Number Theory Foundations

Divisibility, Integers, and more Number Theory Techniques

Aryan Ayyanger

Contents

Introduction

Divisibility and multiples make up the foundation of Olympiad number theory. At first glance, the ideas may appear elementary: a number divides another or it doesn't. However, contest mathematics requires a flexibility in divisbility application to apply seemingly simple concepts to hard problems.

There are many properties and subjects under the study of divisibility that this handout will explore. These include the Division Algorithm, modular arithmetic, Euclidean methods, prime factorization, and algebraic transformations.

Rather than approaching number theory as the memorization of formulas, this handout focuses on building intuition and familiarity for application in scenarios beyond expected.

It is suggested to review the theory for each section and then work on the practice problems. The examples are intentionally written in a teaching style so that the reasoning behind each step is visible.

Basic Definitions

Key Idea

For integers a and b with $b \neq 0$, we say:

$$b \mid a$$

if there exists an integer k such that:

$$a = bk.$$

In words, b divides a.

Translating a divisibility condition into an algebraic equation allows for manipulations and standard algebraic rules.

Common Mistake

Division and divisibility are not the same thing: do not get them confused! The expression $\frac{20}{7}$ exists as a real number, but $7 \nmid 20$ because $\frac{20}{7}$ is not an integer.

When a problem mentions divisibility or remainders, write it out as an equation or a congruence. Setting up equations early on prevents aimless guessing.

Core Divisibility Properties

Suppose a, b, c are integers.

Key Idea

Important properties:

$$a \mid b \text{ and } a \mid c \Rightarrow a \mid (b+c),$$
$$a \mid b \text{ and } a \mid c \Rightarrow a \mid (b-c),$$
$$a \mid b \Rightarrow a \mid bc,$$
$$a \mid b \text{ and } b \mid c \Rightarrow a \mid c.$$

Subtracting known multiples is a quick way to isolate needed variables. For example, if $7 \mid (a+b)$ and $7 \mid b$, then taking the difference yields $7 \mid a$

Linear Combination Principle

A stronger and very useful form is the following.

Key Idea

If:

$$c \mid a \qquad \text{and} \qquad c \mid b,$$

then:

$$c \mid (ax + by)$$

for all integers x and y.

Proof. Since $c \mid a$, there exists an integer m such that $a = cm$. Since $c \mid b$, there exists an integer n such that $b = cn$. Then:

$$ax + by = (cm)x + (cn)y = c(mx + ny).$$

Because $mx + ny$ is an integer, it follows that:

$$c \mid (ax + by).$$

Common Mistake

It is false in general that:

$$a \mid bc \Rightarrow a \mid b \text{ or } a \mid c.$$

For example:

$$6 \mid (2 \cdot 3),$$

but:

$$6 \nmid 2 \qquad \text{and} \qquad 6 \nmid 3.$$

This becomes valid under additional conditions, such as $\gcd(a, b) = 1$ and $a \mid bc$, in which case $a \mid c$.

Prime Numbers and Factorization

Key Idea

A prime number is an integer greater than 1 with exactly two positive divisors:

$$1 \text{ and itself.}$$

Examples of primes:

$$2, 3, 5, 7, 11, 13, 17.$$

Fundamental Property in Arithmetic

Key Idea

Every integer greater than 1 can be written uniquely as a product of prime powers.

Example:

$$360 = 2^3 \cdot 3^2 \cdot 5.$$

Prime factorization can be useful because divisibility questions become exponent comparisons. For example:

$$2^a 3^b 5^c \mid 2^x 3^y 5^z$$

exactly when:

$$a \leq x, \qquad b \leq y, \qquad c \leq z.$$

Example. Determine whether:

$$360 \mid 7200.$$

We factor:

$$360 = 2^3 \cdot 3^2 \cdot 5,$$

and:

$$7200 = 2^5 \cdot 3^2 \cdot 5^2.$$

Since every prime exponent in 7200 is at least as large as the corresponding exponent in 360, we conclude:

$$360 \mid 7200.$$

Legendre's Formula

Key Idea

For a prime p, the exponent of p in $n!$ is:

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Only finitely many terms are nonzero because of the floor function. Also note that the summation is summing the number of the multiples of each prime power. This is because each higher prime contributes one extra factor than previously counted.

Example. Find the exponent of 2 in 100!.

$$v_2(100!) = \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor.$$

Thus:

$$v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97.$$

Greatest Common Divisor and Least Common Multiple

Prime factorization is how integers are built. This leads to greatest common divisors and least common multiples.

