Basic Concepts and Facts

Based on Chapter 2 of *The IMO Compendium*

The following is a list of the most basic concepts and theorems frequently used in this book. We encourage the reader to become familiar with them and perhaps read up on them further in other literature.

Algebra

Polynomials

Theorem. The quadratic equation $ax^2 + bx + c = 0$ ($a, b, c \in \mathbb{R}$, $a \neq 0$) has solutions

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The *discriminant* D of the quadratic equation is defined as $D = b^2 - 4ac$. For $D < 0$ the solutions are complex and conjugate to each other, for $D = 0$ the solutions degenerate to one real solution, and for $D > 0$ the equation has two distinct real solutions.

Definition. Binomial coefficients $\binom{n}{k}$, $n, k \in \mathbb{N}_0$, $k \leq n$, are defined as

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

They satisfy $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$ for $i > 0$ and also $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$, $\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n \binom{n}{n} = 0$, $\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$.

Theorem. [(Newton's) binomial formula] For $x, y \in \mathbb{C}$ and $n \in \mathbb{N}$,

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

Theorem. [Bézout's theorem] A polynomial $P(x)$ is divisible by the binomial $x - a$ ($a \in \mathbb{C}$) if and only if $P(a) = 0$.

Theorem. [The rational root theorem] If $x = p/q$ is a rational zero of a polynomial $P(x) = a_n x^n + \cdots + a_0$ with integer coefficients and $(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$.

Theorem. [The fundamental theorem of algebra] Every nonconstant polynomial with coefficients in $\mathbb{C}$ has a complex root.

Theorem. [Eisenstein's criterion (extended)] Let $P(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If there exist a prime p and an integer $k \in \{0, 1, \ldots, n-1\}$ such that $p \mid a_0, a_1, \ldots, a_k$, $p \nmid a_{k+1}$, and $p^2 \nmid a_0$, then there exists an irreducible factor $Q(x)$ of $P(x)$ whose degree is at least k. In particular, if p can be chosen such that $k = n - 1$, then $P(x)$ is irreducible.

The IMO Compendium Group,
D. Djukić, V. Janković, I. Matić, N. Petrović
www.imo.org.yu

Definition. *Symmetric polynomials* in $x_1, \dots, x_n$ are polynomials that do not change on permuting the variables $x_1, \dots, x_n$. *Elementary symmetric polynomials* are $\sigma_k(x_1, \dots, x_n) = \sum x_{i_1} \cdots x_{i_k}$ (the sum is over all k-element subsets $\{i_1, \dots, i_k\}$ of $\{1, 2, \dots, n\}$).

Theorem. Every symmetric polynomial in $x_1, \dots, x_n$ can be expressed as a polynomial in the elementary symmetric polynomials $\sigma_1, \dots, \sigma_n$.

Theorem. [Vieta's formulas] Let $\alpha_1, \dots, \alpha_n$ and $c_1, \dots, c_n$ be complex numbers such that

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n\ .$$

Then $c_k = (-1)^k \sigma_k(\alpha_1, \dots, \alpha_n)$ for $k = 1, 2, \dots, n$.

Theorem. [Newton's formulas on symmetric polynomials] Let

$$\sigma_k = \sigma_k(x_1, \dots, x_n)$$

and let $s_k = x_1^k + x_2^k + \cdots + x_n^k$, where $x_1, \dots, x_n$ are arbitrary complex numbers. Then

$$k\sigma_k = s_1 \sigma_{k-1} - s_2 \sigma_{k-2} + \cdots + (-1)^k s_{k-1} \sigma_1 + (-1)^{k-1} s_k\ .$$

Recurrence Relations

Definition. A *recurrence relation* is a relation that determines the elements of a sequence x_n, $n \in \mathbb{N}_0$, as a function of previous elements. A recurrence relation of the form

$$(\forall n \geq k) \qquad x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0$$

for constants $a_1, \dots, a_k$ is called a *linear homogeneous recurrence relation of order k*. We define the *characteristic polynomial* of the relation as $P(x) = x^k + a_1 x^{k-1} + \cdots + a_k$.

Theorem. Using the notation introduced in the above definition, let $P(x)$ factorize as $P(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \cdots (x - \alpha_r)^{k_r}$, where $\alpha_1, \dots, \alpha_r$ are distinct complex numbers and $k_1, \dots, k_r$ are positive integers. The general solution of this recurrence relation is in this case given by

$$x_n = p_1(n)\alpha_1^n + p_2(n)\alpha_2^n + \cdots + p_r(n)\alpha_r^n,$$

where p_i is a polynomial of degree less than k_i. In particular, if $P(x)$ has k distinct roots, then all p_i are constant.

If $x_0, \dots, x_{k-1}$ are set, then the coefficients of the polynomials are uniquely determined.

Inequalities

Theorem. The quadratic function is always positive; i.e., $(\forall x \in \mathbb{R})\ x^2 \geq 0$. By substituting different expressions for x, many of the inequalities below are obtained.

Theorem. [Bernoulli's inequalities]

1. If $n \geq 1$ is an integer and $x > -1$ a real number then $(1+x)^n \geq 1 + nx$.
2. If $a > 1$ or $a < 0$ then for $x > -1$ the following inequality holds: $(1+x)^\alpha \geq 1 + \alpha x$.
3. If $a \in (0,1)$ then for $x > -1$ the following inequality holds: $(1+x)^\alpha \leq 1 + \alpha x$.

Theorem. [The mean inequalities] For positive real numbers $x_1, x_2, \ldots, x_n$ it follows that $QM \geq AM \geq GM \geq HM$, where

$$\begin{aligned} QM &= \sqrt{\frac{x_1^2 + \cdots + x_n^2}{n}}, & AM &= \frac{x_1 + \cdots + x_n}{n}, \\ GM &= \sqrt[n]{x_1 \cdots x_n}, & HM &= \frac{n}{1/x_1 + \cdots + 1/x_n}. \end{aligned}$$

Each of these inequalities becomes an equality if and only if $x_1 = x_2 = \cdots = x_n$. The numbers QM, AM, GM, and HM are respectively called the *quadratic mean*, the *arithmetic mean*, the *geometric mean*, and the *harmonic mean* of $x_1, x_2, \ldots, x_n$.

Theorem. [The general mean inequality] Let $x_1, \ldots, x_n$ be positive real numbers. For each $p \in \mathbb{R}$ we define the *mean of order* p of $x_1, \ldots, x_n$ by $M_p = \left(\frac{x_1^p + \cdots + x_n^p}{n}\right)^{1/p}$ for $p \neq 0$, and $M_q = \lim_{p \to q} M_p$ for $q \in \{\pm\infty, 0\}$. In particular, $\max x_i$, QM, AM, GM, HM, and $\min x_i$ are M_∞, M_2, M_1, M_0, M_{-1}, and $M_{-\infty}$ respectively. Then

$$M_p \leq M_q \quad \text{whenever} \quad p \leq q.$$

Theorem. [Cauchy–Schwarz inequality] Let a_i, b_i, $i = 1, 2, \ldots, n$, be real numbers. Then

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

Equality occurs if and only if there exists $c \in \mathbb{R}$ such that $b_i = ca_i$ for $i = 1, \ldots, n$.

