{p} \\
\Rightarrow\ & 4n - 2 \equiv -3 \pmod{p} \\
& \ldots \quad \ldots \quad \ldots \\
\Rightarrow\ & 4n - (2n-1) \equiv -2n \pmod{p} \\
\text{i.e.,}\ & 2n + 1 \equiv -2n \pmod{p}
\end{aligned}$$

Hence multiplying all the congruence, we get,

$$4n \cdot (4n-1) \cdot (4n-2) \ldots (2n+1) \equiv (-1)^{2n}(2n)! \pmod{p} \tag{11}$$

Combining (10) and (11), we get,

$$\begin{aligned}
& (-1)^{2n}(2n)! \cdot (2n)! + 1 \equiv 0 \pmod{p} \\
\Rightarrow\ & ((2n)!)^2 \equiv -1 \pmod{p} \\
\Rightarrow\ & x^2 \equiv -1 \pmod{p}, \\
& \text{where } x = (2n)!
\end{aligned}$$

Thus, $x = (2n)!$ is a solution of the given congruence $x^2 \equiv -1 \pmod{p}$.

Question 21. Show that, $a^7 - a$ is divisible by 42.

Solution. Let, $T = a^7 - a = a(a^6 - 1) = a(a^3 - 1)(a^3 + 1)$
i.e., $T = a(a-1)(a+1)(a^2+a+1)(a^2-a+1)$
$\qquad = (a-1)a(a+1)(a^4+a^2+1)$
Since $(a-1)a(a+1)$ is a product of three consecutive integers, hence is divisible by $3! = 6$ and so $(a-1)a(a+1)$ is divisible by 6.
Now, by Fermat's theorem,

$$\begin{aligned}
& a^{7-1} \equiv 1 \pmod{7} \\
\Rightarrow\ & a(a^6 - 1) \equiv 0 \pmod{7}
\end{aligned}$$

Hence the product $(a-1)a(a+1)(a^4+a^2+1)$ is divisible by the product of 6 and 7. That is, $a^7 - a$ is divisible by 42.

Question 22. Show that, $a^{36} - 1$ is divisible by 33744. If a is prime to 2, 3, 19 and 37.

Solution. Given, $(a, 2) = 1$, $(a, 3) = 1$, $(a, 19) = 1$, and $(a, 37) = 1$.
By Fermat's theorem,

$$\begin{aligned}
& a^{2-1} \equiv 1 \pmod{2} \\
\Rightarrow\ & a^{36} \equiv 1 \pmod{2}
\end{aligned}$$

Similarly,

$$\begin{aligned} a^{36} &\equiv 1 \pmod{3} \\ a^{36} &\equiv 1 \pmod{19} \\ a^{36} &\equiv 1 \pmod{37} \end{aligned}$$

Since 2, 3, 19 and 37 are relatively prime in pairs.
So, $a^{36} \equiv 1 \pmod{2 \cdot 3 \cdot 19 \cdot 37}$
$a^{36} \equiv 1 \pmod{4218}$
That is $a^{36} - 1$ is divisible by 4218.
Again, $a^{36} - 1 = (a^{18})^2 - 1 = (a^{18} + 1)(a^{18} - 1)$
When a is odd, then $(a^{18} - 1)$ and $(a^{18} + 1)$ are two consecutive even numbers and hence one of them is divisible by 2 and the other is by 4.
So, their product $(a^{18} + 1)(a^{18} - 1)$ is divisible by 8.
Therefore, $a^{36} - 1$ is divisible by $8 \times 4218 = 33744$.

Question 23. Solve these congruences

(a) $5x \equiv 2 \pmod{7}$

(b) $98x \equiv 7 \pmod{105}$

(c) $15x \equiv 6 \pmod{21}$

Solution.

(a) Here $(5, 7) = 1$ so the given congruence $5x \equiv 2 \pmod{7}$ has exactly one solution.

$$\begin{aligned} & 5x \equiv 2 \pmod{7} \\ \Rightarrow\ & 15x \equiv 6 \pmod{7} \\ \Rightarrow\ & x \equiv 6 \pmod{7} \end{aligned}$$

Hence, $x = 6$ is a root of $5x \equiv 2 \pmod{7}$.

(b) Here $(98, 105) = 7$ and $7 \mid 7$. So there are 7 incongruent roots of the congruence $98x \equiv 7 \pmod{105}$.

$$\begin{aligned} & 98x \equiv 7 \pmod{105} \\ \Rightarrow\ & 14x \equiv 1 \pmod{15} \\ \Rightarrow\ & -x \equiv 1 \pmod{15} \\ \text{i.e., }\ & x \equiv -1 + 15 \pmod{15} \\ \text{i.e., }\ & x = 14 \text{ is a solution.} \end{aligned}$$

Hence, the other incongruent solution are given by,

$$x = 14,\ 14 + \frac{105}{7},\ 14 + \frac{2 \cdot 105}{7},\ 14 + \frac{3 \cdot 105}{7},\ 14 + \frac{4 \cdot 105}{7},\ 14 + \frac{5 \cdot 105}{7},\ 14 + \frac{6 \cdot 105}{7}$$

i.e., $x = 14,\ 29,\ 44,\ 59,\ 74,\ 89,\ 104$

(c) Here $(98, 105) = 7$ and $7 \nmid 1$ so $98x \equiv 1 \pmod{105}$ has no solution.

Question 24. Solve the following simultaneous congruences

(a) $x \equiv 1 \pmod{15}$ and $x \equiv 11 \pmod{21}$

(b) $x \equiv 2 \pmod{12}$ and $x \equiv 5 \pmod{13}$

Solution.