Greatest Common Divisor

Key Idea

The greatest common divisor of integers a and b, denoted:

$$\gcd(a, b),$$

is the largest positive integer dividing both numbers.

Example:

$$\gcd(36, 48) = 12.$$

The GCD is fundamentally measured by the product of the lower power of shared primes that divide inspected integers.

Least Common Multiple

Key Idea

The least common multiple of integers a and b, denoted:

$$\operatorname{lcm}(a, b),$$

is the smallest positive integer divisible by both.

Example:

$$\operatorname{lcm}(12, 18) = 36.$$

The LCM measures the smallest number that contains both divisibility structures.

Important Identity

Key Idea

For positive integers a and b:

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

Example. Let:

$$a = 2^3 \cdot 3^2, \qquad b = 2 \cdot 3^5.$$

Then:

$$\gcd(a, b) = 2^1 \cdot 3^2,$$

and:

$$\operatorname{lcm}(a, b) = 2^3 \cdot 3^5.$$

Multiplying gives:

$$\gcd(a, b) \operatorname{lcm}(a, b) = 2^4 \cdot 3^7 = ab.$$

Euclidean Algorithm

The Euclidean Algorithm is one of the most powerful tools in elementary number theory.

Key Idea

$$\gcd(a, b) = \gcd(b, a - b).$$

More generally,

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Example

Find:

$$\gcd(252, 105).$$

$$\begin{aligned} 252 &= 2(105) + 42, \\ 105 &= 2(42) + 21, \\ 42 &= 2(21) + 0. \end{aligned}$$

Thus:

$$\gcd(252, 105) = 21.$$

Many students attempt to factor large numbers immediately. However, the Euclidean Algorithm avoids unnecessary computation and reveals patterns reliably.

Reversing the Euclidean Algorithm expresses the GCD as an integer linear combination of the original numbers. This idea leads to Bezout's identity:

$$\gcd(a, b) = ax + by$$

for some integers x and y.

When a problem involves $\gcd(a, b)$ and the expressions $a + b$, $a - b$, $ka + b$, or remainders, try applying the Euclidean Algorithm. It often reduces a complicated expression to a much smaller one.

Divisibility Tests

Standard divisibility rules stem from modular arithmetic in base 10.

Divisibility by 2

A number is divisible by 2 if its last digit is even. This works because powers of 10 beyond the units digit are divisible by 2.

Divisibility by 3

A number is divisible by 3 if the sum of its digits is divisible by 3.

Example:

$$813 \to 8 + 1 + 3 = 12.$$

Since 12 is divisible by 3, so is 813.

The reason is:

$$10 \equiv 1 \pmod 3,$$

so every power of 10 is also congruent to 1 modulo 3.

Divisibility by 9

A number is divisible by 9 if its digit sum is divisible by 9. This works because:

$$10 \equiv 1 \pmod 9.$$

Divisibility by 11

Take alternating sums of digits.

Example:

$$2728.$$

Compute:

$$(2 + 2) - (7 + 8) = -11.$$

Since -11 is divisible by 11, the number is divisible by 11.

This works because:

$$10 \equiv -1 \pmod{11}.$$

Thus the powers of 10 alternate between 1 and -1 modulo 11.

Modular Arithmetic

Key Idea

We write:

$$a \equiv b \pmod n$$

if:

$$n \mid (a - b).$$

Modular arithmetic simplifies calculations by making remainder tracking a more algebraic task. This keeps divisibility relationships in a more structured manner.

Examples

$$17 \equiv 2 \pmod 5$$

because:

$$17 - 2 = 15,$$

which is divisible by 5.

Similarly:

$$-1 \equiv 4 \pmod 5.$$

Key Operations

If:

$$a \equiv b \pmod n$$

and:

$$c \equiv d \pmod n,$$

then:

$$\begin{aligned} a + c &\equiv b + d \pmod n, \\ a - c &\equiv b - d \pmod n, \\ ac &\equiv bd \pmod n. \end{aligned}$$

These rules allow ordinary algebra to be performed with remainders.

Power Cycles

Powers often repeat modulo n. This is one of the main reasons modular arithmetic is so useful.

