Number Theory Theorems

www.fractionshub.com

Arkabrata Das , Diganta Bhattacharya

Number Theory Theorems
www.fractionshub.com
email:admin@fractionshub.com

1. **Theorem** (Principle of Mathematical Induction) If a set $\mathscr{S}$ of non-negative integers contains the integer 0, and also contains the integer $n+1$ whenever it contains the integer n, then $\mathscr{S} = N$.

2. **Theorem** (Arithmetic-Mean-Geometric-Mean Inequality) Let $a_1, a_2, ..., a_n$ be nonnegative real numbers. Then
$$\sqrt[n]{a_1 a_2 \dots a_n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}$$

3. **Theorem** (Cassini's Identity)
$$f_{n-1} f_{n+1} - f_n^2 = (-1)^n, n \geq 1.$$

4. **Theorem** (Binet's Formula) The $n-th$ Fibonacci number is given by
$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$
$n = 0, 2....$

5. **Theorem** If $s \geq 1, t \geq 0$ are integers then
$$f_{s+t} = f_{s-1} f_t + f_s f_{t+1}.$$

6. **Theorem**
   (a) If a, b, c, m, n are integers with $c|a, c|b$, then $c|(am + nb)$.
   (b) If x, y, z are integers with $x|y, y|z$ then $x|z$.

7. **Theorem** The product of n consecutive integers is divisible by $n!$.

8. **Theorem** If $k|n$ then $f_k|f_n$.

9. **Theorem** (Division Algorithm) If a, b are positive integers, then there are unique integers q, r such that $a = bq + r, 0 \leq r < b$.

10. **Theorem** (Casting-out $9's$) A natural number n is divisible by 9 if and only if the sum of it digits is divisible by 9.

11. **Theorem** (Bachet-Bezout Theorem) The greatest common divisor of any two integers a, b can be written as a linear combination of a and b, i.e., there are integers x, y with

$$(a, b) = ax + by.$$

12. **Theorem** If $(a, b) = d$, then

$$(\frac{a}{d}, \frac{b}{d}) = 1$$

13. **Theorem** Let c be a positive integer. Then

$$(ca, cb) = c(a, b).$$

14. **Theorem** $(a^2, b^2) = (a, b)^2$.

15. **Theorem** If $n > 1$, then n is divisible by at least one prime.

16. **Theorem** (Euclid) There are infinitely many primes.

17. **Theorem** There are infinitely many primes of the form $4n + 3$.

18. **Theorem** If the positive integer n is composite, then it must have a prime factor p with $p \leq \sqrt{n}$.

19. **Theorem** Every integer greater than 1 is a product of prime numbers.

20. **Theorem** (Fundamental Theorem of Arithmetic) Every integer > 1 can be represented as a product of primes in only one way, apart from the order of the factors.

21. **Theorem** Prove that if a, b, n are positive integers, then

$$(a, b) = (a + nb, b).$$

22. **Theorem** If r_n is the last non-zero remainder found in the process of the Euclidean Algorithm, then

$$r_n = (a, b).$$

23. **Theorem** Assume that a, b, c are integers such that $(a, b)|c$. Then given any solution (x_0, y_0) of the linear diophantine equation.

$$ax + by = c$$

any other solution of this equation will have the form

$$x = x_0 + t\frac{b}{d}, y = y_0 - t\frac{a}{d},$$

Where $d = (a, b)$ and $t \in \mathbb{Z}$

24. **Theorem** Let a, b, n be integers. If the congruence $ax \equiv b \bmod n$ has a solution, then it has (a, n) incongruent solutions mod n

25. **Theorem** Let x, y be integers and let a, n be non-zero integers. Then

$$ax \equiv ay \bmod n$$

if and only if

$$x \equiv y \bmod \frac{n}{(a,n)}.$$

26. **Theorem** (Frobenius) Let a, b be positive integers. If $(a, b) = 1$ then the number of positive integers m that cannot be written in the form $ar + bs = m$ for nonnegative integers r, s equals $(a-1)(b-1)/2$.

27. **Theorem** Let a, b be relatively prime positive integers. Then the equation

$$ax + by = n$$

is unsoluble in nonnegative integers x, y for $n = ab - a - b$. If $n > ab - a - b$, then the equation is soluble in nonnegative integers.