(a)

$$x \equiv 1 \pmod{15}$$
$$\Rightarrow \left.\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 1 \pmod 5 \end{aligned}\right\} \text{Since 15 must be divisible by each of 3 and 5 and } (3,5)=1.$$

Again,

$$\begin{aligned} & x \equiv 11 \pmod{21} \\ \Rightarrow\ & x \equiv 11 \equiv 2 \pmod 3 \\ & x \equiv 11 \equiv 4 \pmod 7 \end{aligned}$$

$$\left.\begin{aligned} \text{But} \quad x &\equiv 1 \pmod 3 \\ \text{and} \quad x &\equiv 2 \pmod 3 \end{aligned}\right\} \text{is impossible.}$$

So the given congruences has no solution.

(b)

$$x \equiv 2 \pmod{12}$$
$$\Rightarrow \left\{\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 4 \end{aligned}\right.$$

Thus, we have to solve

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 5 \pmod{13} \end{aligned}$$

Here $a_1 = 2, \quad a_2 = 2, \quad a_3 = 5$

$m_1 = 3, \quad m_2 = 4, \quad m_3 = 15; \quad m = m_1 m_2 m_3 = 156$

$Q_1 = 52, \quad Q_2 = 39, \quad Q_3 = 12; \quad \text{where } Q_i = \dfrac{m}{m_i}$

Consider the congruence $Q_i y_i \equiv 1 \pmod{m_i}$

$$\begin{aligned} & 52y_1 \equiv 1 \pmod 3 \\ \Rightarrow\ & y_1 \equiv 1 \pmod 3 \end{aligned}$$

$$\begin{aligned} & 39y_2 \equiv 1 \pmod 4 \\ \Rightarrow\ & -y_2 \equiv 1 \pmod 4 \end{aligned}$$

$$\begin{aligned} & 12y_3 \equiv 1 \pmod{13} \\ \Rightarrow\ & -y_3 \equiv 1 \pmod{13} \\ \Rightarrow\ & y_3 \equiv 12 \pmod{13} \end{aligned}$$

$$
\begin{aligned}
\text{Now, } X &= Q_1y_1a_1 + Q_2y_2a_2 + Q_3y_3a_3 \\
&= 104 + 234 + 720 \\
&\equiv 1058 \pmod{156} \\
&\equiv 122 \pmod{156}
\end{aligned}
$$

Thus, $x = 122$ is the least solution and the other solutions are given by $x = 22 + 156y$.

Question 25. Show that $2^{2n+1} - 9n^2 + 3n - 2$ is divisible by 54.

Solution. Let, $f(n) = 2^{2n+1} - 9n^2 + 3n - 2$
Then $f(1) = 8 - 9 + 3 - 2 = 0$ is divisible by 54.
Now,

$$
\begin{aligned}
f(n+1) - f(n) &= 2^{2n+3} - 9(n+1)^2 + 3(n+1) - 2 - 2^{2n+1} + 9n^2 - 3n + 2 \\
&= 2^2 \cdot 2^{2n+1} - 2^{2n+1} - 18n - 6 \\
&= 3 \cdot 2^{2n+1} - 18n - 6 \\
&= 6(2^2)^n - 18n - 6 \\
&= 6(3+1)^n - 18n - 6 \\
&= 6\left[(1 + 3\,{}^nC_1 + {}^nC_2 3^{n-2} + {}^nC_3 3^{n-3} + \cdots + 3^n)\right] - 18n - 6 \\
&= 6\left({}^nC_2 3^{n-2} + {}^nC_3 3^{n-3} + \cdots + 3^n\right) \\
&= 54\left({}^nC_2 3^{n-4} + {}^nC_3 3^{n-5} + \cdots + 3^{n-2}\right) \\
&= 54k, \text{ where } k \text{ is an integer}
\end{aligned}
$$

Hence, if $f(n)$ is divisible by 54 then $f(n+1)$ is divisible by 54. Now, $f(1)$ is divisible by 54 so $f(1+1) = f(2)$ is divisible by 54. Thus, it follows that $f(3)$, $f(4)$, ... etc. are divisible by 54.
$\therefore$ $2^{2n+1} - 9n^2 + 3n - 2$ is divisible by 54.

Question 26. Prove that if a is an even integer, then $a(a^2 + 20)$ is divisible by 48.

Solution. Let $f(a) = a(a^2 + 20)$
$\therefore$ $f(2) = 2(2^2 + 20) = 48$ which is divisible by 48.
Now,

$$
\begin{aligned}
f(2n+2) - f(2n) &= (2n+2)\left\{(2n+2)^2 + 20\right\} - 2n\left(4n^2 + 20\right) \\
&= 24n^2 + 24n + 48 \\
&= 48\left(\frac{n^2 + n + 1}{2}\right) \\
&= 48k
\end{aligned}
$$

Hence if $f(2n)$ is divisible by 48 then $f(2n+2)$ is also divisible by 48.
Now, $f(2 \cdot 1) = f(2) = 48$ is divisible by 48 so $f(2 \cdot 1 + 2) = f(4)$ is divisible by 48 and hence by succession we get $f(6)$, $f(8)$, ... etc. are divisible by 48.

Question 27. Using Chinese remainder theorem, solve $13x \equiv 17 \pmod{42}$.

Question 28. Solve $x \equiv 5 \pmod{6}$ and $x \equiv 8 \pmod{15}$.

Question 29. Find the four roots of the congruence $x^2 \equiv -1 \pmod{65}$.