Theorem. [Hölder's inequality] Let a_i, b_i, $i = 1, 2, \ldots, n$, be nonnegative real numbers, and let p, q be positive real numbers such that $1/p + 1/q = 1$. Then

$$\sum_{i=1}^n a_i b_i \leq \left(\sum_{i=1}^n a_i^p\right)^{1/p} \left(\sum_{i=1}^n b_i^q\right)^{1/q}.$$

Equality occurs if and only if there exists $c \in \mathbb{R}$ such that $b_i = ca_i$ for $i = 1, \ldots, n$. The Cauchy–Schwarz inequality is a special case of Hölder's inequality for $p = q = 2$.

Theorem. [Minkowski's inequality] Let a_i, b_i $(i = 1, 2, \ldots, n)$ be nonnegative real numbers and p any real number not smaller than 1. Then

$$\left(\sum_{i=1}^{n}(a_i + b_i)^p\right)^{1/p} \le \left(\sum_{i=1}^{n} a_i^p\right)^{1/p} + \left(\sum_{i=1}^{n} b_i^p\right)^{1/p}.$$

For $p > 1$ equality occurs if and only if there exists $c \in \mathbb{R}$ such that $b_i = ca_i$ for $i = 1, \ldots, n$. For $p = 1$ equality occurs in all cases.

Theorem. [Chebyshev's inequality] Let $a_1 \ge a_2 \ge \cdots \ge a_n$ and $b_1 \ge b_2 \ge \cdots \ge b_n$ be real numbers. Then

$$n\sum_{i=1}^{n} a_i b_i \ge \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) \ge n\sum_{i=1}^{n} a_i b_{n+1-i}.$$

The two inequalities become equalities at the same time when $a_1 = a_2 = \cdots = a_n$ or $b_1 = b_2 = \cdots = b_n$.

Definition. A real function f defined on an interval I is *convex* if $f(\alpha x + \beta y) \le \alpha f(x) + \beta f(y)$. for all $x, y \in I$ and all $\alpha, \beta > 0$ such that $\alpha + \beta = 1$. A function f is said to be *concave* if the opposite inequality holds, i.e., if $-f$ is convex.

Theorem. If f is continuous on an interval I, then f is convex on that interval if and only if

$$f\left(\frac{x+y}{2}\right) \le \frac{f(x) + f(y)}{2} \qquad \text{for all } x, y \in I.$$

Theorem. If f is differentiable, then it is convex if and only if the derivative f' is nondecreasing. Similarly, differentiable function f is concave if and only if f' is nonincreasing.

Theorem. [Jensen's inequality] If $f : I \to \mathbb{R}$ is a convex function, then the inequality

$$f(\alpha_1 x_1 + \cdots + \alpha_n x_n) \le \alpha_1 f(x_1) + \cdots + \alpha_n f(x_n)$$

holds for all $\alpha_i \ge 0$, $\alpha_1 + \cdots + \alpha_n = 1$, and $x_i \in I$. For a concave function the opposite inequality holds.

Theorem. [Muirhead's inequality] Given $x_1, x_2, \ldots, x_n \in \mathbb{R}^+$ and an n-tuple $\mathbf{a} = (a_1, \cdots, a_n)$ of positive real numbers, we define

$$T_{\mathbf{a}}(x_1, \ldots, x_n) = \sum y_1^{a_1} \ldots y_n^{a_n},$$

the sum being taken over all permutations $y_1, \ldots, y_n$ of $x_1, \ldots, x_n$. We say that an n-tuple $\mathbf{a}$ *majorizes* an n-tuple $\mathbf{b}$ if $a_1 + \cdots + a_n = b_1 + \cdots + b_n$ and $a_1 + \cdots + a_k \ge b_1 + \cdots + b_k$ for each $k = 1, \ldots, n-1$. If a nonincreasing n-tuple $\mathbf{a}$ majorizes a nonincreasing n-tuple $\mathbf{b}$, then the following inequality holds:

$$T_{\mathbf{a}}(x_1, \ldots, x_n) \ge T_{\mathbf{b}}(x_1, \ldots, x_n).$$

Equality occurs if and only if $x_1 = x_2 = \cdots = x_n$.

Theorem. [Schur's inequality] Using the notation introduced for Muirhead's inequality,

$$T_{\lambda+2\mu,0,0}(x_1,x_2,x_3) + T_{\lambda,\mu,\mu}(x_1,x_2,x_3) \geq 2T_{\lambda+\mu,\mu,0}(x_1,x_2,x_3),$$

where $\lambda, \mu \in \mathbb{R}^+$. Equality occurs if and only if $x_1 = x_2 = x_3$ or $x_1 = x_2$, $x_3 = 0$ (and in analogous cases).

Groups and Fields

Definition. A *group* is a nonempty set G equipped with an operation $*$ satisfying the following conditions:

(i) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

(ii) There exists a (unique) *additive identity* $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.

(iii) For each $a \in G$ there exists a (unique) *additive inverse* $a^{-1} = b \in G$ such that $a * b = b * a = e$.

If $n \in \mathbb{Z}$, we define a^n as $a * a * \cdots * a$ (n times) if $n \geq 0$, and as $(a^{-1})^{-n}$ otherwise.

Definition. A group $\mathcal{G} = (G, *)$ is *commutative* or *abelian* if $a * b = b * a$ for all $a, b \in G$.

Definition. A set A *generates* a group $(G, *)$ if every element of G can be obtained using powers of the elements of A and the operation $*$. In other words, if A is the generator of a group G then every element $g \in G$ can be written as $a_1^{i_1} * \cdots * a_n^{i_n}$, where $a_j \in A$ and $i_j \in \mathbb{Z}$ for every $j = 1, 2, \ldots, n$.

Definition. The *order* of $a \in G$ is the smallest $n \in \mathbb{N}$ such that $a^n = e$, if it exists. The *order* of a group is the number of its elements, if it is finite. Each element of a finite group has a finite order.

Theorem. [Lagrange's theorem] In a finite group, the order of an element divides the order of the group.

Definition. A *ring* is a nonempty set R equipped with two operations $+$ and $\cdot$ such that $(R, +)$ is an abelian group and for any $a, b, c \in R$,

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(ii) $(a + b) \cdot c = a \cdot c + b \cdot c$ and $c \cdot (a + b) = c \cdot a + c \cdot b$.

A ring is *commutative* if $a \cdot b = b \cdot a$ for any $a, b \in R$ and *with identity* if there exists a *multiplicative identity* $i \in R$ such that $i \cdot a = a \cdot i = a$ for all $a \in R$.

Definition. A *field* is a commutative ring with identity in which every element a other than the additive identity has a *multiplicative inverse* a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = i$.