Example. Find:

$$2^{100} \pmod 7.$$

Since:

$$2^3 = 8 \equiv 1 \pmod 7,$$

we have:

$$2^{99} = (2^3)^{33} \equiv 1^{33} \equiv 1 \pmod 7.$$

Therefore:

$$2^{100} \equiv 2 \pmod 7.$$

Fermat's Little Theorem

Key Idea

If p is prime, then for any integer a:

$$a^p \equiv a \pmod p.$$

If additionally $\gcd(a, p) = 1$, then:

$$a^{p-1} \equiv 1 \pmod p.$$

Example. Compute:

$$3^{100} \pmod 7.$$

Since:

$$3^6 \equiv 1 \pmod 7,$$

and:

$$100 = 6(16) + 4,$$

we get:

$$3^{100} \equiv 3^4 = 81 \equiv 4 \pmod 7.$$

Euler's Totient Theorem

Key Idea

If:

$$\gcd(a, n) = 1,$$

then:

$$a^{\phi(n)} \equiv 1 \pmod n,$$

where $\phi(n)$ counts the positive integers less than or equal to n that are relatively prime to n.

Example. Since:

$$\phi(10) = 4,$$

and:

$$\gcd(3, 10) = 1,$$

we have:

$$3^4 \equiv 1 \pmod{10}.$$

Therefore:

$$3^{100} = (3^4)^{25} \equiv 1 \pmod{10}.$$

$$\gcd(a, n) = 1.$$

Classic Olympiad Techniques

Working Backwards

Instead of directly proving divisibility, manipulate expressions until familiar factors appear.

Example:

$$n^3 - n.$$

Factor:

$$n(n^2 - 1) = n(n - 1)(n + 1).$$

This is the product of three consecutive integers.

Among any three consecutive integers:

- one is divisible by 3,
- at least one is divisible by 2.

Thus:

$$6 \mid n(n-1)(n+1).$$

Therefore:

$$6 \mid (n^3 - n).$$

Pattern Recognition. Expressions like:

$$n^3 - n, \quad n^5 - n, \quad a^n - b^n$$

often suggest factorization. Before using modular arithmetic or checking cases, always ask whether the expression has a standard algebraic factorization.

Bounding and Contradiction

Bounding involves placing quantities within upper or lower limits, while contradiction proves a statement by assuming the opposite and deriving an impossibility.

In olympiad number theory, bounding and contradiction are especially useful when integer restrictions are present. A real-valued quantity may lie in an interval, but an integer cannot lie between two consecutive integers. This simple idea is often decisive.

1. Definitions

Definition 9.1 (Upper Bound)**.** *A number M is an **upper bound** for a quantity x if:*

$$x \leq M.$$

Definition 9.2 (Lower Bound)**.** *A number m is a **lower bound** for a quantity x if:*

$$x \geq m.$$

Definition 9.3 (Proof by Contradiction)**.** *To prove a statement P, assume that P is false and show that this assumption leads to a contradiction.*

2. Common Bounding Ideas

- Compare expressions with known inequalities:

$$a^2 + b^2 \geq 2ab.$$

- Use extremal values, such as the largest or smallest element.
- Count the same object in two different ways.
- Replace complicated expressions with simpler upper or lower estimates.
- Use integer constraints: if an integer satisfies

$$3 < n < 4,$$

then no such integer exists.

Olympiad Insight. Bounding becomes especially strong when combined with equality conditions. If an inequality forces equality, then the equality case often reveals the only possible solution.

3. Example: Bounding

Problem 9.1. *Show that for positive real numbers a, b:*

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Solution. Since:

$$(a-b)^2 \geq 0,$$

we expand:

$$a^2 - 2ab + b^2 \geq 0.$$

Adding $4ab$ gives:

$$a^2 + 2ab + b^2 \geq 4ab.$$

Thus:

$$(a+b)^2 \geq 4ab.$$

Because $a, b > 0$, both sides are nonnegative, so taking square roots gives:

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Equality occurs exactly when:

$$a = b.$$

□

4. Example: Contradiction

Problem 9.2. *Prove that $\sqrt{2}$ is irrational.*

Solution. Assume for contradiction that:

$$\sqrt{2} = \frac{a}{b}$$

for integers a, b with $\gcd(a, b) = 1$.

Squaring:

$$2 = \frac{a^2}{b^2},$$

so:

$$a^2 = 2b^2.$$

Thus a^2 is even, implying a is even. Write:

$$a = 2k.$$

Substituting:

$$(2k)^2 = 2b^2,$$

which gives:

$$4k^2 = 2b^2,$$

and therefore:

$$b^2 = 2k^2.$$

Hence b is also even.

