Trivium of Theorems and Lemmas

American Masters in Mathematics

OMEGA

February 2026

Contents

1 Preface **2**
1.1 Motivation . . . 2
1.2 What this TOTAL is not . . . 2
1.3 Contributing . . . 2
1.4 Explicitly forbidden theorems . . . 2

2 General blanket statements **3**

3 Additional theorems in algebra **3**
3.1 Functional equations . . . 3
3.2 Polynomials . . . 3

4 Additional theorems in combinatorics **4**
4.1 Graph theory . . . 4
4.2 Game theory . . . 4
4.3 Extremal combinatorics . . . 4
4.4 Enumerative identities . . . 4

5 Additional theorems in geometry **4**
5.1 Blanket statements . . . 4
5.2 Projective results . . . 4

6 Additional theorems in number theory **5**
6.1 Famous theorems . . . 5
6.2 Modular arithmetic . . . 5
6.3 Integer polynomials . . . 5
6.4 Results relating to ν_p . . . 6
6.5 Numerical semigroups . . . 6

7 Additional theorems in linear algebra **6**

8 Additional theorems in abstract algebra **6**

9 Additional theorems in real and complex analysis **7**

§1 Preface

§1.1 Motivation

In math competitions, there is often significant confusion or "gray areas" in what results are allowed to cite on competitions. The aim of the TOTAL is to resolve that ambiguity, as follows:

- Every theorem that appears in TOTAL may be quoted on our exams. We expect this to cover the extreme majority of use cases.
- On rare occasions, we may choose to disallow certain results (see subsection 1.4).
- In the case of results which are neither allowed nor forbidden, the discretion is up to the organizers. Our general guidance is to accept named theorems that do not trivialize the problem. However, we hope that this situation will be extremely rare, and to not occur in a typical year.

§1.2 What this TOTAL is not

The TOTAL is *not* the following:

- **This is not a list of theorems we expect everyone to know.**

  In fact, if a theorem is actually present in this PDF (rather than under "blanket statements"), that is actually an indication that it may be fairly obscure: the most important results are covered by the blanket statements.

  We strongly anti-recommend using the TOTAL as any sort of study guide, or trying to memorize theorems that you see in TOTAL. That would be a lot like trying to learn English as a second language by memorizing the Merriam-Webster dictionary.
- The TOTAL is meant to cover 99% of the common situations, not 100%. We don't think it's prudent to try to anticipate literally everything, and we leave the extremely rare corner cases up to grader discretion.

§1.3 Contributing

If your favorite theorem is not included here, you may submit a pull request on GitHub to consider it for inclusion. See CONTRIBUTING.md for guidelines.

§1.4 Explicitly forbidden theorems

In rare cases, OMEGA may decide to reject a request to add a certain theorem to the TOTAL. A list of such cases, and their accompanying pull requests, are listed here:

No forbidden results yet.

§2 General blanket statements

Any theorem appearing in any of the following sources may be quoted:

- The OMEGA syllabus
- The Art and Craft of Problem Solving (Paul Zeitz)
- The Art of Problem Solving Volumes 1 and 2 (Sandor Lehoczky and Richard Rusczyk)
- Chapter 2: Basic Concepts and Facts, from The IMO Compendium

§3 Additional theorems in algebra

As a blanket statement, we allow any results in *Olympiad Inequalities* by Thomas Mildorf.[1]

§3.1 Functional equations

Theorem 3.1 (Properties of Cauchy functional equation)**.** Suppose $f\colon \mathbb{R} \to \mathbb{R}$ satisfies $f(x+y) = f(x) + f(y)$. Then $f(qx) = qf(x)$ for any $q \in \mathbb{Q}$. Moreover, f is linear if there exists $(a, b) \in \mathbb{R}^2$ and $\varepsilon > 0$ such that $(x-a)^2 + (f(x)-b)^2 > \varepsilon$ for every x.

§3.2 Polynomials

Theorem 3.2 (Mason–Stothers theorem)**.** Let $a(t)$, $b(t)$, $c(t)$ be pairwise coprime polynomials over a field, not all constant, satisfying $a + b + c = 0$. Then

$$\max(\deg a, \deg b, \deg c) \le n_0(abc) - 1,$$

where $n_0(f)$ denotes the number of distinct roots of f.

Theorem 3.3 (Lagrange interpolation formula)**.** Let k be a field of characteristic zero. Given $n+1$ distinct pairs $(x_0, y_0), \ldots, (x_n, y_n)$ in k^2 with x_i pairwise distinct, the unique polynomial of degree at most n passing through all of them is

$$P(x) = \sum_{i=0}^{n} y_i \prod_{\substack{0 \le j \le n \\ j \ne i}} \frac{x - x_j}{x_i - x_j}.$$

Theorem 3.4 (Newton's forward difference formula)**.** Define forward differences by $\Delta^0 f(x) = f(x)$ and $\Delta^k f(x) = \Delta^{k-1} f(x+1) - \Delta^{k-1} f(x)$. Then for any polynomial f of degree at most n,

$$f(x) = \sum_{k=0}^{n} \binom{x}{k} \Delta^k f(0).$$

[1] This includes the so-called $n-1$ equal value principle mentioned in the footnote on page 15: suppose $f\colon \mathbb{R} \to \mathbb{R}$ is a function with exactly one inflection point and s is a fixed real number. Consider optimizing $\sum f(x_i)$ subject to $\sum x_i = s$. If a maximum or minimum exists, it can be achieved when $n-1$ variables are equal.