Solution.

$$
\begin{aligned}
& x^2 \equiv -1 \pmod{65} \\
\Rightarrow\ & x^2 \equiv -1 + 65 \pmod{65} \\
\Rightarrow\ & (x-8)(x+8) \equiv 0 \pmod{65}
\end{aligned}
$$

Now, $x \equiv 8 \pmod{65}$ and $x \equiv -8 \pmod{65}$.
Since $65 = 5 \times 13$ and 5, 13 are relatively prime to each other.

$$
\therefore \begin{aligned} x &\equiv 8 \pmod{5} \\ x &\equiv 8 \pmod{13} \end{aligned} \quad \text{or} \quad \begin{aligned} x &\equiv -8 \pmod{5} \\ x &\equiv -8 \pmod{13} \end{aligned}
$$

Now, we shall use solve these congruences by Chinese remainder theorem.

$$
\begin{aligned}
x &\equiv 8 \equiv 3 \pmod{5} \qquad & m_1 = 5,\ m_2 = 13,\ m = 65 \\
x &\equiv 8 \pmod{13} \qquad & a_1 = 3,\ a_2 = 8 \\
& & Q_1 = 13,\ Q_2 = 5
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
& 13y_1 \equiv 1 \pmod{5} \\
\Rightarrow\ & y_1 \equiv 2 \pmod{5} \\
& 5y_2 \equiv 1 \pmod{13} \\
& 26y_2 - y_2 \equiv 5 \pmod{13} \\
\Rightarrow\ & -y_2 \equiv 5 \pmod{13} \\
\text{i.e., }\ & y_2 \equiv 8 \pmod{13} \\
\therefore\ & x = 78 + 320 = 398 \equiv 8 \pmod{65}
\end{aligned}
$$

Thus, $x = 8$ is a solution of the congruence $x^2 \equiv -1 \pmod{65}$ and $65 - 8 = 57$ is —- root of this congruence.

Again,

$$
\begin{aligned}
x &\equiv -8 \equiv 3 \pmod{5} \qquad & m_1 = 5,\ m_2 = 13,\ m = 65 \\
x &\equiv -8 \equiv 5 \pmod{13} \qquad & a_1 = 3,\ a_2 = 5 \\
& & Q_1 = 13,\ Q_2 = 5
\end{aligned}
$$

Consider,

$$
\begin{aligned}
& 13y_1 \equiv 1 \pmod{5} \\
\Rightarrow\ & y_1 \equiv 2 \pmod{5} \\
\text{and }\ & 5y_2 \equiv 1 \pmod{13} \\
& y_2 \equiv 8 \pmod{13}
\end{aligned}
$$

$\therefore\ x = 78 + 200 = 278 \equiv 18 \pmod{65}$
Hence, the other solution of $x^2 \equiv -1 \pmod{65}$ is $65 - 18 = 47$.
Hence, the four roots of the congruence $x^2 \equiv -1 \pmod{65}$ is 8, 18, 47, 57.

Question 30. Find the four roots of the congruence $x^2 \equiv -2 \pmod{33}$.

Solution.

$$\begin{aligned}
& x^2 \equiv -2 \pmod{33} \\
\Rightarrow\ & x^2 \equiv -2 \pmod{3} \\
& x^2 \equiv -2 \pmod{11} \qquad \text{as } (3, 11) = 1 \text{ and } 3 \times 11 = 33
\end{aligned}$$

Now,

$$\begin{aligned}
& x^2 \equiv -2 \pmod{3} \\
\Rightarrow\ & x^2 \equiv 16 \pmod{3} \\
\Rightarrow\ & x \equiv 4 \pmod{3} \\
\Rightarrow\ & x \equiv 1 \pmod{3}
\end{aligned}$$

Again,

$$\begin{aligned}
& x^2 \equiv -2 \pmod{11} \\
\Rightarrow\ & x^2 \equiv 9 \pmod{11} \\
\Rightarrow\ & x \equiv 3 \pmod{11}
\end{aligned}$$

Thus, solving $x \equiv 1 \pmod{3}$ and $x \equiv 3 \pmod{11}$ by Chinese remainder theorem, we get 8, 14, 19, 25 are the four incongruent roots of $x^2 \equiv -2 \pmod{33}$.

Question 31. Find the four roots of the congruence $x^2 \equiv 9 \pmod{16}$

Solution. Given, $\quad x^2 \equiv 9 \pmod{16}$

$$\Rightarrow x^2 \equiv (\pm 3)^2 \pmod{16}$$

So, roots of the given congruence are ± 3.
The other root is $16 - 3 = 13$ of $x^2 \equiv 9 \pmod{16}$
So, $3, 13$ are two roots of the congruence $x^2 \equiv 9 \pmod{16}$.
Again, Since,

$$\begin{aligned}
& x^2 \equiv 9 \pmod{16} \\
\therefore\ & x^2 \equiv 9 \pmod{8}
\end{aligned}$$

Now, another roots of the given congruence will be $\pm 3 + 8k$ where $k = 0, 1$
For $k = 0$, $x = \pm 3 + 0 = 3,\ -3 = 3,\ 16 - 3 = 3, 13$
For $k = 1$, $x = \pm 3 + 8 = 11, 5$
So, $x^2 \equiv 9 \pmod{16}$
Therefore, the four roots of the congruence $x^2 \equiv 9 \pmod{16}$ are $3, 5, 11, 13$.