Theorem. The following are common examples of groups, rings, and fields:

Groups: $(\mathbb{Z}_n,+)$, $(\mathbb{Z}_p\setminus\{0\},\cdot)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{R}\setminus\{0\},\cdot)$.

Rings: $(\mathbb{Z}_n,+,\cdot)$, $(\mathbb{Z},+,\cdot)$, $(\mathbb{Z}[x],+,\cdot)$, $(\mathbb{R}[x],+,\cdot)$.

Fields: $(\mathbb{Z}_p,+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{Q}(\sqrt{2}),+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$.

Analysis

Definition. A sequence $\{a_n\}_{n=1}^{\infty}$ has a *limit* $a=\lim_{n\to\infty} a_n$ (also denoted by $a_n\to a$) if

$$(\forall\varepsilon>0)(\exists n_\varepsilon\in\mathbb{N})(\forall n\geq n_\varepsilon)\ |a_n-a|<\varepsilon.$$

A function $f:(a,b)\to\mathbb{R}$ has a limit $y=\lim_{x\to c} f(x)$ if

$$(\forall\varepsilon>0)(\exists\delta>0)(\forall x\in(a,b))\ 0<|x-c|<\delta\Rightarrow|f(x)-y|<\varepsilon.$$

Definition. A sequence x_n *converges* to $x\in\mathbb{R}$ if $\lim_{n\to\infty}x_n=x$. A series $\sum_{n=1}^{\infty}x_n$ converges to $s\in\mathbb{R}$ if and only if $\lim_{m\to\infty}\sum_{n=1}^{m}x_n=s$. A sequence or series that does not converge is said to *diverge*.

Theorem. A sequence a_n is convergent if it is monotonic and bounded.

Definition. A function f is *continuous* on $[a,b]$ if for every $x_0\in[a,b]$, $\lim_{x\to x_0}f(x)=f(x_0)$.

Definition. A function $f:(a,b)\to\mathbb{R}$ is *differentiable* at a point $x_0\in(a,b)$ if the following limit exists:

$$f'(x_0)=\lim_{x\to x_0}\frac{f(x)-f(x_0)}{x-x_0}.$$

A function is differentiable on (a,b) if it is differentiable at every $x_0\in(a,b)$. The function f' is called the *derivative* of f. We similarly define the second derivative f'' as the derivative of f', and so on.

Theorem. A differentiable function is also continuous. If f and g are differentiable, then fg, $\alpha f+\beta g$ $(\alpha,\beta\in\mathbb{R})$, $f\circ g$, $1/f$ (if $f\neq 0$), f^{-1} (if well-defined) are also differentiable. It holds that $(\alpha f+\beta g)'=\alpha f'+\beta g'$, $(fg)'=f'g+fg'$, $(f\circ g)'=(f'\circ g)\cdot g'$, $(1/f)'=-f'/f^2$, $(f/g)'=(f'g-fg')/g^2$, $(f^{-1})'=1/(f'\circ f^{-1})$.

Theorem. The following are derivatives of some elementary functions (a denotes a real constant): $(x^a)'=ax^{a-1}$, $(\ln x)'=1/x$, $(a^x)'=a^x\ln a$, $(\sin x)'=\cos x$, $(\cos x)'=-\sin x$.

Theorem. [Fermat's theorem] Let $f:[a,b]\to\mathbb{R}$ be a differentiable function. The function f attains its maximum and minimum in this interval. If $x_0\in(a,b)$ is an extremum (i.e., a maximum or minimum), then $f'(x_0)=0$.

The IMO Compendium Group,
D. Djukić, V. Janković, I. Matić, N. Petrović
www.imo.org.yu

Theorem. [Rolle's theorem] Let $f(x)$ be a continuously differentiable function defined on $[a, b]$, where $a, b \in \mathbb{R}$, $a < b$, and $f(a) = f(b) = 0$. Then there exists $c \in [a, b]$ such that $f'(c) = 0$.

Definition. Differentiable functions $f_1, f_2, \dots, f_k$ defined on an open subset D of $\mathbb{R}^n$ are *independent* if there is no nonzero differentiable function $F : \mathbb{R}^k \to \mathbb{R}$ such that $F(f_1, \dots, f_k)$ is identically zero on some open subset of D.

Theorem. Functions $f_1, \dots, f_k : D \to \mathbb{R}$ are independent if and only if the $k \times n$ matrix $[\partial f_i / \partial x_j]_{i,j}$ is of rank k, i.e. when its k rows are linearly independent at some point.

Theorem. [Lagrange multipliers] Let D be an open subset of $\mathbb{R}^n$ and $f, f_1, f_2, \dots, f_k : D \to \mathbb{R}$ independent differentiable functions. Assume that a point a in D is an extremum of the function f within the set of points in D such that $f_1 = f_2 = \cdots = f_n = 0$. Then there exist real numbers $\lambda_1, \dots, \lambda_k$ (so-called Lagrange multipliers) such that a is a stationary point of the function $F = f + \lambda_1 f_1 + \cdots + \lambda_k f_k$, i.e., such that all partial derivatives of F at a are zero.

Definition. Let f be a real function defined on $[a, b]$ and let $a = x_0 \le x_1 \le \cdots \le x_n = b$ and $\xi_k \in [x_{k-1}, x_k]$. The sum $S = \sum_{k=1}^{n} (x_k - x_{k-1}) f(\xi_k)$ is called a *Darboux sum.* If $I = \lim_{\delta \to 0} S$ exists (where $\delta = \max_k (x_k - x_{k-1})$), we say that f is *integrable* and I its *integral.* Every continuous function is integrable on a finite interval.

Geometry

Triangle Geometry

Definition. The *orthocenter* of a triangle is the common point of its three altitudes.

Definition. The *circumcenter* of a triangle is the center of its circumscribed circle (i.e. *circumcircle*). It is the common point of the perpendicular bisectors of the sides of the triangle.

Definition. The *incenter* of a triangle is the center of its inscribed circle (i.e. *incircle*). It is the common point of the internal bisectors of its angles.

Definition. The *centroid* of a triangle (*median point*) is the common point of its medians.

Theorem. The orthocenter, circumcenter, incenter and centroid are well-defined (and unique) for every non-degenerate triangle.

Theorem. [Euler's line] The orthocenter H, centroid G, and circumcircle O of an arbitrary triangle lie on a line (Euler's line) and satisfy $\overrightarrow{HG} = 2\overrightarrow{GO}$.

Theorem. [The nine-point circle] The feet of the altitudes from A, B, C and the midpoints of AB, BC, CA, AH, BH, CH lie on a circle (The nine-point circle).

The IMO Compendium Group,
D. Djukić, V. Janković, I. Matić, N. Petrović
www.imo.org.yu

Theorem. [Feuerbach's theorem] The nine-point circle of a triangle is tangent to the incircle and all three excircles of the triangle.

