# Question Bank on Number Theory

Sudev N.K.

*Department of Mathematics*
*CHRIST (Deemed to be University)*
*Bengaluru-560029, Karnataka, India.*
sudevnk@gmail.com

## Unit 1

**(4 marks Questions)**

1. If $a|b,\ c|d$, then show that $ac|bd$.
2. If $a|b,\ a|c$, then show that $a|bc$.
3. Show that $a|b$ and $b|a$ if and only if $a = \pm b$.
4. For any integer $a$, show that $5a + 2$ and $7a + 3$ are relatively prime.
5. If $a|b,\ b|c$ and $(a, b) = 1$, show that $ab|c$.
6. For two integers $a$ and $b$, not both of which are zero, show that there exist integers $x$ and $y$ such that $\gcd(a, b) = ax + by$.
7. For two integers $a$ and $b$, not both of which are zero, show that the set $T = \{ax + by : x, y \in \mathbb{Z}\}$ is precisely the set of multiples of $\gcd(a, b)$.
8. If $(a, b) = d$, then show that $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.
9. Explain Euclidean algorithm to find GCD of two integers.
10. If $(a, b) = 1$ and $c|a$, verify whether $(b, c) = 1$.
11. If $(a, b) = 1$, verify whether $(ac, b) = (c, b)$.
12. If $(a, b) = 1$, then show that $(a^2, b^2) = 1$.
13. Show that $\text{lcm}(a, b) = ab$ if and only if $a$ and $b$ are relatively prime.
14. Show that $\gcd(a, b)$ divides $\text{lcm}(a, b)$.
15. Show that $\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$.
16. Using Euclidean Algorithm, find the LCM of 306 and 657.

17. Using Euclidean Algorithm, find the LCM of 272 and 1479.
18. For any $k \neq 0$, show that $(ak, bk) = |k|(a, b)$.
19. Let $p$ be a prime number. If $p|ab$, then either $p|a$ or $p|b$.
20. If $p, q_1, q_2, \ldots, q_n$ are all primes and $p|q_1q_2q_3\ldots q_n$, show that $p|q_k$ for some $k$, where $1 \leq k \leq n$.

**(8 Mark Questions)**

1. Show that if $a$ is odd, then $32|(a^2+3)(a^2+7)$.
2. For $n \geq 1$, show that $21|4^{n+1} + 5^{2n-1}$.
3. For $n \geq 1$, show that $3^{3n+1} + 2^{n+1}$ is divisible by 5.
4. Show that the product of three consecutive integers is divisible by 6.
5. Show that the product of four consecutive integers is divisible by 24.
6. State and prove division algorithm.
7. Find integers $x$ and $y$ such that $(1769, 2378) = 1769x + 2378y$.
8. Find integers $x$ and $y$ such that $(119, 272) = 119x + 272y$.
9. Determine all integer solutions of the Diophantine equation $172x + 20y = 1000$.
10. Determine all integer solutions of the Diophantine equation $51x + 21y = 906$.
11. Show that $\sqrt{2}$ is irrational.
12. For any prime $p$, show that $\sqrt{p}$ is irrational.
13. Show that if $d$ is a common divisor of $a$ and $b$, $\gcd(a, b) = d$ if and only if $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

**(10 Mark Questions)**

1. (a) Show that the sum of squares of two odd integers cannot be a perfect square.
   (b) Show that the product of four consecutive integers is 1 less than a perfect square.
2. If $a$ and $b$ are integers, then
   (a) Show that there exists integers $x$ and $y$ for which $c = ax + by$ if and only if $\gcd(a, b)|c$.
   (b) Show that there exists integers $x$ and $y$ for which $\gcd(a, b) = ax + by$ if and only if $\gcd(x, y) = 1$.
3. State and prove fundamental theorem on arithmetic.

4. A customer bought a dozen of pieces of fruit, apples and oranges, for Rs. 132/-. If an apple costs Rs. 3/- more than an orange and more apples than oranges were bought, how many pieces of each kind were bought?

5. A neighbourhood theater charges Rs. 180/- for adult admission and Rs. 75/- for children. On a particular evening, the total receipts were Rs. 9000/-. Assuming that more adults than children were present, how many people were present?