Question 32. If p is a prime of the form $4n + 3$, show that $(2n + 1)!$ is a root of the congruence $x^2 \equiv 1 \pmod{p}$

Solution. Since p is a prime of the form $4n + 3$,
We have,

$$\begin{aligned}
& 4n + 3 \equiv 0 \pmod{p} \\
\Rightarrow\ & -3 \equiv 4n \pmod{p}
\end{aligned}$$

Now,

$$
\begin{aligned}
&-1 \equiv 4n+2 \pmod p\\
&-2 \equiv 4n+1 \pmod p\\
&-3 \equiv 4n \pmod p\\
&-4 \equiv 4n-1 \pmod p\\
&\dots \quad \dots \quad \dots\\
&-(2n+1) \equiv 4n+\{-(2n+1)+3\} \pmod p\\
\text{i.e.,}\quad &-(2n+1) \equiv 2n+2 \pmod p
\end{aligned}
$$

Multiplying both sides we get,

$$
\begin{aligned}
&(-1)^{2n+1}\{1\cdot 2\cdot 3\cdot \dots (2n+1)\} \equiv (4n+2)(4n+1)(4n)(4n-1)\dots(2n+2) \pmod p\\
\Rightarrow\ &-(2n+1)! \equiv \frac{(4n+2)(4n+1)(4n)\dots(2n+2)(2n+1)(2n-1)(2n-2)\dots 2\cdot 1}{(2n+1)\dots 3\cdot 2\cdot 1} \pmod p\\
\Rightarrow\ &-(2n+1)!^2 \equiv (4n+2)! \pmod p \qquad (12)
\end{aligned}
$$

Again, since p is a prime of the form $4n+3$, by Wilson's theorem we have,

$$
\begin{aligned}
&(4n+3-1)!+1 \equiv 0 \pmod p\\
&(4n+2)!+1 \equiv 0 \pmod p \qquad (13)
\end{aligned}
$$

From (12) and (13),

$$
\begin{aligned}
&-(2n+1)!^2 \equiv -1 \pmod p\\
\Rightarrow\ &(2n+1)!^2 \equiv 1 \pmod p\\
\therefore\ &x^2 \equiv 1 \pmod p \qquad \text{where, } x=(2n+1)!
\end{aligned}
$$

Thus, $x=(2n+1)!$ is a root of the congruence $x^2 \equiv -1 \pmod p$.

Question 33. If p is an odd prime and $h+k=p-1$ prove that $h!k!+(-1)^h \equiv 0 \pmod p$.

Solution. If p is a prime of the form $h+k+1=p$ then we can write,

$$
\begin{aligned}
h+k+1 &\equiv 0 \pmod p\\
h+1 &\equiv -k \pmod p\\
h+2 &\equiv -(k-1) \pmod p\\
h+3 &\equiv -(k-2) \pmod p\\
h+4 &\equiv -(k-3) \pmod p\\
\dots \quad &\dots \quad \dots\\
h+k &\equiv -1 \pmod p
\end{aligned}
$$

Multiplying the above congruences, we get

$$
\begin{aligned}
&(h+1)(h+2)(h+3)\dots(h+k) \equiv (-1)^k k! \pmod p\\
\Rightarrow\ &h!\,(h+1)(h+2)(h+3)\dots(h+k) \equiv (-1)^k\,k!\,h! \pmod p\\
\Rightarrow\ &(h+k)! \equiv (-1)^k\,k!\,h! \pmod p \qquad (14)
\end{aligned}
$$

Again p is a prime of the form $h+k+1$, so by Wilson's theorem we have,

$$\begin{aligned}(h+k+1-1)! &\equiv -1 \pmod p\\ \text{i.e., } (h+k)! &\equiv -1 \pmod p \end{aligned} \tag{15}$$

Hence, by (14) and (15), we write,

$$(-1)^k\, h!\; k! \equiv -1 \pmod p$$

Since, p is a prime, $(-1) = (-1)^{k+h+1}$

$$\begin{aligned}\therefore (-1)^k\, h!\; k! &\equiv (-1)^{k+h+1} \pmod p\\ \Rightarrow (-1)^h + h!\; k! &\equiv 0 \pmod p\end{aligned}$$

Question 34. Prove/Find the number of divisors and sum of divisors if a composite number.

Solution.

- The function $d(n)$ is the number of divisors of the composite number n including 1 and n.
- The function $\sigma(n)$ is the sum of the divisors of the composite number n.

Consider the factorization of the composite number n into primes be $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\dots{p_r}^{\alpha_r}$ where ${p_r}^{\alpha}$s are pairwise relatively prime.
Then, the divisors of ${p_1}^{\alpha_1}$ are $1, p_1, p_1^2, \dots, {p_1}^{\alpha_1}$.
Therefore, $d\left({p_1}^{\alpha_1}\right) = \alpha_1 + 1$ and hence,

$$\begin{aligned} d\left(n\right) &= d\left({p_1}^{\alpha_1}\right) d\left({p_2}^{\alpha_2}\right)\dots d\left({p_r}^{\alpha_r}\right)\\ &= (\alpha+1)(\alpha+1)\dots(\alpha+1)\\ &= \prod_{i=1}^{r}(\alpha_i+1)\end{aligned}$$

Now, sum of the divisors of ${p_1}^{\alpha_1}$ is $1 + p_1 + p_1^2 + \dots + {p_1}^{\alpha_1} = \frac{{p_1}^{\alpha_1+1}-1}{p_1-1}$.
i.e., $\sigma\left({p_1}^{\alpha_1}\right) = \frac{{p_1}^{\alpha_1+1}-1}{p_1-1}$
and therefore,

$$\begin{aligned}\sigma\left(n\right) &= \sigma\left({p_1}^{\alpha_1}\right)\sigma\left({p_2}^{\alpha_2}\right)\dots\sigma\left({p_r}^{\alpha_r}\right)\\ &= \frac{{p_1}^{\alpha_1+1}-1}{p_1-1}\cdot\frac{{p_2}^{\alpha_2+1}-1}{p_2-1}\dots\frac{{p_r}^{\alpha_r+1}-1}{p_r-1}\\ &= \prod_{i=1}^{r}\left(\frac{{p_i}^{\alpha_i+1}-1}{p_i-1}\right)\end{aligned}$$

Question 35. Show that

$$\sum_{d/n}\{f(d)\}^3 = \left\{\sum_{d/n} f(d)\right\}^2$$

Solution.
Left-Hand side.
Suppose that $n = p^k$. Since $f(d)$ is multiplicative function and $f(d)$ denotes the numbers of divisors of n.

