

MATHEMATICS 374

PROBLEM METHODS

1. Notation. $[n] = \{1, 2, 3, \dots, n\}$, i.e. the positive integers which are less than or equal to n .
2. Principle of Mathematical Induction (strong form). Let $P(n)$ be a proposition about the positive integer n . If
 - (a) $P(1)$ is true, and
 - (b) for each positive integer k , the truth of $P(1), P(2), \dots, P(k)$, implies the truth of $P(k+1)$, then $P(n)$ is true for all positive integers n .
3. Pigeonhole Principle. If $kn+1$ objects ($k \geq 0$) are distributed among n boxes, one of the boxes will contain at least $k+1$ objects.
4. Binomial Theorem.

$$(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i.$$

5. Unique Factorization Theorem. Every positive integer $n > 1$ may be uniquely written as the product of prime factors in the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where each p_i is a prime integer, $2 \leq p_1 < p_2 < \cdots < p_k$, and each α_i is a positive integer.

6. Division Algorithm. If a and b are arbitrary integers, $b > 0$, there are unique integers q and r such that $a = qb + r$, with $r = 0$ or $0 < r < b$.
7. Division Algorithm for Polynomials. If $F(x)$ and $G(x)$ are polynomials over a field K (for example, K might be the rationals, the reals, the complexes, the integers modulo p for p prime), there exist unique polynomials $Q(x)$ and $R(x)$ over the field K such that $F(x) = Q(x)G(x) + R(x)$, where $R(x)$ is the zero polynomial or $\deg R(x) < \deg G(x)$ (\deg means degree).
8. Factor Theorem. If $F(x)$ is a polynomial over an integral domain D (the integers are an integral domain, any field is an integral domain), an element of D is a root of $F(x) = 0$ if and only if $x - a$ is a factor of $F(x)$.
9. Identity Theorem. Suppose that two polynomials in x over an integral domain are each of degree less than $n+1$. If these polynomials have equal values for more than n distinct values of x , then the two polynomials are identical.
10. Rational-Root Theorem. If $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is a polynomial with integer coefficients and if the rational number r/s (r and s relatively prime integers) is a root of $P(x) = 0$, then $r|a_0$ and $s|a_n$.
11. Gauss' Lemma. Let $P(x)$ be a polynomial with integer coefficients. If $P(x)$ can be factored into a product of two polynomials with rational coefficients, then $P(x)$ can be factored into a product of two polynomials with integer coefficients.

12. Fundamental Theorem of Algebra (Gauss). Let $P(x)$ be an n^{th} order monic polynomial with complex coefficients. (The coefficient on x^n is one; there are no terms with higher powers of x than the n^{th} power.) Then $P(x)$ may be factored into n linear factors of the form $x - \alpha$ where α is a complex number.
13. Factoring Real Polynomials Theorem. Let $P(x)$ be an n^{th} order polynomial with real coefficients. Then $P(x)$ may be factored into real linear and irreducible (over the reals) quadratic factors. Further the two zeros of each of the quadratic factors are complex conjugate pairs.
14. Fermat's Little Theorem. Let p be a prime and assume that p does not divide a . Then, $a^{p-1} \equiv 1 \pmod{p}$.
15. Euler's ϕ -function. Definition.

$$\phi(N) = |\{k \in [n] : \gcd(k, n) = (k, n) = 1\}|.$$

Defintion. A function ψ is said to be multiplicative in case for p_1, p_2, \dots, p_r are distinct primes and $N = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$, then

$$\psi(N) = \psi(p_1^{c_1})\psi(p_2^{c_2}) \cdots \psi(p_r^{c_r}).$$

Euler's ϕ -function is multiplicative.

A related function is the σ or sum of positive divisors function given by

$$\sigma(N) = \sum_{d>0, d|N} d.$$

The σ -function is also multiplicative.

16. Euler's Theorem. Let N be any positive integer and let r be the number of integers of the sequence $1, 2, 3, \dots, N - 1$ which are relatively prime to N , i.e. $r = \phi(N)$. If a is any integer relatively prime to N , then N divides $a^r - 1$.
17. Wilson's Theorem. Let p be a prime. Then, $(p - 1)! \equiv -1 \pmod{p}$.
18. Chinese Remainder Theorem. If m_1, m_2, \dots, m_k are (pairwise) relatively prime positive integers greater than one, and a_1, a_2, \dots, a_k are arbitrary integers, then there exists an integer x such that

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \dots, k.$$

19. Bertrand's Postulate. Let n be a positive integer. Then, there exists at least one prime p for which $n < p < 2n$.
20. Sum of Arithmetic Series.