# Unit 2

**(4 marks Questions)**

1. Show that $2^{20} \equiv 1 \pmod{41}$.
2. Find the remainder when $2^{1000}$ is divided by 17.
3. Find the remainder when the sum $1! + 2! + 3! + ... + 99! + 100!$ is divided by 12.
4. What is the remainder when the sum $1^5 + 2^5 + 3^5 + ... + 99^5 + 100^5$ is divided by 4?
5. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{\frac{n}{d}}$, where $d = \gcd(c, n)$.
6. If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.
7. If $ca \equiv cb \pmod{p}$ and $p \not| c$, where $p$ is a prime number, then $a \equiv b \pmod{p}$.
8. Show that $3^{n+2} + 4^{2n+1} \equiv 0 \pmod{13}$.
9. Show that $2^{5n+1} + 5^{n+2} \equiv 0 \pmod{27}$.
10. Show that $6^{n+2} + 7^{2n+1} \equiv 0 \pmod{43}$.
11. For $n \geq 1$, use congruence theory to show that $7 \mid 5^{2n} + 3 \,.\, 2^{5n-2}$.
12. If $p$ is a prime and $p$ does not divide $a$, then show that $a^{p-1} \equiv 1 \pmod{p}$.
13. If $p$ is a prime, show that $a^p \equiv a \pmod{p}$.
14. Use Fermat's Theorem to factor the numbers 2279 and 10541.
15. Factor $2^{11} - 1$ using Fermat's method.
16. Use generalised Fermat's method to factor 2911 and 4573.
17. Use Fermat's Theorem to verify that $11^{104} + 1$ is divisible by 17.
18. Using Fermat's Theorem, show for any integer that $13 | 11^{12n+6} + 1$.
19. If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$.
20. Solve the linear congruence $18x \equiv 30 \pmod{42}$.

21. Solve the linear congruence $140x \equiv 133 \pmod{301}$.

**(8 Mark Questions)**

1. Using theory of congruence, verify that
   (a) 89 divides $2^{44} - 1$.
   (b) 97 divides $2^{48} - 1$.
2. For any integer $a$, show that
   (a) $a^3 \equiv 0, 1, 6 \pmod{7}$.
   (b) $a^4 \equiv 0, 1 \pmod{5}$.
3. If $\gcd(a, 42) = 1$, then show that $168|a^6 - 1$.
4. If $\gcd(a, 133) = 1$, then show that $133|a^{18} - b^{18}$.
5. State and prove Wilson's Theorem.
6. Find the remainder when
   (a) $15!$ is divided by 17.
   (b) $2(26!)$ is divided by 29.
7. Let $n > 1$ be fixed and $a, b, c, d$ be arbitrary integers. Then prove that
   (a) if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
   (b) if $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.
8. Derive the following congruences:
   (a) $a^7 \equiv a (\text{mod } 42)$.
   (b) $a^{13} \equiv a (\text{mod } 3 \cdot 7 \cdot 13)$.
9. If $a \equiv b \pmod{n}$ and the integers $a, b, n$ are all divisible by $d > 0$, then show that $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.
10. Let $a \equiv b \pmod{n}$. Then, prove the following:
    (a) If $m|n$, then $a \equiv b \pmod{m}$.
    (b) If $c > 0$, then $ca \equiv cb \pmod{cn}$.
11. Use the binary exponentiation algorithm to compute $5^{110} \pmod{131}$.

**(10 Mark Questions)**

1. Given an integer $b > 1$, show that any positive integer $N$ can uniquely be written in powers of $b$ as $N = a_m b^m + a_{m-1} b^{m-1} + a_{m-2} b^{m-2} + \ldots + a_1 b + a_0$.

2. If $a, b$ and $n$ are positive integers such that $d|b$, where $d = \gcd(a, n)$. Then, show that the linear congruence $ax \equiv b(\text{mod } n)$ has $d$ mutually incongruent solutions modulo $n$.

3. If $a$ and $n$ are relatively prime, then show that the linear congruence $ax \equiv b\,(\text{mod } n)$ has a unique solution modulo $n$.

4. State and prove Chinese Remainder Theorem.

5. Using Chinese Remainder Theorem, solve the following simultaneous congruences:

$$\begin{aligned} x &\equiv 5(\text{mod } 6) \\ x &\equiv 4(\text{mod } 11) \\ x &\equiv 3(\text{mod } 17) \end{aligned}$$

6. Using Chinese Remainder Theorem, solve the following simultaneous congruences:

$$\begin{aligned} x &\equiv 5(\text{mod } 11) \\ x &\equiv 14(\text{mod } 29) \\ x &\equiv 15(\text{mod } 317) \end{aligned}$$

7. Let $a$ and $b$ are integers not divisible by the prime $p$, Then, prove the following:

   (a) If $a^p \equiv b^p\,(\text{mod } p)$, then $a \equiv b\,(\text{mod } p)$.