$$\begin{aligned}
\therefore \sum_{d/n} \{f(d)\}^3 &= \{f(1)\}^3 + \{f(p)\}^3 + \left\{f(p^2)\right\}^3 + \cdots + \left\{f(p^k)\right\}^3 \\
&= 1^3 + 2^3 + 3^3 + \cdots + (k+1)^3 \\
&= \left\{\frac{(k+1)(k+2)}{2}\right\}^2
\end{aligned}$$

Right-Hand side.

$$\begin{aligned}
\therefore \left\{\sum_{d/n} f(d)\right\}^2 &= \left\{f(1) + f(p) + f(p^2) + \cdots + f(p^k)\right\}^2 \\
&= \{1 + 2 + 3 + \cdots + (k+1)\}^2 \\
&= \left\{\frac{(k+1)(k+2)}{2}\right\}^2
\end{aligned}$$

Hence proved.

Question 36. If a is an even number then show that $48 \mid a(a^2 + 20)$.

Solution. We have,

$$\begin{aligned}
p &= a\left(a^2 + 20\right) \\
&= a\left(a^2 - 4 + 24\right) \\
&= a\left((a-2)(a+2) + 24\right) \\
&= (a-2)(a)(a+2) + 24a
\end{aligned}$$

Now, since a is an even number so let $a = 2n$ for any integer n.
Then,

$$\begin{aligned}
p &= (2n-2)(2n)(2n+2) + 48a \\
&= 8(n-1)(n)(n+1) + 48a
\end{aligned}$$

Now, since $(n-1)\ n\ (n+1)$ is the product of three consecutive integers, so it is divisible by $3! = 6$. And hence $8(n-1)(n)(n+1)$ is divisible by $8 \times 6 = 48$. Again $48a$ is —— divisible by 48. Hence, the term $p = a(a^2 + 20)$ is divisible by 48.

Question 37. If n is an odd integer, $n(n^2 + 1)$ is divisible by 24.

Solution. Since, n is odd integer so $n-1$ and $n+1$ are two consecutive integers and hence one of them is divisible by 2 and the other is divisible by 4.

Again, $(n-1), n, (n+1)$ are three consecutive integers so one of them is divisible by 3. Thus, the given expression is divisible by 2, 3 and 4 and hence by their product 24.

Question 38. Find $d(n)$ and $\sigma(n)$ for $n = 21600$.

Solution. Here, $n = 21600 = 2^5 \cdot 3^3 \cdot 5^2$

$$\begin{aligned}\therefore d(n) &= \text{ number of divisors of } n \\ &= \prod_{i=1}^{3}(\alpha_i + 1) \\ &= (5+1)(3+1)(2+1) \\ &= 72\end{aligned}$$

And,

$$\begin{aligned}\therefore \sigma(n) &= \text{ sum of the divisors} \\ &= \prod_{i=1}^{3} \frac{{p_i}^{\alpha_i+1} - 1}{p_i - 1} \\ &= \frac{2^6 - 1}{2 - 1} \cdot \frac{3^4 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} \\ &= 78120\end{aligned}$$

Question 39. Find the positive integer solution of the linear Diophantine equation $62x + 11y = 788$.

Solution. Here, $a = 62$, $b = 11$, and $c = 788$.
Now using Euclid's algorithm,

$$\begin{aligned}62 &= 11 \cdot 5 + 7 \\ 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0\end{aligned}$$

Now, $(62, 11) = 1$ and $1 \mid 788$, so it has a solution.
Now,

$$\begin{aligned}1 &= 4 + 3 \cdot (-1) \\ &= 4 + (-1)\{7 + 4 \cdot (-1)\} \\ &= 2 \cdot 4 + (-1) \cdot 7 \\ &= 2\{11 + (-1) \cdot 7\} + (-1) \cdot 7 \\ &= 2 \cdot 11 + (-3) \cdot 7 \\ &= 2 \cdot 11 + (-3)\{62 + 11 \cdot (-5)\} \\ &= 11(17) + 62(-3) \\ \Rightarrow\ 62(-2364) + 11(13396) &= 788\end{aligned}$$

Hence, $x_0 = -2364$ and $y_0 = 13396$ is a particular solution of $62x + 11y = 788$.
Hence, the general solution of the given linear Diophantine equation is given by $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$.

Where t is an integer.
i.e., $x = -2364 + 11t$ and $y = 13396 - 62t$.
Hence, the positive integral solutions are given by

$$\begin{aligned} &-2364 + 11t > 0 \qquad \text{and} \qquad 13396 - 62t > 0 \\ &\Rightarrow t > 214.91 \qquad \text{and} \qquad t < 216.0645 \end{aligned}$$

Now, $214.91 < t < 216.0645$ and since t is integer, so we conclude that $t = 215$ and 216.
Hence, the positive integral solution is

(i) $x = 1$, $y = 66$ and

(ii) $x = 12$, $y = 4$

Theorem 0.0.1. If p is a prime then

$$\sum_{i=0}^{\alpha} \phi\left(p^i\right) = p^{\alpha}$$

Proof.

$$\begin{aligned} \sum_{i=0}^{\alpha} \phi\left(p^i\right) &= \phi\left(p^0\right) + \phi\left(p\right) + \phi\left(p^1\right) + \cdots + \phi\left(p^{\alpha}\right) \\ &= 1 + (p-1) + p^2\left(1 - \frac{1}{p}\right) + p^3\left(1 - \frac{1}{p}\right) + \cdots + p^{\alpha}\left(1 - \frac{1}{p}\right) \\ &= 1 + (p-1) + p\,(p-1) + p^2\,(p-1) + \cdots + p^{\alpha-1}\,(p-1) \\ &= 1 + (p-1)\frac{p^{\alpha-1+1} - 1}{p-1} \\ &= p^{\alpha} \end{aligned}$$

