Shree H.N. Shukla College of Science
M.Sc. (Mathematics) Sem-3
IMP questions of Number Theory-1

---

1. State and Prove : Division Algorithm
2. Let a and b be integers such that $a \neq 0$ or $b \neq 0$ then the GCD of a and b exist and g=gcd(a,b) then $g = ax_0 + by_0$ for some integer x_0 and y_0
3. State and Prove : Euclid's Algorithm
4. State and Prove : Fundamental theorem of Arithmatic
5. Prove that There are infinitely many prime numbers.
6. Let $m \neq 0$ then $ax \equiv ay (\mathrm{mod}\ m)$ if and only if $x \equiv y$ ($\mathrm{mod} \frac{m}{(a,m)}$)
7. State and Prove : Euler's Theorem
8. State and Prove : Wilson's Theorem
9. Let p be a prime number then there is an integer x_0 which satisfies $x^2 + 1 \equiv 0$ (mod p) iff p=2 or p=4k + 1, for some k
10. If p is prime of the form 4k+3 and p divides a^2+b^2 then p divides a and p divides b.
11. State and Prove : Chinese remainder theorem
12. Prove that : Suppose $f(x) \equiv 0(mod\ p)$ has degree n then number of solutions of $f(x) \equiv 0(mod\ p)$ in any CRS(mod p) is less than or equal to n.
13. State and Prove : Hensel's lemma
14. Let $m, m_1, m_2 \geq 1, m = m_1 m_2$ and $(m_1, m_2) = 1$. Then number of Solutions of $f(x) \equiv 0(mod\ m)$ is equal to the number of solution of $f(x) \equiv 0(mod\ m_1) \times$ the number of solution of $f(x) \equiv 0(mod\ m_2)$
15. Let $m \geq 1$ and g be a primitive root of m then the set $S = \{1, g, g^2, \ldots, g^{\varphi(m)-1}\}$ is RRS (mod m)
16. If p is a prime number then p has a primitive roots and p has exactly $\varphi(p-1)$ primitive root (mod p)
17. If p is a prime number then p^2 has $(p-1)\varphi(p-1)$ primitive roots (mod p^2)
18. If p is a prime number $n \geq 1$ and $p \nmid a$ then either $x^n \equiv a(mod\ p)$ has no solutions or there are gcd(n,p-1) solutions (in any CRS(mod p)) Also $x^n \equiv a(mod\ p)$ has a solution if $a^{\frac{p-1}{(n,p-1)}} \equiv 1(mod\ p)$
19. Let $\alpha \geq 3$ then the set $S = \{-5^{2^{\alpha-2}}, \ldots, -5^3, -5^2, -5, 5, 5^2, \ldots, 5^{2^{\alpha-2}}\}$ is a RRS(mod 2^α)
20. Suppose $n \geq 1$ is odd, $\alpha \geq 3$ and a is and integer . Then $x^n \equiv a(mod\ 2^\alpha)$ has a unique solution any CRS(RRS) $(mod\ 2^\alpha)$
21. Suppose $n > 1$ is an even number, $\alpha \geq 3$ and a is an odd integer. Let $2^\beta = (n, 2^{\alpha-2})$ .Then $x^n \equiv a(mod\ 2^\alpha)$ has $2^{\beta+1}$ solutions, if $a \equiv 1(mod\ 2^{\beta+2})$ and no solution otherwise.
22. Suppose $m, m_1, m_2 \geq 1, m = m_1 m_2, (m_1, m_2) = 1$ and ($\varphi(m_1), \varphi(m_2)$) ≥ 2. Then m does not have a primitive root.
23. Let $n \geq 1$, p be a prime number. if e= the highest power of p which devides $n!$ then $e = \sum_{j=1}^{\infty}[\frac{n}{p^j}]$.

24. Let $m \geq 1, m_1, m_2, \ldots, m_k \geq 1$ and $m = m_1 + m_2 + \cdots + m_k$ then $\frac{m!}{m_1! m_2! \ldots m_k!}$ is an integer.
25. Suppose $f: \mathbb{N} \rightarrow \mathbb{C}$ is a multiplicative function. Define $F: \mathbb{N} \rightarrow \mathbb{C}$ as $F(n) = \sum_{\substack{d|n \\ d \geq 1}} f(d)$ Then F is a multiplicative function.
26. State and Prove : Mobius Inversion Theorem