§4 Additional theorems in combinatorics

§4.1 Graph theory

Theorem 4.1 (Max flow min cut)**.** In a flow network, the maximum value of a flow from source s to sink t equals the minimum capacity of an s-t cut.

Theorem 4.2 (Four color theorem)**.** Every planar graph is 4-colorable.

§4.2 Game theory

Theorem 4.3 (Sprague–Grundy theorem)**.** Every impartial game under the normal play convention is equivalent to a Nim heap of some size $n \geq 0$. The Grundy value of a position is the minimum excludant (mex) of the Grundy values of the positions reachable in one move.

§4.3 Extremal combinatorics

Theorem 4.4 (Dilworth's theorem)**.** In any finite partially ordered set, the maximum size of an antichain equals the minimum number of chains needed to partition the set.

Theorem 4.5 (Erdős–Szekeres theorem)**.** Every sequence of more than $(r-1)(s-1)$ distinct real numbers contains an increasing subsequence of length r or a decreasing subsequence of length s.

§4.4 Enumerative identities

Theorem 4.6 (Hook-length formula)**.** The number of standard Young tableaux of shape λ with $n = |\lambda|$ cells is

$$\frac{n!}{\prod_{u \in \lambda} h(u)},$$

where $h(u)$ is the hook length of cell u.

§5 Additional theorems in geometry

§5.1 Blanket statements

We will allow without proof any results from *Euclidean Geometry in Mathematical Olympiads* by Evan Chen.

§5.2 Projective results

Theorem 5.1 (Desargues involution theorem)**.** Let $ABCD$ be four points on a conic, and let ℓ be a line. Then the three pairs of points $(AB \cap \ell,\ CD \cap \ell)$, $(AC \cap \ell,\ BD \cap \ell)$, $(AD \cap \ell,\ BC \cap \ell)$ are in involution. If ℓ meets the conic at points P and Q, then (P, Q) is also a pair in this involution.

§6 Additional theorems in number theory

§6.1 Famous theorems

Theorem 6.1 (Prime number theorem for arithmetic progressions)**.** For coprime positive integers a and q, the number of primes $p \leq x$ with $p \equiv a \pmod{q}$ is

$$(1 + o(1))\frac{x}{\varphi(q)\ln x}$$

as $x \to \infty$. In particular, every such arithmetic progression contains infinitely many primes.

Theorem 6.2 (Zsigmondy's theorem)**.** For coprime integers $a > b > 0$ and $n \geq 3$, the number $a^n - b^n$ has a prime divisor that does not divide $a^k - b^k$ for any $1 \leq k < n$, with the sole exception $(a, b, n) = (2, 1, 6)$.

Theorem 6.3 (Kobayashi's theorem)**.** Let S be an infinite set of integers. Then there is at most one integer $a \in \mathbb{Z}$ such that

$$\{p \text{ prime} : p \mid s + a \text{ for some} s \in S\}$$

is finite.

Theorem 6.4 (Bertrand's postulate)**.** For every integer $n \geq 2$, there exists a prime p with $n < p < 2n$.

Theorem 6.5 (Bounded gaps)**.** There are infinitely many pairs of primes differing by at most 246.

Theorem 6.6 (Faltings' theorem)**.** An algebraic curve of genus $g \geq 2$ over a number field has only finitely many rational points.

Theorem 6.7 (Mihăilescu's theorem, aka Catalan conjecture)**.** The only solution in integers $x, y, a, b > 1$ to $x^a - y^b = 1$ is $3^2 - 2^3 = 1$.

Theorem 6.8 (Vinogradov's theorem)**.** Every sufficiently large odd integer can be expressed as the sum of three primes.

Theorem 6.9 (Chen's theorem)**.** Every sufficiently large even integer can be written as the sum of a prime and a semiprime (a product of at most two primes).

Theorem 6.10 (Fermat's last theorem)**.** There are no solutions in positive integers to $a^n + b^n = c^n$ for any integer $n \geq 3$.

§6.2 Modular arithmetic

Theorem 6.11 (Thue's lemma)**.** For a prime p and integer a with $p \nmid a$, there exist integers x, y with $1 \leq x, y \leq \lfloor\sqrt{p}\rfloor$ such that $ax \equiv \pm y \pmod{p}$.

§6.3 Integer polynomials

Theorem 6.12 (Cohn's criterion)**.** Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$ and $0 \leq a_i \leq b - 1$ for some integer $b \geq 2$. If $f(b)$ is prime, then $f(x)$ is irreducible over $\mathbb{Z}$.