$$a + (a + d) + (a + 2d) + \cdots + (a + nd) = \left(\frac{(2a + nd)(n + 1)}{2} \right).$$

In particular,

$$\sum_{i=1}^n i = \left(\frac{n(n + 1)}{2} \right).$$

21. Sum of Geometric Series.

$$1 + x + x^2 + x^3 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}, \quad x \neq 1.$$

$$1 + x + x^2 + x^3 + \cdots + x^n + \cdots = 1/(1 - x), \quad |x| < 1.$$

22. Monotonic Convergence Theorem. Let a_n be a bounded monotonic sequence of real numbers. Then a_n converges to a (finite) real number.
23. Extreme-Value Theorem. If f is a continuous function on $[a, b]$, then there are numbers $c, d \in [a, b]$ such that $f(c) \leq f(x) \leq f(d)$ for all $x \in [a, b]$.
24. Intermediate Value Theorem. If f is a continuous function on $[a, b]$ and if $f(a) < y < f(b)$ or $f(b) < y < f(a)$, then there is a number $c \in (a, b)$ such that $f(c) = y$.
25. Rolle's Theorem. Suppose that f is a real valued continuous function defined on $[a, b]$ and differentiable on (a, b) . If $f(a) = f(b)$, then there is a $c \in (a, b)$ such that $f'(c) = 0$.
26. Mean-Value Theorem. Suppose that f is a real valued continuous function defined on $[a, b]$ and differentiable on (a, b) , then there is a $c \in (a, b)$ such that

$$\frac{f(b) - f(a)}{b - a} = f'(c).$$

27. Fundamental Theorem of Calculus. If F has a continuous derivative on $[a, b]$, then

$$\int_a^b F'(x)dx = F(b) - F(a),$$

or, if f is a continuous function on $[a, b]$, then

$$\frac{d}{dx} \left(\int_a^x f'(t)dt \right) = f(x).$$

28. Cauchy-Schwarz Inequality. For all real numbers $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$,

$$\left(\sum_{i=1}^n a_i b_i \right)^2 \leq \left(\sum_{i=1}^n a_i^2 \right) \left(\sum_{i=1}^n b_i^2 \right)$$

29. Arithmetic Mean-Geometric Mean Inequality. Let $x_1, x_2, x_3, \dots, x_n$, be positive real numbers. Then,

$$\sqrt[n]{\prod_{i=1}^n x_i} \leq \frac{1}{n} \sum_{i=1}^n x_i,$$

with equality if and only if $x_1 = x_2 = x_3 = \cdots = x_n$.

30. Pick's Theorem. The area of a simple (no crossing edges) lattice (integer coordinates) polygon in the xy -plane is given by $I + \frac{1}{2}B - 1$, where I and B denote respectively the number of interior and boundary lattice points of the polygon.
31. Hurwitz's Theorem. If b is an irrational number, then there exist infinitely many pairs of integers (m, n) with $\gcd(m, n) = 1$ such that

$$\left| b - \frac{m}{n} \right| < \frac{1}{n^2\sqrt{5}}.$$

The inequality is best possible in the sense that it becomes false if $\sqrt{5}$ is replaced with any larger constant.

32. The Squeeze Principle (sequence form). If a_n, b_n, c_n are infinite sequences such that $a_n \leq b_n \leq c_n$ for all n sufficiently large, and if $\lim_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} c_n = L$, then $\lim_{n \rightarrow \infty} b_n = L$.
33. Trigonometric formulae. Let the sides of triangle T be a, b, c , and define $s = (a+b+c)/2$, then the area of T is $A(T) = \sqrt{s(s-a)(s-b)(s-c)}$. Inradius of T is $I(T) = A(T)/s$. Circumradius of T is $C(T) = abc/4A(T)$.
34. Definition of modulus of the complex number $z = x + iy$, the distance from z to the origin in the complex plane: $|z| = \sqrt{z\bar{z}} = \sqrt{(x+iy)(x-iy)} = \sqrt{x^2 + y^2}$, where $\bar{z} = x - iy$ is the complex conjugate of z .
35. Definition of floor function of real number x , the greatest integer less than or equal to x : $\lfloor x \rfloor = n$, where n is the integer satisfying $n \leq x < n + 1$.
36. Definition of ceiling function of real number x , the least integer greater than or equal to x : $\lceil x \rceil = n$, where n is the integer satisfying $n - 1 < x \leq n$.
37. Definition of and notation for n choose r :

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Last modified 09/20/08