But then both a and b are divisible by 2, contradicting:

$$\gcd(a, b) = 1.$$

Therefore $\sqrt{2}$ is irrational. □

5. Olympiad Problems

Problem 9.3. *Let x, y, z be positive integers satisfying:*

$$x + y + z = 10.$$

Find the maximum possible value of:

$$xyz.$$

Solution. By AM-GM:

$$\frac{x + y + z}{3} \geq \sqrt[3]{xyz}.$$

Thus:

$$\frac{10}{3} \geq \sqrt[3]{xyz}.$$

Cubing:

$$xyz \leq \left(\frac{10}{3}\right)^3 \approx 37.03.$$

Since xyz is an integer:

$$xyz \leq 37.$$

Now check triples closest to equality in AM-GM. Equality would occur near:

$$x = y = z = \frac{10}{3}.$$

The closest positive integer triple is:

$$3, 3, 4,$$

which gives:

$$xyz = 36.$$

Hence the maximum value is:

$$\boxed{36}.$$

□

Problem 9.4. *Prove that there do not exist positive integers $a > 1, b > 1$ such that:*

$$a^2 - b^2 = 1$$

Solution. Factor:

$$a^2 - b^2 = (a-b)(a+b) = 1.$$

Since $a, b > 1$, both factors are positive integers.

The only way to positively factor 1 is:

$$1 \cdot 1.$$

Thus:

$$a - b = 1, \qquad a + b = 1.$$

Adding:

$$2a = 2,$$

so:

$$a = 1,$$

contradicting $a > 1$.

Therefore no such integers exist. □

6. Practice Problems

1. Prove that among any $n+1$ integers, two have the same remainder modulo n.
2. Show that if:

   $$a + b + c = 1,$$

   then:

   $$a^2 + b^2 + c^2 \geq \frac{1}{3}.$$

3. Prove that there is no rational number whose square is 3.
4. Let x, y be positive reals with:

   $$xy = 1.$$

   Find the minimum value of:

   $$x + y.$$

5. Prove that in any group of six people, either three mutually know each other or three mutually do not know each other.

Worked Example Problems

Example

Problem 1.
Prove that for every integer n:

$$5 \mid (n^5 - n).$$

Solution.
Factor:

$$n^5 - n = n(n^4 - 1).$$

Continue:

$$= n(n^2 - 1)(n^2 + 1).$$

Then:

$$= n(n-1)(n+1)(n^2+1).$$

This factorization is useful, but it does not immediately show divisibility by 5 for every case. A cleaner method uses modular arithmetic.

Any integer is congruent to one of:

$$0, 1, 2, 3, 4 \pmod 5.$$

Checking each case:

$$0^5 \equiv 0, \quad 1^5 \equiv 1, \quad 2^5 = 32 \equiv 2, \quad 3^5 = 243 \equiv 3, \quad 4^5 \equiv 4 \pmod 5.$$

Thus:

$$n^5 \equiv n \pmod 5.$$

Therefore:

$$n^5 - n \equiv 0 \pmod 5,$$

so:

$$5 \mid (n^5 - n).$$

Key Observation. This is a special case of Fermat's Little Theorem:

$$n^5 \equiv n \pmod 5.$$

Example

Problem 2.
Find all integers n such that:

$$12 \mid n^2 - 4.$$

Solution.

Factor:

$$n^2 - 4 = (n-2)(n+2).$$

We require divisibility by:

$$12 = 3 \cdot 4.$$

It is often easier to analyze divisibility by 3 and by 4 separately.

Modulo 3:

$$n^2 - 4 \equiv n^2 - 1 \pmod 3.$$

Thus:

$$n^2 \equiv 1 \pmod 3,$$

so:

$$n \not\equiv 0 \pmod 3.$$

Modulo 4:

$$n^2 - 4 \equiv n^2 \pmod 4.$$

Thus:

$$n^2 \equiv 0 \pmod 4,$$

which means:

$$n \equiv 0 \text{ or } 2 \pmod 4.$$

Combining these conditions modulo 12, we get:

$$n \equiv 2, 4, 8, 10 \pmod{12}.$$

Key Takeaway: Rather than evaluating modulo 12 directly, factor $n^2 - 4 = (n-2)(n+2)$ and split 12 into its coprime factors 3 and 4. Solving smaller congruences independently and combining their conditions is consistently faster than brute-forcing composite moduli.

Factorizations

Difference of Squares

$$a^2 - b^2 = (a-b)(a+b).$$

This identity is especially useful when two squares differ by a small number.