Theorem 6.13 (Hensel's lemma)**.** Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime. If $a \in \mathbb{Z}$ satisfies $f(a) \equiv 0 \pmod{p^k}$ and $p \nmid f'(a)$, then there is a unique $b \pmod{p^{k+1}}$ with $b \equiv a \pmod{p^k}$ and $f(b) \equiv 0 \pmod{p^{k+1}}$.

§6.4 Results relating to ν_p

Theorem 6.14 (Legendre's formula)**.** For a prime p and positive integer n,

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of the digits of n in base p.

Theorem 6.15 (Lifting the exponent lemma)**.** Let p be an odd prime and let a, b be integers with $p \mid a - b$ but $p \nmid a$ and $p \nmid b$. Then

$$\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n).$$

Similarly, if $p \mid a + b$ and n is odd, then $\nu_p(a^n + b^n) = \nu_p(a+b) + \nu_p(n)$.

When $p = 2$, we instead have the following result for all odd integers x and y:

$$\nu_2(x^n - y^n) = \begin{cases} \nu_2(x-y) + \nu_2(x+y) + \nu_2(n) - 1 & n \text{ even} \\ \nu_2(x-y) & n \text{ odd.} \end{cases}$$

§6.5 Numerical semigroups

Theorem 6.16 (Chicken McNugget theorem)**.** For coprime positive integers m and n, the greatest integer that cannot be represented as $am + bn$ for nonnegative integers a, b is $mn - m - n$.

§7 Additional theorems in linear algebra

Theorem 7.1 (Spectral theorem for Hermitian matrices on $\mathbb{C}$)**.** Every Hermitian matrix can be unitarily diagonalized. Equivalently, it admits an orthonormal basis of eigenvectors, and all eigenvalues are real.

Theorem 7.2 (Cayley–Hamilton theorem)**.** Every square matrix over a commutative ring satisfies its own characteristic polynomial.

Theorem 7.3 (Farkas' lemma)**.** Let A be an $m \times n$ real matrix and $b \in \mathbb{R}^m$. Then exactly one of the following holds:

1. There exists $x \in \mathbb{R}^n$ with $Ax = b$ and $x \geq 0$.
2. There exists $y \in \mathbb{R}^m$ with $A^\top y \geq 0$ and $b^\top y < 0$.

§8 Additional theorems in abstract algebra

Theorem 8.1 (Burnside's lemma)**.** The number of orbits of a finite group G acting on a set X is

$$\frac{1}{|G|} \sum_{g \in G} |X^g|,$$

where $X^g = \{x \in X : g \cdot x = x\}$ is the set of elements fixed by g.

Theorem 8.2 (Sylow theorems)**.** Let G be a finite group of order $p^a m$ where $p \nmid m$.

1. There exists a subgroup of G of order p^a (a Sylow p-subgroup).

2. All Sylow p-subgroups are conjugate to each other.

3. The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.

Theorem 8.3 (Fundamental theorem of Galois theory)**.** Let L/K be a finite Galois extension with Galois group G. There is an inclusion-reversing bijection between intermediate fields $K \subseteq E \subseteq L$ and subgroups $H \leq G$, given by $E \mapsto \mathrm{Gal}(L/E)$ and $H \mapsto L^H$. Moreover, E/K is a normal extension if and only if the corresponding subgroup is normal in G.

Theorem 8.4 (Chebotarev density theorem)**.** Let L/K be a Galois extension of number fields with Galois group G. For any conjugacy class $C \subseteq G$, the set of unramified primes of K whose Frobenius conjugacy class equals C has natural density $|C|/|G|$.

§9 Additional theorems in real and complex analysis

Theorem 9.1 (Picard's theorem)**.** A nonconstant entire function $f\colon \mathbb{C} \to \mathbb{C}$ takes every complex value with at most one exception.

Theorem 9.2 (Taylor series for sin and cos)**.** The following two Taylor series provide analytic extensions of the sine and cosine functions from $\mathbb{C}$ to $\mathbb{C}$:

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \frac{z^6}{6!} + \dots$$
$$\sin z = z - \frac{z^3}{2!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \dots.$$

Theorem 9.3 (Extreme value theorem on compact sets)**.** A continuous real-valued function on a nonempty compact set attains its maximum and minimum values.

Theorem 9.4 (Heine–Borel theorem)**.** A subset of $\mathbb{R}^n$ is compact if and only if it is closed and bounded.

Theorem 9.5 (Bolzano–Weierstrass theorem)**.** Every bounded sequence in $\mathbb{R}^n$ has a convergent subsequence.

Theorem 9.6 (Weierstrass approximation theorem)**.** Let $f\colon [a,b] \to \mathbb{R}$ be continuous. For every $\varepsilon > 0$, there exists a polynomial p such that $|f(x) - p(x)| < \varepsilon$ for all $x \in [a,b]$.

Theorem 9.7 (Arzelà–Ascoli theorem)**.** A sequence of real-valued functions on a compact metric space has a uniformly convergent subsequence if and only if it is uniformly bounded and equicontinuous.

Theorem 9.8 (Rouché's theorem)**.** If f and g are holomorphic inside and on a simple closed contour C, and $|g(z)| < |f(z)|$ on C, then f and $f+g$ have the same number of zeros inside C, counted with multiplicity.