   (b) If $a^p \equiv b^p\,(\text{mod } p)$, then $a^p \equiv b^p\,(\text{mod } p^2)$.

# Unit 3

**(4 marks Questions)**

1. Calculate $\phi(1001)$, $\phi(5040)$.

2. For $n > 1$, the sum of the positive integers less than $n$ and relatively prime to $n$ is $\frac{1}{2}\,n\,\phi(n)$.

3. Show that the function $\tau(n)$ is multiplicative.

4. Show that the function $\sigma(n)$ is multiplicative.

5. Find the number of zeros with which the decimal representation of 50! terminates.

6. If $n$ and $r$ integers, then show that the binomial coefficient $\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$ is also an integer.

7. Show that $\phi(3n) = 3\phi(n)$ if and only if $3|n$.

8. Show that $\phi(3n) = 2\,\phi(n)$ if and only if $n$ is not a multiple of 3.
9. If $n$ is an odd integer, then show that $\phi(2n) = \phi(n)$.
10. If $n$ is an even integer, then show that $\phi(2n) = 2\,\phi(n)$.
11. Show that there are infinitely many integers for which $\phi(n)$ is a perfect square.
12. Prove that if the integer $n$ has $r$ distinct odd prime factors , then $2^r | \phi(n)$
13. Show that for $n > 2$, $\phi(n)$ is an even integer.
14. For any integer $a$, show that $a$, $a^{37} \equiv a (\text{mod } 1729)$.
15. For any integer $a$, show that $a$, $a^{23} \equiv a (\text{mod } 2730)$.
16. Find the units digitof $3^{100}$ by means of Euler's Theorem.
17. For any prime $p$, show that $\tau(p!) = 2\tau((p-1)!)$
18. For any prime $p$, show that $\sigma(p!) = (p+1)\sigma((p-1)!)$
19. For any prime $p$, show that $\phi(p!) = (p-1)\phi((p-1)!)$
20. if $a$ and $n$ are relatively prime, then show that the linear congruence $ax \equiv b(\text{mod } n)$ has the solution $x \equiv ba^{\phi(n)-1}(\text{mod } n)$.

**(8 Mark Questions)**

1. Show that if $f$ is a multiplicative function, then the function $F$, defined by $F(n) = \sum\limits_{d|n} f(d)$, is also multiplicative.
2. If $p$ is prime and $k > 0$, then show that $\phi(p^k) = p^k(1 - \frac{1}{p})$.
3. Prove that for given integers $a, b, c$, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.
4. Show that if $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1\,(\text{mod } n)$.
5. Show that $\phi(n) = \frac{n}{2}$ if and only if $n = 2^k$ for some $k \geq 1$.
6. Show that if $p$ is a prime and $p \not| a$, then $a^{p-1} \equiv 1\,(\text{mod } p)$.
7. Show that for each positive integer $n \geq 1$, $n = \sum\limits_{d|n} \phi(d)$, the sum being extended over all positive divisors of $n$.
8. For any positive integer $n$, show that $\frac{1}{2}\sqrt{n} \leq \phi(n) \leq n$.
9. prove that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$, whenever $p$ and $2p-1$ are both odd primes.

10. If $m$ and $n$ are relatively prime integers, then show that $m^{\phi(n)} + n^{\phi(m)} \equiv 1(\text{mod } mn)$.
11. Show that $\sum_{d|n} \phi(d) = n$, for each positive integer $n \geq 1$.
12. For $n > 1$, show that the sum of positive integers less than $n$ and relatively prime to $n$ is $\frac{1}{2} n\phi(n)$.
13. Assuming that $d|n$, show that $\phi(d)|\phi(n)$.

**(10 Mark Questions)**

1. Show that the Euler phi-function is multiplicative.
2. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, then prove that $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_r})$.
3. Show that for positive integers $m$ and $n$,
   (a) $\phi(m)\,\phi(n) = \phi(mn)\frac{\phi(d)}{d}$, where $d = \gcd(m, n)$.
   (b) $\phi(m)\,\phi(n) = \phi(gcd(m, n))\phi(lcm(m, n))$.
4. If $n \geq 1$ and $\gcd(a, n) = 1$, then show that $a^{\phi(n)} \equiv 1 \,(\text{mod } n)$.
5. If $p$ is a prime and $p$ does not divide $a$, then show that $a^{p-1} \equiv 1(\text{mod } p)$.