Theorem. Given a triangle $\triangle ABC$, let $\triangle ABC'$, $\triangle AB'C$, and $\triangle A'BC$ be equilateral triangles constructed outwards. Then AA', BB', CC' intersect in one point, called *Torricelli's point*.

Definition. Let ABC be a triangle, P a point, and X, Y, Z respectively the feet of the perpendiculars from P to BC, AC, AB. Triangle XYZ is called the pedal triangle *of $\triangle ABC$ corresponding to point P.*

Theorem. [Simson's line] The pedal triangle XYZ is degenerate, i.e., X, Y, Z are collinear, if and only if P lies on the circumcircle of ABC. Points X, Y, Z are in this case said to lie on *Simson's line*.

Theorem. [Carnot's theorem] The perpendiculars from X, Y, Z to BC, CA, AB respectively are concurrent if and only if

$$BX^2 - XC^2 + CY^2 - YA^2 + AZ^2 - ZB^2 = 0.$$

Theorem. [Desargues's theorem] Let $A_1B_1C_1$ and $A_2B_2C_2$ be two triangles. The lines A_1A_2, B_1B_2, C_1C_2 are concurrent or mutually parallel if and only if the points $A = B_1C_2 \cap B_2C_1$, $B = C_1A_2 \cap A_1C_2$, and $C = A_1B_2 \cap A_2B_1$ are collinear.

Vectors in Geometry

Definition. For any two vectors $\overrightarrow{a}, \overrightarrow{b}$ in space, we define the *scalar product* (also known as *dot product*) of $\overrightarrow{a}$ and $\overrightarrow{b}$ as $\overrightarrow{a} \cdot \overrightarrow{b} = |\overrightarrow{a}||\overrightarrow{b}|\cos\varphi$, and the *vector product* as $\overrightarrow{a} \times \overrightarrow{b} = \overrightarrow{p}$, where $\varphi = \angle(\overrightarrow{a}, \overrightarrow{b})$ and $\overrightarrow{p}$ is the vector with $|\overrightarrow{p}| = |\overrightarrow{a}||\overrightarrow{b}||\sin\varphi|$ perpendicular to the plane determined by $\overrightarrow{a}$ and $\overrightarrow{b}$ such that the triple of vectors $\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{p}$ is positively oriented (note that if $\overrightarrow{a}$ and $\overrightarrow{b}$ are collinear, then $\overrightarrow{a} \times \overrightarrow{b} = \overrightarrow{0}$). These products are both linear with respect to both factors. The scalar product is commutative, while the vector product is anticommutative, i.e. $\overrightarrow{a} \times \overrightarrow{b} = -\overrightarrow{b} \times \overrightarrow{a}$. We also define the *mixed vector product* of three vectors $\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}$ as $[\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}] = (\overrightarrow{a} \times \overrightarrow{b}) \cdot \overrightarrow{c}$.
Remark. Scalar product of vectors $\overrightarrow{a}$ and $\overrightarrow{b}$ is often denoted by $\langle \overrightarrow{a}, \overrightarrow{b} \rangle$.

Theorem. [Thales' theorem] Let lines AA' and BB' intersect in a point O, $A' \neq O \neq B'$. Then $AB \parallel A'B' \Leftrightarrow \frac{\overrightarrow{OA}}{\overrightarrow{OA'}} = \frac{\overrightarrow{OB}}{\overrightarrow{OB'}}$. (Here $\frac{\overrightarrow{a}}{\overrightarrow{b}}$ denotes the ratio of two nonzero collinear vectors).

Theorem. [Ceva's theorem] Let ABC be a triangle and X, Y, Z be points on lines BC, CA, AB respectively, distinct from A, B, C. Then the lines AX, BY, CZ are concurrent if and only if

$$\frac{\overrightarrow{BX}}{\overrightarrow{XC}} \cdot \frac{\overrightarrow{CY}}{\overrightarrow{YA}} \cdot \frac{\overrightarrow{AZ}}{\overrightarrow{ZB}} = 1, \text{ or equivalently, } \frac{\sin\measuredangle BAX}{\sin\measuredangle XAC}\frac{\sin\measuredangle CBY}{\sin\measuredangle YBA}\frac{\sin\measuredangle ACZ}{\sin\measuredangle ZCB} = 1$$

(the last expression being called the *trigonometric form* of Ceva's theorem).

Theorem. [Menelaus's theorem] Using the notation introduced for Ceva's theorem, points X, Y, Z are collinear if and only if

$$\frac{\overrightarrow{BX}}{\overrightarrow{XC}} \cdot \frac{\overrightarrow{CY}}{\overrightarrow{YA}} \cdot \frac{\overrightarrow{AZ}}{\overrightarrow{ZB}} = -1.$$

Theorem. [Stewart's theorem] If D is an arbitrary point on the line BC, then

$$AD^2 = \frac{\overrightarrow{DC}}{\overrightarrow{BC}} BD^2 + \frac{\overrightarrow{BD}}{\overrightarrow{BC}} CD^2 - \overrightarrow{BD} \cdot \overrightarrow{DC}.$$

Specifically, if D is the midpoint of BC, then $4AD^2 = 2AB^2 + 2AC^2 - BC^2$.

Barycenters

Definition. A *mass point* (A, m) is a point A which is assigned a *mass* $m > 0$.

Definition. The *mass center* (*barycenter*) of the set of mass points (A_i, m_i), $i = 1, 2, \dots, n$, is the point T such that $\sum_i m_i \overrightarrow{TA_i} = 0$.

Theorem. [Leibniz's theorem] Let T be the mass center of the set of mass points $\{(A_i, m_i) \mid i = 1, 2, \dots, n\}$ of total mass $m = m_1 + \cdots + m_n$, and let X be an arbitrary point. Then

$$\sum_{i=1}^{n} m_i XA_i^2 = \sum_{i=1}^{n} m_i TA_i^2 + mXT^2.$$

Specifically, if T is the centroid of $\triangle ABC$ and X an arbitrary point, then

$$AX^2 + BX^2 + CX^2 = AT^2 + BT^2 + CT^2 + 3XT^2 .$$

Quadrilaterals

Theorem. A quadrilateral $ABCD$ is cyclic (i.e., there exists a circumcircle of $ABCD$) if and only if $\angle ACB = \angle ADB$ and if and only if $\angle ADC + \angle ABC = 180^\circ$.

Theorem. [Ptolemy's theorem] A convex quadrilateral $ABCD$ is cyclic if and only if

$$AC \cdot BD = AB \cdot CD + AD \cdot BC.$$

For an arbitrary quadrilateral $ABCD$ we have *Ptolemy's inequality* (see , Geometric Inequalities).

Theorem. [Casey's theorem] Let k_1, k_2, k_3, k_4 be four circles that all touch a given circle k. Let t_{ij} be the length of a segment determined by an external common tangent of circles k_i and k_j $(i, j \in \{1, 2, 3, 4\})$ if both k_i and k_j touch k internally, or both touch k externally. Otherwise, t_{ij} is set to be the internal common tangent. Then one of the products $t_{12}t_{34}$, $t_{13}t_{24}$, and $t_{14}t_{23}$ is the sum of the other two.