□

Properties of Legendre Symbol

Theorem 0.0.2. If p is an odd prime and $(a, p) = 1$, $(b, p) = 1$ then

(i) $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

(ii) $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right) = \left(\dfrac{ab}{p}\right)$

(iii) $a \equiv b \pmod p$ implies $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$

(iv) $\left(\dfrac{a^2}{p}\right) = 1$; $\left(\dfrac{a^b}{p}\right) = \left(\dfrac{b}{p}\right)$; $\left(\dfrac{1}{p}\right) = 1$, $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(v) $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

(vi) If p and q are distinct odd prime then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

Question 40. Find: 1. $\left(\frac{231}{997}\right)$ 2. $\left(\frac{3}{101}\right)$ 3. $\left(\frac{60}{29}\right)$ 4. $\left(\frac{20}{7}\right)$ 5. $\left(\frac{85}{11}\right)$ 6. $\left(\frac{100}{7}\right)$

Solution.

1. Here 231 and 997 are two distinct odd primes, so

$$\begin{aligned}\left(\frac{231}{997}\right) &= \left(\frac{997}{231}\right)(-1)^{\left(\frac{231-1}{2}\right)\left(\frac{997-1}{2}\right)}\\ &= \left(\frac{73}{231}\right)(-1)^{(115)(498)}\\ &= \left(\frac{231}{73}\right)(-1)^{(115)(36)}\\ &= \left(\frac{12}{73}\right)\end{aligned}$$

Now, by Jacobi symbol, we have

$$\left(\frac{12}{73}\right) = \left(\frac{1}{73}\right)\left(\frac{2^2}{73}\right)\left(\frac{3}{73}\right)$$

$$\begin{aligned}\therefore \left(\frac{1}{73}\right) &= 1;\\ \therefore \left(\frac{2^2}{73}\right) &= 1;\\ \therefore \left(\frac{3}{73}\right) &= \left(\frac{73}{3}\right)(-1)^{\left(\frac{3-1}{2}\right)\left(\frac{73-1}{2}\right)}\\ &= \left(\frac{1}{3}\right)\\ &= 1\end{aligned}$$

Hence, $\left(\frac{231}{997}\right) = \left(\frac{12}{73}\right) = \left(\frac{1}{73}\right) = \left(\frac{2^2}{73}\right)\left(\frac{3}{73}\right) = 1 \cdot 1 \cdot 1 = 1.$

2. $\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right)(-1)^{1\cdot 50} = \left(\frac{2}{3}\right) = (-1)^{\left(\frac{3^2-1}{8}\right)} = (-1)^{\frac{8}{9}} = -1$

3. $\left(\frac{60}{29}\right) = \left(\frac{1}{29}\right)\left(\frac{2^2}{29}\right)\left(\frac{3}{29}\right)\left(\frac{5}{29}\right)$

Now,

$$
\begin{aligned}
\left(\frac{1}{29}\right) &= 1; \\
\left(\frac{2^2}{29}\right) &= 1; \\
\left(\frac{3}{29}\right) &= (-1)^{14\cdot 1} \\
&= \left(\frac{2}{3}\right) \\
&= (-1)^{\frac{3^2-1}{8}} \\
&= -1 \\
\left(\frac{5}{29}\right) &= \left(\frac{29}{5}\right)(-1)^{2\cdot 14} \\
&= \left(\frac{4}{5}\right) \\
&= \left(\frac{2^2}{5}\right) \\
&= 1
\end{aligned}
$$

$\therefore \left(\frac{60}{29}\right) = 1 \cdot 1 \cdot -1 \cdot 1 = -1$

4.

$$\left(\frac{20}{7}\right) = \left(\frac{1}{7}\right)\left(\frac{2^2}{7}\right)\left(\frac{5}{7}\right)$$

$$\left(\frac{1}{7}\right) = 1,\ \left(\frac{2^2}{7}\right) = 1,\ \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)(-1)^{2\cdot 3} = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$

$\therefore \left(\frac{20}{7}\right) = 1 \cdot 1 \cdot -1 = -1.$

5.

$$
\begin{aligned}
\left(\frac{85}{11}\right) &= \left(\frac{8}{11}\right) \text{ as } x^2 \equiv 85 \pmod{11} \Rightarrow\ x^2 \equiv 8 \pmod{11} \\
&= \left(\frac{2^2\cdot 2}{11}\right) \\
&= \left(\frac{2}{11}\right) \text{ as } \left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right) \\
&= (-1)^{\frac{11^2-1}{8}} \\
&= (-1)^{15} \\
&= -1
\end{aligned}
$$

6. $\left(\frac{100}{7}\right) = \left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = (-1)^6 = 1$

Question 41. Find the values $d\,(1968)$, $d\,(255)$, $d\,(111)$, $d\,(353650)$, $\sigma\,(1968)$, $\sigma\,(255)$, $\sigma\,(111)$, $\sigma\,(353650)$, $\mu\,(25)$, $\mu\,(235)$, $\mu\,(300)$.