28. **Theorem** (Chinese Remainder Theorem) Let $m_1, m_2, ...m_k$ be pairwise relatively prime positive integers, each exceeding 1, and let $a_1, a_2, ...a_k$ be arbitrary integers. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \quad \vdots \quad \vdots \\ x &\equiv a_k \bmod m_k \end{aligned}$$

has a unique solution modulo $m_1, m_2 \dots m_k$.

29. **Theorem** Let $\alpha, \beta \in \mathbb{R}, a \in \mathbb{Z}, n \in \mathbb{N}$. Then

(a) $\lfloor \alpha + a \rfloor = \lfloor \alpha \rfloor + a$

(b) $\lfloor \frac{\alpha}{n} \rfloor = \lfloor \frac{\lfloor \alpha \rfloor}{n} \rfloor$

(c) $\lfloor \alpha \rfloor + \lfloor \beta \rfloor \leq \lfloor \alpha + \beta \rfloor \leq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 1$

30. **Theorem** If a, b are relatively prime natural numbers then

$$\sum_{k-1}^{a-1} \lfloor \frac{kb}{a} \rfloor = \sum_{k=1}^{b-1} \lfloor \frac{ka}{b} \rfloor = \frac{(a-1)(b-1)}{2}$$

31. **Theorem** (De Polignac's Formula) The highest power of a prime p dividing $n!$ is given by

$$\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor.$$

32. **Theorem** (Beatty's Theorem, 1926) If $a > 1$ is irrational and

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1.$$

then the sequences

$$Spec(\alpha) \text{ and } Spec(\beta)$$

are complementary.

33. **Theorem** (Bang's Theorem, 1957) If the sequences

$$Spec(\alpha) \text{ and } Spec(\beta)$$

are complementary, then α, β are positive irrational numbers with

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1$$

34. **Theorem** Let f be a multiplicative function and let $F(n) = \sum_{d|n} f(d)$. Then F is also multiplicative

35. **Theorem** An even number is perfect if and only if it is of the form $2^{p-1}(2^p - 1)$ where both p and $2^p - 1$ are primes.

36. **Theorem** The function ϕ is multiplicative

37. **Theorem** Let n be a positive integer. Then $\sum_{d|n} \phi(d) = n$.

38. **Theorem** Let $n > 1, a$ be integers. Then a possesses an inverse modulo n if and only if a is relatively prime to n.

39. **Theorem** If a is relatively prime to the positive integer n, there exists a positive integer $k \leq n$ such that $a^k \equiv 1 \bmod n$.

40. **Theorem** Let $n > 1$ be a positive integer. Then $a \in \mathbb{Z}$ has an order mod n if and only if $(a, n) = 1$.

41. **Theorem** Let $(a, n) = 1$ and let t be an integer. Then $a^t \equiv 1 \bmod n$ if and only if $ord_n a | t$.

42. **Theorem** Let $n > 1, a \in \mathbb{Z}, (a, n) = 1$. If $r_1, r_2, ..., r_{\phi(n)}$ is a reduced set of residues modulo n, then $ar_1, ar_2, ..., ar_{\phi(n)}$ is also a reduced set of residues modulo n

43. **Theorem** The Möbius Function m is multiplicative.

44. **Theorem**

    (a) $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

45. **Theorem** (Möbius Inversion Formula) Let f be an arithmetical function and $F(n) = \sum_{d|n} f(d)$. Then
$$f(n) = \sum_{d|n} \mu(d)F(n/d) = \sum_{d|n} \mu(n/d)F(d).$$

46. **Theorem** Let f, F be arithmetic functions with $f(n) = \sum_{d|n} \mu(d)F(n/d)$ for all natural numbers n. Then $F(n) = \sum_{d|n} f(d)$.

47. **Theorem** (Fermat's Little Theorem) Let p be a prime and let $p \nmid a$. Then
$$a^{p-1} \equiv 1 \bmod p.$$

48. **Theorem** (Wilson's Theorem) If p is a prime, then $(p-1)! \equiv -1 \bmod p$.

49. **Theorem** (Euler's Theorem) Let $(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \bmod n$.