The IMO Compendium Group,
D. Djukić, V. Janković, I. Matić, N. Petrović
www.imo.org.yu

Some of the circles k_1, k_2, k_3, k_4 may be degenerate, i.e. of 0 radius and thus reduced to being points. In particular, for three points A, B, C on a circle k and a circle k' touching k at a point on the arc of AC not containing B, we have $AC \cdot b = AB \cdot c + a \cdot BC$, where a, b, and c are the lengths of the tangent segments from points A, B, and C to k'. *Ptolemy's theorem* is a special case of Casey's theorem when all four circles are degenerate.

Theorem. A convex quadrilateral $ABCD$ is tangent (i.e., there exists an incircle of $ABCD$) if and only if

$$AB + CD = BC + DA.$$

Theorem. For arbitrary points A, B, C, D in space, $AC \perp BD$ if and only if

$$AB^2 + CD^2 = BC^2 + DA^2.$$

Theorem. [Newton's theorem] Let $ABCD$ be a quadrilateral, $AD \cap BC = E$, and $AB \cap DC = F$ (such points A, B, C, D, E, F form a *complete quadrilateral*). Then the midpoints of AC, BD, and EF are collinear. If $ABCD$ is tangent, then the incenter also lies on this line.

Theorem. [Brocard's theorem] Let $ABCD$ be a quadrilateral inscribed in a circle with center O, and let $P = AB \cap CD$, $Q = AD \cap BC$, $R = AC \cap BD$. Then O is the orthocenter of $\triangle PQR$.

Circle Geometry

Theorem. [Pascal's theorem] If $A_1, A_2, A_3, B_1, B_2, B_3$ are distinct points on a conic γ (e.g., circle), then points $X_1 = A_2B_3 \cap A_3B_2$, $X_2 = A_1B_3 \cap A_3B_1$, and $X_3 = A_1B_2 \cap A_2B_1$ are collinear. The special result when γ consists of two lines is called *Pappus's theorem.*

Theorem. [Brianchon's theorem] Let $ABCDEF$ be an arbitrary convex hexagon circumscribed about a conic (e.g., circle). Then AD, BE and CF meet in a point.

Theorem. [The butterfly theorem] Let AB be a segment of circle k and C its midpoint. Let p and q be two different lines through C that, respectively, intersect k on one side of AB in P and Q and on the other in P' and Q'. Let E and F respectively be the intersections of PQ' and $P'Q$ with AB. Then it follows that $CE = CF$.

Definition. The *power* of a point X with respect to a circle $k(O, r)$ is defined by $\mathcal{P}(X) = OX^2 - r^2$. For an arbitrary line l through X that intersects k at A and B ($A = B$ when l is a tangent), it follows that $\mathcal{P}(X) = \overrightarrow{XA} \cdot \overrightarrow{XB}$.

Definition. The *radical axis* of two circles is the locus of points that have equal powers with respect to both circles. The radical axis of circles $k_1(O_1, r_1)$ and $k_2(O_2, r_2)$ is a line perpendicular to O_1O_2. The radical axes of three distinct circles are concurrent or mutually parallel. If concurrent, the intersection of the three axes is called the *radical center.*

Definition. The *pole* of a line $l \not\ni O$ with respect to a circle $k(O,r)$ is a point A on the other side of l from O such that $OA \perp l$ and $d(O,l)\cdot OA = r^2$. In particular, if l intersects k in two points, its pole will be the intersection of the tangents to k at these two points.

Definition. The polar *of the point A from the previous definition is the line l. In particular, if A is a point outside k and AM, AN are tangents to k ($M,N \in k$), then MN is the polar of A.*
Poles and polares are generally defined in a similar way with respect to arbitrary non-degenerate conics.

Theorem. If A belongs to a polar of B, then B belongs to a polar of A.

Inversion

Definition. An *inversion* of the plane π around the circle $k(O,r)$ (which belongs to π), is a transformation of the set $\pi\backslash\{O\}$ onto itself such that every point P is transformed into a point P' on $(OP$ such that $OP \cdot OP' = r^2$. In the following statements we implicitly assume exclusion of O.

Theorem. The fixed points of the inversion are on the circle k. The inside of k is transformed into the outside and vice versa.

Theorem. If A,B transform into A',B' after an inversion, then $\angle OAB = \angle OB'A'$, and also $ABB'A'$ is cyclic and perpendicular to k. A circle perpendicular to k transforms into itself. Inversion preserves angles between continuous curves (which includes lines and circles).

Theorem. An inversion transforms lines not containing O into circles containing O, lines containing O into themselves, circles not containing O into circles not containing O, circles containing O into lines not containing O.

Geometric Inequalities

Theorem. [The triangle inequality] For any three points A,B,C in a plane $AB + BC \geq AC$. Equality occurs when A,B,C are collinear and $\mathcal{B}(A,B,C)$.

Theorem. [Ptolemy's inequality] For any four points A, B, C, D,

$$AC \cdot BD \leq AB \cdot CD + AD \cdot BC.$$

Theorem. [The parallelogram inequality] For any four points A, B, C, D,

$$AB^2 + BC^2 + CD^2 + DA^2 \geq AC^2 + BD^2.$$

Equality occurs if and only if $ABCD$ is a parallelogram.

Theorem. For a given triangle $\triangle ABC$ the point X for which $AX + BX + CX$ is minimal is Toricelli's point when all angles of $\triangle ABC$ are less than or equal to $120°$, and is the vertex of the obtuse angle otherwise. The point X_2 for which $AX_2^2 + BX_2^2 + CX_2^2$ is minimal is the centroid (see Leibniz's theorem).

The IMO Compendium Group,
D. Djukić, V. Janković, I. Matić, N. Petrović
www.imo.org.yu

Theorem. [The Erdős–Mordell inequality] Let P be a point in the interior of $\triangle ABC$ and X, Y, Z projections of P onto BC, AC, AB, respectively. Then

$$PA + PB + PC \geq 2(PX + PY + PZ).$$

Equality holds if and only if $\triangle ABC$ is equilateral and P is its center.

Trigonometry

Definition. The *trigonometric circle* is the unit circle centered at the origin O of a coordinate plane. Let A be the point $(1,0)$ and $P(x,y)$ be a point on the trigonometric circle such that $\measuredangle AOP = \alpha$. We define $\sin\alpha = y$, $\cos\alpha = x$, $\tan\alpha = y/x$, and $\cot\alpha = x/y$.

Theorem. The functions sin and cos are periodic with period 2π. The functions tan and cot are periodic with period π. The following simple identities hold: $\sin^2 x + \cos^2 x = 1$, $\sin 0 = \sin\pi = 0$, $\sin(-x) = -\sin x$, $\cos(-x) = \cos x$, $\sin(\pi/2) = 1$, $\sin(\pi/4) = 1/\sqrt{2}$, $\sin(\pi/6) = 1/2$, $\cos x = \sin(\pi/2 - x)$. From these identities other identities can be easily derived.