Difference of Cubes

$$a^3 - b^3 = (a-b)(a^2+ab+b^2).$$

Sum of Cubes

$$a^3 + b^3 = (a+b)(a^2-ab+b^2).$$

Sophie Germain Identity

Key Idea

$$a^4 + 4b^4 = (a^2 - 2ab + 2b^2)(a^2 + 2ab + 2b^2).$$

For example:

$$x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Recognizing these instantly saves enormous amounts of time in contests.

Chinese Remainder Theorem

If congruences involve coprime moduli, they can often be combined into a single congruence.

Key Idea

If $\gcd(m, n) = 1$, then a system:

$$x \equiv a \pmod m, \qquad x \equiv b \pmod n$$

has a unique solution modulo mn.

Example. Solve:

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5.$$

Checking numbers congruent to 2 modulo 3:

$$2, 5, 8, 11, 14, \ldots$$

The number 8 satisfies:

$$8 \equiv 3 \pmod 5.$$

Thus:

$$x \equiv 8 \pmod{15}.$$

Problem Set

Introductory Problems

1. Prove that:
$$3 \mid (n^3 - n)$$
for every integer n.
2. Find:
$$\gcd(144, 252).$$
3. Determine whether:
$$11 \mid 918273.$$
4. Prove that the product of two consecutive integers is always even.
5. Show that if:
$$a \mid b$$
and:
$$a \mid c,$$
then:
$$a \mid (5b - 2c).$$

Intermediate Problems

6. Prove that:
$$30 \mid (n^5 - n)$$
for every integer n.
7. Find all integers satisfying:
$$7 \mid n^2 + 3.$$
8. Prove:
$$\gcd(a + b, a - b) \mid 2a.$$
9. Show that among any $n + 1$ integers, two have the same remainder modulo n.
10. Determine all integers n such that:
$$n \mid (n + 5)(n + 7).$$
11. Prove that the only even prime number is 2.

Advanced Problems

11. Prove that if:
$$2^n - 1$$
is prime, then n is prime.

12. Show that:
$$\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m,n)} - 1.$$

13. Prove that there are infinitely many integers not representable as:
$$a^2 + b^2.$$

14. Let:
$$a + b + c = 0.$$
Prove that:
$$a^3 + b^3 + c^3$$
is divisible by:
$$3abc.$$

15. Find all positive integers n such that:
$$n^2 + 2 \mid n!.$$

Problem-Solving Guidance

Focus on divisibility arguments through GCD and modular arithmetic for beginner problems. Intermediate problems will often use a combination. For example, proving:

$$30 \mid n^5 - n$$

requires divisibility by 2, 3, and 5. This shows a combination between modular arithmetic and factorizations.

Olympiad Problem-Solving Stratgies

When problems get difficult, try to apply techniques and starting steps through the following: factorizations, modular arithmetic, prime exponents, and GCD/LCM analysis.

Common Mistake

Many olympiad students lose points not because the problem is impossible, but because they abandon structure too early and begin brute forcing calculations.

Answers to Problem Set

1. Proof
2. 36
3. Does not divide.
4. One is even; therefore, their product is even.
5. $a \mid (5b - 2c)$
6. Proof
7. $n \equiv 2, 5 \pmod 7$
8. $\gcd(a + b, a - b) \mid 2a$
9. Pigeonhole Principle
10. $n \in \{\pm 1, \pm 5, \pm 7, \pm 35\}$
11. Proof
12. n is prime
13. $2^{\gcd(m,n)} - 1$
14. Proof
15. $n = 14, 22, 25, 32, 41, 44, 52, 58, 59, \ldots$

Closing Thoughts

Mastery in contest number theory comes from recognizing what tool to use, whether it is bounding, modular arithmetic, factor-analysis, etc. Work through the problem set, and analyze where specific strategies work or fail.

Resources and References

(a) Art of Problem Solving - `https://artofproblemsolving.com/?srsltid=AfmBOopV5ZIDR_i1thFxW75wFTQC3mt-NVH7PEoFs4xxWrjtubG1UMeF`

(b) HMMT Problem Sets - `https://www.hmmt.org/www/archive/problems`

(c) David Altizio's Web Page - `https://davidaltizio.web.illinois.edu/mathlinks.html`

(d) Yufei Zhao's Notes - `https://yufeizhao.com/olympiad/`

(e) Sohil Rathi - `https://www.youtube.com/c/SohilRathi`