Solution. Here,

$$\begin{aligned}
1968 &= 3 \cdot 4^2 \cdot 41 = 2^4 \cdot 3^1 \cdot 41^1 \\
255 &= 3 \cdot 5 \cdot 17 \\
111 &= 3 \cdot 37 \\
353650 &= 2 \cdot 5^2 \cdot 11 \cdot 643 \\
25 &= 5^2 \\
235 &= 5 \cdot 47 \\
300 &= 3 \cdot 4 \cdot 5^2 = 2^2 \cdot 3^1 \cdot 5^2
\end{aligned}$$

$$\begin{aligned}
\therefore\ d\,(1968) &= d\left(2^4 \cdot 3^1 \cdot 41^1\right) = (1+1)(4+1)(1+1) = 20 \\
\therefore\ d\,(255) &= d\,(3 \cdot 5 \cdot 13) = (1+1)(1+1)(1+1) = 8 \\
\therefore\ d\,(111) &= d\,(3 \cdot 37) = 4 \\
\therefore\ d\,(353650) &= d\left(2 \cdot 5^2 \cdot 11 \cdot 643\right) = (1+1)(2+1)(1+1)(1+1) = 24 \\
\therefore\ \sigma\,(353650) &= \sigma\left(2^4 \cdot 3^1 \cdot 41^1\right) = \prod_{i=1}^{3} \frac{p_i^{\alpha_i+1}-1}{p_i-1} \\
&= \left(\frac{3^{1+1}-1}{3-1}\right)\left(\frac{2^{4+1}-1}{2-1}\right)\left(\frac{41^{1+1}-1}{41-1}\right) \\
&= \frac{8}{2} \cdot 31 \cdot \frac{1680}{40} = 5208 \\
\therefore\ \sigma\,(255) &= \sigma\,(3 \cdot 5 \cdot 17) = \left(\frac{3^2-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)\left(\frac{17^2-1}{17-1}\right) = 432 \\
\therefore\ \sigma\,(111) &= \sigma\,(3 \cdot 37) = \left(\frac{3^2-1}{3-1}\right)\left(\frac{37^2-1}{37-1}\right) = 152 \\
\therefore\ \sigma\,(353650) &= \sigma\left(2 \cdot 5^2 \cdot 11 \cdot 643\right) = \left(\frac{2^3-1}{2-1}\right)\left(\frac{5^3-1}{5-1}\right)\left(\frac{11^2-1}{11-1}\right)\left(\frac{643^2-1}{643-1}\right) = 1676976 \\
\therefore\ \mu\,(25) &= \mu\left(5^2\right) = 0 \qquad \text{as } \mu\,(n) = 0 \text{ if } a^2 \mid n \text{ where } a > 1 \\
\therefore\ \mu\,(235) &= \mu\,(5 \cdot 47) = (-1)^2 = 1 \\
\therefore\ \mu\,(300) &= \mu\left(2^2 \cdot 3 \cdot 5^2\right) = (-1)^3 = -1
\end{aligned}$$

Question 42 (T-3)**.** Find the positive integral solution of the linear Diophantine equation $20x+7y = 30$.

Solution. Here, $a = 20$, $b = 7$, $c = 30$
Then applying Euclid's algorithm, we get

$$\begin{aligned}
20 &= 7 \cdot 2 + 6 \\
7 &= 6 \cdot 1 + 1 \\
6 &= 1 \cdot 6 + 0
\end{aligned}$$

Hence, $(20,7)=1$ and $1 \mid 30$ so a solution of $20x+7y=30$ exists.
Using steps of Euclid's algorithm, 1 can be written as a linear combination of 20 and 7.

$$\begin{aligned}
1 &= 7+(-1)\cdot 6 \\
&= 7+(-1)\{20+(-2)\cdot 7\} \\
&= 7(3)+20(-1) \\
\Rightarrow\ 20(-30)+7(90) &= 30
\end{aligned}$$

Hence, $x_0=-30$ and $y_0=90$ is a particular solution of $20x+7y=30$, and hence the general solution is given by

$$\begin{aligned}
x = x_0+\frac{b}{d}t;\ \ y=y_0-\frac{a}{d}t \qquad &\text{where } t \text{ is an integer} \\
\text{i.e., } x=-30+7t,\ y=90-20t &
\end{aligned}$$

The positive integral solution is given by the system of inequalities

$$\begin{aligned}
-30+7t &> 0 \\
90-20t &> 0 \\
\Rightarrow t > 4.28 \text{ and } t &< 4.5
\end{aligned}$$

Hence, $4.28 < t < 4.5 \ \Rightarrow\ t=4$ as t is an integer or $t=5$

(i) $x=-30+7\cdot 4=-2$ and $y=70-20\cdot 4=10$

(ii) $x=5$ and $y=-10$

Hence, there is no positive integral solution of the given linear Diophantine equation.

Question 43. Show that $3^{2n}-32n^2+24n-1=M(5/2)$

Question 44. Solve the congruence $7x \equiv 15 \pmod{40}$

Question 45 (100E)**.** Solve

$$\begin{aligned}
x &\equiv 7 \pmod{30} \\
x &\equiv 25 \pmod{42} \\
x &\equiv 37 \pmod{45}
\end{aligned}$$

Solution. Alternative method except Chinese Remainder method:

$$\begin{aligned}
x &\equiv 7 \pmod{30} && (16) \\
x &\equiv 25 \pmod{42} && (17) \\
x &\equiv 37 \pmod{45} && (18)
\end{aligned}$$

From (16),

$$x = 7+30t \tag{19}$$

where t is integer and putting this in (17) we get,

$$\begin{aligned}
&7+30t \equiv 25 \pmod{42}\\
\Rightarrow\ &30t \equiv 25-7 \pmod{42}\\
\Rightarrow\ &30t \equiv 18 \pmod{42} \qquad \left[(30,42)=6,\ \therefore\ \left(\frac{30}{6},\frac{42}{6}\right)=1\right]\\
\Rightarrow\ &5t \equiv 3 \pmod{7}\\
\Rightarrow\ &t \equiv 2 \pmod{7}
\end{aligned}$$

Now, $t = 2+7u$, u is any integer and putting in (19) we get

$$x = 7+30(2+7u) = 67+210u$$

Putting this value in (18) we get,

$$\begin{aligned}
&210u \equiv -30 \pmod{45}\\
\Rightarrow\ &14u \equiv -2 \pmod{3}\\
\Rightarrow\ &-u \equiv -2 \pmod{3} \qquad \text{as } 144 \equiv -u \pmod{3}\\
\Rightarrow\ &u \equiv 2 \pmod{3}
\end{aligned}$$

Now, $u = 2+3v$, where v is integer

$$\begin{aligned}
&\therefore x = 67+210(2+3v) = 487+630v\\
\Rightarrow\ &x \equiv 487 \pmod{630}
\end{aligned}$$

Question 46 (100E)**.** Solve $371x \equiv 287 \pmod{460}$.