Theorem. Additive formulas for trigonometric functions:

$$\begin{array}{ll} \sin(\alpha \pm \beta) = \sin\alpha\cos\beta \pm \cos\alpha\sin\beta, & \tan(\alpha \pm \beta) = \frac{\tan\alpha \pm \tan\beta}{1 \mp \tan\alpha\tan\beta}, \\ \cos(\alpha \pm \beta) = \cos\alpha\cos\beta \mp \sin\alpha\sin\beta, & \cot(\alpha \pm \beta) = \frac{\cot\alpha\cot\beta \mp 1}{\cot\alpha \pm \cot\beta}. \end{array}$$

Theorem. Formulas for trigonometric functions of $2x$ and $3x$:

$$\begin{array}{rclrcl} \sin 2x & = & 2\sin x\cos x, & \sin 3x & = & 3\sin x - 4\sin^3 x, \\ \cos 2x & = & 2\cos^2 x - 1, & \cos 3x & = & 4\cos^3 x - 3\cos x, \\ \tan 2x & = & \frac{2\tan x}{1 - \tan^2 x}, & \tan 3x & = & \frac{3\tan x - \tan^3 x}{1 - 3\tan^2 x}. \end{array}$$

Theorem. For any $x \in \mathbb{R}$, $\sin x = \frac{2t}{1+t^2}$ and $\cos x = \frac{1-t^2}{1+t^2}$, where $t = \tan\frac{x}{2}$.

Theorem. Transformations from product to sum:

$$\begin{array}{rcl} 2\cos\alpha\cos\beta & = & \cos(\alpha+\beta) + \cos(\alpha-\beta), \\ 2\sin\alpha\cos\beta & = & \sin(\alpha+\beta) + \sin(\alpha-\beta), \\ 2\sin\alpha\sin\beta & = & \cos(\alpha-\beta) - \cos(\alpha+\beta). \end{array}$$

Theorem. The angles α, β, γ of a triangle satisfy

$$\begin{array}{rcl} \cos^2\alpha + \cos^2\beta + \cos^2\gamma + 2\cos\alpha\cos\beta\cos\gamma & = & 1, \\ \tan\alpha + \tan\beta + \tan\gamma & = & \tan\alpha\tan\beta\tan\gamma. \end{array}$$

Theorem. [De Moivre's formula] If $i^2 = -1$, then

$$(\cos x + i\sin x)^n = \cos nx + i\sin nx.$$

Formulas in Geometry

Theorem. [Heron's formula] The area of a triangle ABC with sides a, b, c and semiperimeter s is given by

$$S = \sqrt{s(s-a)(s-b)(s-c)} = \frac{1}{4}\sqrt{2a^2b^2 + 2a^2c^2 + 2b^2c^2 - a^4 - b^4 - c^4}.$$

Theorem. [The law of sines] The sides a, b, c and angles α, β, γ of a triangle ABC satisfy

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R,$$

where R is the circumradius of $\triangle ABC$.

Theorem. [The law of cosines] The sides and angles of $\triangle ABC$ satisfy

$$c^2 = a^2 + b^2 - 2ab\cos\gamma.$$

Theorem. The circumradius R and inradius r of a triangle ABC satisfy $R = \frac{abc}{4S}$ and $r = \frac{2S}{a+b+c} = R(\cos\alpha + \cos\beta + \cos\gamma - 1)$. If x, y, z denote the distances of the circumcenter in an acute triangle to the sides, then $x + y + z = R + r$.

Theorem. [Euler's formula] If O and I are the circumcenter and incenter of $\triangle ABC$, then $OI^2 = R(R-2r)$, where R and r are respectively the circumradius and the inradius of $\triangle ABC$. Consequently, $R \geq 2r$.

Theorem. The area S of a quadrilateral $ABCD$ with sides a, b, c, d, semiperimeter p, and angles α, γ at vertices A, C respectively is given by

$$S = \sqrt{(p-a)(p-b)(p-c)(p-d) - abcd\cos^2\frac{\alpha+\gamma}{2}}\;.$$

If $ABCD$ is a cyclic quadrilateral, the above formula reduces to

$$S = \sqrt{(p-a)(p-b)(p-c)(p-d)}.$$

Theorem. [Euler's theorem for pedal triangles] Let X, Y, Z be the feet of the perpendiculars from a point P to the sides of a triangle ABC. Let O denote the circumcenter and R the circumradius of $\triangle ABC$. Then

$$S_{XYZ} = \frac{1}{4}\left|1 - \frac{OP^2}{R^2}\right| S_{ABC}\;.$$

Moreover, $S_{XYZ} = 0$ if and only if P lies on the circumcircle of $\triangle ABC$ (see *Simson's line*).

Theorem. If $\overrightarrow{a} = (a_1, a_2, a_3)$, $\overrightarrow{b} = (b_1, b_2, b_3)$, $\overrightarrow{c} = (c_1, c_2, c_3)$ are three vectors in coordinate space, then

$$\overrightarrow{a}\cdot\overrightarrow{b} = a_1b_1 + a_2b_2 + a_3b_3, \quad \overrightarrow{a}\times\overrightarrow{b} = (a_1b_2 - a_2b_1, a_2b_3 - a_3b_2, a_3b_1 - a_1b_3),$$

$$[\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}] = \left\| \begin{array}{ccc} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{array} \right\| .$$

Theorem. The area of a triangle ABC and the volume of a tetrahedron $ABCD$ are equal to $|\overrightarrow{AB} \times \overrightarrow{AC}|$ and $\left|\left[\overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{AD}\right]\right|$, respectively.

Theorem. [Cavalieri's principle] If the sections of two solids by the same plane always have equal area, then the volumes of the two solids are equal.

Number Theory

Divisibility and Congruences

Definition. *The greatest common divisor* $(a, b) = \gcd(a, b)$ of $a, b \in \mathbb{N}$ is the largest positive integer that divides both a and b. Positive integers a and b are *coprime* or *relatively prime* if $(a, b) = 1$. *The least common multiple* $[a, b] = \operatorname{lcm}(a, b)$ of $a, b \in \mathbb{N}$ is the smallest positive integer that is divisible by both a and b. It holds that $[a, b](a, b) = ab$. The above concepts are easily generalized to more than two numbers; i.e., we also define $(a_1, a_2, \dots, a_n)$ and $[a_1, a_2, \dots, a_n]$.

Theorem. [Euclid's algorithm] Since $(a, b) = (|a - b|, a) = (|a - b|, b)$ it follows that starting from positive integers a and b one eventually obtains (a, b) by repeatedly replacing a and b with $|a - b|$ and $\min\{a, b\}$ until the two numbers are equal. The algorithm can be generalized to more than two numbers.

Theorem. [Corollary to Euclid's algorithm] For each $a, b \in \mathbb{N}$ there exist $x, y \in \mathbb{Z}$ such that $ax + by = (a, b)$. The number (a, b) is the smallest positive number for which such x and y can be found.

Theorem. [Second corollary to Euclid's algorithm] For $a, m, n \in \mathbb{N}$ and $a > 1$ it follows that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Theorem. [Fundamental theorem of arithmetic] Every positive integer can be uniquely represented as a product of primes, up to their order.

Theorem. The fundamental theorem of arithmetic also holds in some other rings, such as $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$ (where ω is a complex third root of 1). In these cases, the factorization into primes is unique up to the order and divisors of 1.

Definition. Integers a, b are *congruent modulo* $n \in \mathbb{N}$ if $n \mid a - b$. We then write $a \equiv b \pmod{n}$.

Theorem. [Chinese remainder theorem] If $m_1, m_2, \dots, m_k$ are positive integers pairwise relatively prime and $a_1, \dots, a_k$, $c_1, \dots, c_k$ are integers such that $(a_i, m_i) = 1$ $(i = 1, \dots, n)$, then the system of congruences

$$a_i x \equiv c_i \ (mod\ m_i), \qquad i = 1, 2, \dots, n\ ,$$

has a unique solution modulo $m_1 m_2 \cdots m_k$.

www.imo.org.yu

The IMO Compendium Group,
D. Djukić, V. Janković, I. Matić, N. Petrović
www.imo.org.yu

Exponential Congruences

Theorem. [Wilson's theorem] If p is a prime, then $p \mid (p-1)! + 1$.

Theorem. [Fermat's (little) theorem] Let p be a prime number and a be an integer with $(a, p) = 1$. Then $a^{p-1} \equiv 1$ *(mod p)*. This theorem is a special case of Euler's theorem.

Definition. *Euler's function* $\varphi(n)$ is defined for $n \in \mathbb{N}$ as the number of positive integers less than n and coprime to n. It holds that

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

where $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the factorization of n into primes.

Theorem. [Euler's theorem] Let n be a natural number and a be an integer with $(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1$ *(mod n)*.

Theorem. [Existence of primitive roots] Let p be a prime. There exists $g \in \{1, 2, \ldots, p-1\}$ (called a *primitive root* modulo p) such that the set $\{1, g, g^2, \ldots, g^{p-2}\}$ is equal to $\{1, 2, \ldots, p-1\}$ modulo p.

Definition. Let p be a prime and α be a nonnegative integer. We say that p^α is the *exact power* of p that divides an integer a (and α the *exact exponent*) if $p^\alpha \mid a$ and $p^{\alpha+1} \nmid a$.

Theorem. Let a, n be positive integers and p be an odd prime. If p^α ($\alpha \in \mathbb{N}$) is the exact power of p that divides $a-1$, then for any integer $\beta \geq 0$, $p^{\alpha+\beta} \mid a^n - 1$ if and only if $p^\beta \mid n$.

A similar statement holds for $p = 2$. If 2^α ($\alpha \in \mathbb{N}$) is the exact power of 2 that divides $a^2 - 1$, then for any integer $\beta \geq 0$, $2^{\alpha+\beta} \mid a^n - 1$ if and only if $2^{\beta+1} \mid n$.

Quadratic Diophantine Equations

Theorem. The solutions of $a^2 + b^2 = c^2$ in integers are given by $a = t(m^2 - n^2)$, $b = 2tmn$, $c = t(m^2 + n^2)$ (provided that b is even), where $t, m, n \in \mathbb{Z}$. The triples (a, b, c) are called *Pythagorean* (or *primitive Pythagorean* if $\gcd(a, b, c) = 1$).

Definition. Given $D \in \mathbb{N}$ that is not a perfect square, a *Pell's equation* is an equation of the form $x^2 - Dy^2 = 1$, where $x, y \in \mathbb{Z}$.

Theorem. If (x_0, y_0) is the least (nontrivial) solution in $\mathbb{N}$ of the Pell's equation $x^2 - Dy^2 = 1$, then all the integer solutions (x, y) are given by $x + y\sqrt{D} = \pm(x_0 + y_0\sqrt{D})^n$, where $n \in \mathbb{Z}$.

Definition. An integer a is a *quadratic residue* modulo a prime p if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$. Otherwise, a is a *quadratic nonresidue* modulo p.

The IMO Compendium Group
www.imo.org.yu

The IMO Compendium Group,
D. Djukić, V. Janković, I. Matić, N. Petrović
www.imo.org.yu

Definition. *Legendre's symbol* for an integer a and a prime p is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \text{ and } p \nmid a; \\ 0 & \text{if } p \mid a; \\ -1 & \text{otherwise.} \end{cases}$$

Clearly $\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right)$ and $\left(\frac{a^2}{p}\right) = 1$ if $p \nmid a$. Legendre's symbol is multiplicative, i.e., $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Theorem. [Euler's criterion] For each odd prime p and integer a not divisible by p, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \ (mod\ p)$.

Theorem. For a prime $p > 3$, $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{-3}{p}\right)$ are equal to 1 if and only if $p \equiv 1 \ (mod\ 4)$, $p \equiv \pm 1 \ (mod\ 8)$ and $p \equiv 1 \ (mod\ 6)$, respectively.

Theorem. [Gauss's Reciprocity law] For any two distinct odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Definition. *Jacobi's symbol* for an integer a and an odd positive integer b is defined as

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k},$$

where $b = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the factorization of b into primes.

Theorem. If $\left(\frac{a}{b}\right) = -1$, then a is a quadratic nonresidue modulo b, but the converse is false. All the above identities for Legendre symbols except Euler's criterion remain true for Jacobi symbols.

Farey Sequences

Definition. For any positive integer n, the *Farey sequence* F_n is the sequence of rational numbers a/b with $0 \le a \le b \le n$ and $(a, b) = 1$ arranged in increasing order. For instance, $F_3 = \{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\}$.

Theorem. If p_1/q_1, p_2/q_2, and p_3/q_3 are three successive terms in a Farey sequence, then

$$p_2q_1 - p_1q_2 = 1 \quad \text{and} \quad \frac{p_1 + p_3}{q_1 + q_3} = \frac{p_2}{q_2}.$$

Combinatorics

Counting of Objects

Many combinatorial problems involving the counting of objects satisfying a given set of properties can be properly reduced to an application of one of the following concepts.

Definition. A *variation* of order n over k is a 1 to 1 mapping of $\{1,2,\ldots,k\}$ into $\{1,2,\ldots,n\}$. For a given n and k, where $n \geq k$, the number of different variations is $V_n^k = \frac{n!}{(n-k)!}$.

Definition. A *variation with repetition* of order n over k is an arbitrary mapping of $\{1,2,\ldots,k\}$ into $\{1,2,\ldots,n\}$. For a given n and k the number of different variations with repetition is $\overline{V}_n^k = k^n$.

Definition. A *permutation* of order n is a bijection of $\{1,2,\ldots,n\}$ into itself (a special case of variation for $k = n$). For a given n the number of different permutations is $P_n = n!$.