Solution. Given,

$$371x \equiv 287 \pmod{460} \tag{20}$$

Here, $460 = 4\cdot 5\cdot 23$
$\therefore$ (20) can be written as

$$\begin{aligned}
371x &\equiv 287 \pmod{4}\\
371x &\equiv 287 \pmod{5}\\
371x &\equiv 287 \pmod{23}
\end{aligned}$$

$$\text{i.e., } 3x \equiv 3 \pmod{4} \Rightarrow x \equiv 1 \pmod{4} \tag{21}$$
$$x \equiv 2 \pmod{5} \tag{22}$$
$$3x \equiv 11 \pmod{23} \tag{23}$$

From (21) $x = 1+4t$, t is an integer and putting this in (22)

$$\begin{aligned}
4t &\equiv 1 \pmod{5}\\
t &\equiv 4 \pmod{5}
\end{aligned}$$

Now, taking $t = 4 + 5u$, we have $x = 17 + 20u$ and putting this value in (5)

$$\begin{aligned} 60u &\equiv -40 \pmod{23} \\ 3u &\equiv -2 \pmod{23} \\ u &\equiv 7 \pmod{23} \end{aligned}$$

Putting $u = 7 + 23v$ we have, $x = 157 + 460v$.
$\therefore\ x \equiv 157 \pmod{460}$ is the required solution of (20).

Question 47. If n is an integer, then prove that one of n, $n+2$, $n+4$ is divisible by 3.

Solution.
Here, n must be any one of the form $3m$, $3m+1$, $3m+2$.
At $n = 3m$, the first number is divisible by 3.
At $n = 3m+1$, $n+2 = 3(m+1)$ is divisible by 3.
At $n = 3m+2$, $n+4 = 3(m+2)$ is divisible by 3.

Question 48 (C.H.88 E)**.** Show that $a^x + a$ and $a^x - a$ are always even, whatever a and x may be.

Solution. If a is odd, then a^x is odd, hence $a^x + a$ and $a^x - a$ are both even, for all values of x.
If a is even, then a^x is even and hence $a^x + a$ and $a^x - a$ are both even, for all values of x.

Hence, the problem is shown in proof.

Question 49 (I)**.** Show that the sum of the integers less than n and prime to n is $\frac{1}{2}n\phi(n)$ if $n \geq 2$.

Solution. Let x is any integer less than n and prime to n, then $n - x$ is also an integer less than n and prime to it.[1]

Denote the integers by 1, p, q, $r, \ldots$ and their sum by S; then

$$S = 1 + p + q + r + \cdots + (n-p) + (n-q) + (n-r) + (n-1)$$

Which is the series consisting of $\phi(n)$ terms.
Rearranging, we have

$$\begin{aligned} S &= (n-1) + (n-p) + (n-q) + (n-r) + \cdots + r + q + p + 1 \\ \therefore\ 2S &= n + n + n + n + \ldots \text{ upto } \phi(n) \text{ terms } = n\phi(n) \\ \therefore\ S &= \frac{1}{2}n\phi(n) \end{aligned}$$

Theorem 0.0.3 (E). The product of any r consecutive (integer) number is divisible by $r!$.

---

1 $8 = \overbrace{1, 3, 5, 7}^{x}$
$\therefore\ 8 - x = 8 - 5 = 3$
$\therefore\ (8, 3) = 1$

Proof. Let n be the first number if the r consecutive integers.
Then

$$\begin{aligned}&\frac{n(n+1)(n+2)\dots(n+r-1)}{r!}\\ =&\frac{(n+r-1)(n+r-2)\dots(n+2)(n+1)n(n-1)!}{r!(n-1)!}\\ =&\frac{(n+r-1)!}{r!(n-1)!}\\ =&{}^{n+r-1}C_r\end{aligned}$$

Which is the number of combination of $(n+r-1)$ things taken r at a time and to an integer. Hence, the theorem is complete. $\square$

Question 50 (T-1)**.** Show that $n^5 - n$ is divisible by 30.

Solution. As 5 is a prime, $n^5 - n = x(5) =$ multiple of 5.[2]
Again, $n^5 - n = n(n^2+1)(n+1)(n-1) = (n-1)n(n+1)(n^2+1)$
Since, $(n-1)n(n+1)$ is the product of three consecutive integers so it is divisible by $3! = 6$.
Therefore, (n^2+1) is divisible by 5, and hence $n^5 - n$ is divisible by $6 \times 5 = 30$.

Question 51 (I)**.** Show that $n(n+1)(2n+1)$ is divisible by 6.

Solution. In the expression $n(n+1)(2n+1)$, n must be of the form $6m$, $6m+1$, $6m+2$.
Now,
when $n = 6m$, $n(n+1)(2n+1) = 6m(6m+1)(12m+1)$ which is divisible by 6.
when $n = 6m+1$, $n(n+1)(2n+1) = (6m+1)(6m+2)(12m+2+1) = (6m+1)(m+1)(4m+1)\cdot 2\cdot 3$ which is divisible by 6.
when $n = 6m+2$, $n(n+1)(2n+1) = (6m+2)(6m+3)(12m+5) = 3\cdot 2\cdot(3m+1)(2m+1)(12m+5)$ which is divisible by 6.

Thus, $n(n+1)(2n+1)$ is divisible by 6.

[2] x maybe changed to m/M?