Definition. A *combination* of order n over k is a k-element subset of $\{1,2,\ldots,n\}$. For a given n and k the number of different combinations is $C_n^k = \binom{n}{k}$.

Definition. A *permutation with repetition* of order n is a bijection of $\{1,2,\ldots,n\}$ into a *multiset* of n elements. A multiset is defined to be a set in which certain elements are deemed mutually indistinguishable (for example, as in $\{1,1,2,3\}$).

If $\{1,2\ldots,s\}$ denotes a set of different elements in the multiset and the element i appears α_i times in the multiset, then number of different permutations with repetition is $P_{n,\alpha_1,\ldots,\alpha_s} = \frac{n!}{\alpha_1!\cdot\alpha_2!\cdots\alpha_s!}$. A combination is a special case of permutation with repetition for a multiset with two different elements.

Theorem. [The pigeonhole principle] If a set of $nk+1$ different elements is partitioned into n mutually disjoint subsets, then at least one subset will contain at least $k+1$ elements.

Theorem. [The inclusion–exclusion principle] Let $S_1, S_2, \ldots, S_n$ be a family of subsets of the set S. The number of elements of S contained in none of the subsets is given by the formula

$$|S \backslash (S_1 \cup \cdots \cup S_n)| = |S| - \sum_{k=1}^{n} \sum_{1 \leq i_1 < \cdots < i_k \leq n} (-1)^k |S_{i_1} \cap \cdots \cap S_{i_k}| \,.$$

Graph Theory

Definition. A *graph* $G = (V,E)$ is a set of objects, i.e., *vertices*, V paired with the multiset E of some pairs of elements of V, i.e., *edges*. When $(x,y) \in E$, for $x, y \in V$, the vertices x and y are said to be *connected* by an edge; i.e., the vertices are the *endpoints* of the edge.

A graph for which the multiset E reduces to a proper set (i.e., the vertices are connected by at most one edge) and for which no vertex is connected to itself is called a *proper graph*.

A *finite graph* is one in which $|E|$ and $|V|$ are finite.

Definition. An *oriented graph* is one in which the pairs in E are ordered.

Definition. A proper graph K_n containing n vertices and in which each pair of vertices is connected is called a *complete* graph.

Definition. A *k-partite graph* (*bipartite* for $k = 2$) $K_{i_1,i_2,\dots,i_k}$ is a graph whose set of vertices V can be partitioned into k non-empty disjoint subsets of cardinalities $i_1, i_2, \dots, i_k$ such that each vertex x in a subset W of V is connected only with the vertices not in W.

Definition. The *degree* $d(x)$ of a vertex x is the number of times x is the endpoint of an edge (thus, self-connecting edges are counted twice). An *isolated vertex* is one with the degree 0.

Theorem. For a graph $G = (V, E)$ the following identity holds:

$$\sum_{x \in V} d(x) = 2|E|.$$

As a consequence, the number of vertices of odd degree is even.

Definition. A *trajectory* (*path*) of a graph is a finite sequence of vertices, each connected to the previous one. The *length* of a trajectory is the number of edges through which it passes. A *circuit* is a path that ends in the starting vertex. A *cycle* is a circuit in which no vertex appears more than once (except the initial/final vertex).

A graph is *connected* if there exists a trajectory between any two vertices.

Definition. A *subgraph* $G' = (V', E')$ of a graph $G = (V, E)$ is a graph such that $V' \subseteq V$ and E' contains exactly the edges of E connecting points in V'. A *connected component* of a graph is a connected subgraph such that no vertex of the component is connected with any vertex outside of the component.

Definition. A *tree* is a connected graph that contains no cycles.

Theorem. A tree with n vertices has exactly $n-1$ edges and at least two vertices of degree 1.

Definition. An *Euler path* is a path in which each edge appears exactly once. Likewise, an *Euler circuit* is an Euler path that is also a circuit.

Theorem. The following conditions are necessary and sufficient for a finite connected graph G to have an Euler path:

- If each vertex has even degree, then the graph contains an Euler circuit.
- If all vertices except two have even degree, then the graph contains an Euler path that is not a circuit (it starts and ends in the two odd vertices).

Definition. A *Hamilton circuit* is a circuit that contains each vertex of G exactly once (trivially, it is also a cycle).

A simple rule to determine whether a graph contains a Hamilton circuit has not yet been discovered.

Theorem. Let G be a graph with n vertices. If the sum of the degrees of any two nonadjacent vertices in G is greater than n, then G has a Hamiltonian circuit.

Theorem. [Ramsey's theorem] Let $r \geq 1$ and $q_1, q_2, \dots, q_s \geq r$. There exists a minimal positive integer $N(q_1, q_2, \dots, q_s; r)$ such that for $n \geq N$, if all subgraphs K_r of K_n are partitioned into s different sets, labeled $A_1, A_2 \dots, A_s$, then for some i there exists a complete subgraph K_{q_i} whose subgraphs K_r all belong to A_i. For $r = 2$ this corresponds to coloring the edges of K_n with s different colors and looking for i monochromatically colored subgraphs K_{q_i}.

Theorem. $N(p, q; r) \leq N(N(p-1, q; r), N(p, q-1; r); r-1)+1$, and in particular, $N(p, q; 2) \leq N(p-1, q; 2) + N(p, q-1; 2)$.

The following values of N are known: $N(p, q; 1) = p + q - 1$, $N(2, p; 2) = p$, $N(3, 3; 2) = 6$, $N(3, 4; 2) = 9$, $N(3, 5; 2) = 14$, $N(3, 6; 2) = 18$, $N(3, 7; 2) = 23$, $N(3, 8; 2) = 28$, $N(3, 9; 2) = 36$, $N(4, 4; 2) = 18$, $N(4, 5; 2) = 25$.

Theorem. [Turán's theorem] If a simple graph on $n = t(p-1) + r$ vertices has more than $f(n, p)$ edges, where $f(n, p) = \frac{(p-2)n^2 - r(p-1-r)}{2(p-1)}$, then it contains K_p as a subgraph. The graph containing $f(n, p)$ vertices that does not contain K_p is the complete multipartite graph with r subsets of size $t + 1$ and $p - 1 - r$ subsets of size t.

Definition. A *planar graph* is one that can be embedded in a plane such that its vertices are represented by points and its edges by lines (not necessarily straight) connecting the vertices such that the edges do not intersect each other.

Theorem. A planar graph with n vertices has at most $3n - 6$ edges.

Theorem. [Kuratowski's theorem] Graphs K_5 and $K_{3,3}$ are not planar. Every nonplanar graph contains a subgraph which can be obtained from one of these two graphs by a subdivison of its edges.

Theorem. [Euler's formula] For a given convex polyhedron let E be the number of its edges, F the number of faces, and V the number of vertices. Then $E+2 = F + V$. The same formula holds for a planar graph (F is in this case equal to the number of planar regions).