Prime Numbers and Factorization

Advanced Techniques in Olympiad Number Theory

Aryan Ayyanger

Contents

Introduction

Prime numbers are the building blocks of arithmetic. In a first number theory handout, divisibility, greatest common divisors, modular arithmetic, and standard olympiad tools introduce the language of integers. This second handout goes deeper into the prime structure behind those ideas.

The focus here is not to repeat basic divisibility rules. Instead, this guide studies how primes behave inside products, factorials, binomial coefficients, exponential expressions, and olympiad-style equations. Many difficult number theory problems become clearer once the prime factorization of the expression is understood.

A strong contestant learns to ask:

- Which primes control this expression?
- How many times does a prime divide this number?
- Can the problem be reduced to comparing prime exponents?
- Is a factorial hiding more powers of a prime than expected?
- Does the expression have a factorization such as $a^n - b^n$?
- Can Lifting the Exponent simplify a difficult valuation?
- Is a repeated power cycle controlled by a multiplicative order?

This handout is intended as a continuation of foundational number theory. The style remains olympiad-focused: definitions are included, but the emphasis is on recognizing patterns, proving statements, and solving contest problems.

Key Idea

Advanced number theory often begins with a simple question:

How many times does a prime divide this expression?

Prime Numbers as Arithmetic Atoms

A prime number is an integer greater than 1 that has exactly two positive divisors: 1 and itself. Prime numbers are special because they cannot be broken into smaller positive integer factors.

The first few primes are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

Composite numbers are built from primes. For example:

$$84 = 2^2 \cdot 3 \cdot 7.$$

The reason primes are so important is not just that they are smaller pieces. It is that the prime decomposition of an integer is unique.

Why Primes Matter in Olympiad Problems

Many olympiad number theory problems look different on the surface:

- factorial divisibility,
- binomial coefficient divisibility,
- exponential expressions,
- equations involving powers,
- prime-generating expressions,
- integer solutions to equations.

But beneath the surface, these problems often ask about prime exponents.

Example. To decide whether:

$$72 \mid 10!$$

we do not need to compute 10!. Instead:

$$72 = 2^3 \cdot 3^2.$$

Now:

$$10! = 1 \cdot 2 \cdot 3 \cdots 10.$$

There are clearly at least three factors of 2 and at least two factors of 3 in 10!, so:

$$72 \mid 10!.$$

Olympiad Insight. When a problem involves a large product, factorial, or power, do not expand it. Track the primes inside it.

Euclid's Proof of Infinitely Many Primes

One of the most famous proofs in number theory is Euclid's proof that there are infinitely many primes.

Key Idea

There are infinitely many prime numbers.

Proof. Assume for contradiction that there are only finitely many primes:

$$p_1, p_2, \ldots, p_n.$$

Now form the number:

$$N = p_1 p_2 \cdots p_n + 1.$$

When N is divided by any prime p_i, the remainder is 1. Therefore none of the primes:

$$p_1, p_2, \ldots, p_n$$

divides N.

But every integer greater than 1 has some prime divisor. Thus N must have a prime divisor not on the original list. This contradicts the assumption that the list contained all primes.

Therefore there are infinitely many primes. □

Why This Proof Matters. This proof is not only historical. It introduces a common olympiad strategy:

construct a number that avoids all known prime divisors.

A Related Example

Example

Show that there are infinitely many primes of the form not dividing a given finite product.

Solution. Let S be any finite set of primes. Multiply all primes in S and add 1:

$$N = \prod_{p \in S} p + 1.$$

No prime in S divides N. Therefore any prime divisor of N is outside S.

This shows that no finite set of primes can capture all prime divisors that appear in the integers.

□

The Fundamental Theorem Revisited

The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be written uniquely as a product of prime powers.

This was introduced in foundational number theory, but here we focus on why it matters in olympiad settings.

Key Idea

Every integer $n > 1$ has a unique representation:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where the p_i are distinct primes and the a_i are positive integers.

Existence

Every composite number can be broken into smaller factors. If those factors are composite, break them again. This process eventually stops because positive integers decrease. The final factors must be prime.

Uniqueness

Uniqueness is deeper. It relies on the fact that if a prime divides a product, then it divides at least one factor.

Key Idea

If p is prime and:

$$p \mid ab,$$

then:

$$p \mid a \quad \text{or} \quad p \mid b.$$

This property is false for composite numbers. For instance:

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

but:

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

Olympiad Insight. Prime numbers are powerful because they cannot split their divisibility across unrelated factors. A prime divisor of a product must enter through one factor.

Prime Exponents and Valuation

A central tool in advanced olympiad number theory is valuation.

Definition 5.1. *For a prime p and a positive integer n, the notation:*

$$v_p(n)$$

means the exponent of p in the prime factorization of n.

For example:

$$48 = 2^4 \cdot 3,$$

so:

$$v_2(48) = 4, \qquad v_3(48) = 1, \qquad v_5(48) = 0.$$

Basic Properties

Key Idea

For positive integers a, b and prime p:

$$v_p(ab) = v_p(a) + v_p(b).$$

$$v_p(a^k) = k\, v_p(a).$$

If $b \mid a$, then:

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

These rules turn multiplication into addition.

Example

Example

Find $v_3(5400)$.

Solution. Factor:

$$5400 = 54 \cdot 100 = (2 \cdot 3^3)(2^2 \cdot 5^2).$$

Thus:

$$5400 = 2^3 \cdot 3^3 \cdot 5^2.$$

So:

$$v_3(5400) = 3.$$

□

Valuation and Divisibility

The condition:

$$a \mid b$$

is equivalent to:

$$v_p(a) \leq v_p(b)$$

for every prime p.

Example

Determine whether:

$$2^5 \cdot 3^2 \cdot 7 \mid 2^7 \cdot 3 \cdot 5 \cdot 7^2.$$

Solution. Compare exponents prime by prime.

For 2:

$$5 \leq 7.$$

For 3:

$$2 \leq 1$$

is false.

Therefore the divisibility does not hold. □

Valuations of GCD and LCM

Although GCD and LCM were introduced earlier, valuations give a more systematic viewpoint.

Key Idea

For positive integers a, b:

$$v_p(\gcd(a,b)) = \min(v_p(a), v_p(b)),$$

and:

$$v_p(\operatorname{lcm}(a,b)) = \max(v_p(a), v_p(b)).$$

Example

Let:

$$a = 2^4 \cdot 3^2 \cdot 5,$$

and:

$$b = 2^2 \cdot 3^5 \cdot 7.$$

Then:

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

and:

$$\operatorname{lcm}(a, b) = 2^4 \cdot 3^5 \cdot 5 \cdot 7.$$

Olympiad Insight. When GCD and LCM expressions become complicated, rewrite everything in terms of prime exponents. The problem often becomes a comparison of minimums and maximums.

Legendre's Formula in Depth

Factorials contain many prime factors. Legendre's Formula counts them efficiently.

Key Idea

For prime p:

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

Only finitely many terms are nonzero.

Why It Works

The product:

$$n! = 1 \cdot 2 \cdot 3 \cdots n$$

contains a factor of p from every multiple of p.

There are:

$$\left\lfloor \frac{n}{p} \right\rfloor$$

multiples of p.

But multiples of p^2 contain an extra factor of p, so they must be counted again.

There are:

$$\left\lfloor \frac{n}{p^2} \right\rfloor$$

multiples of p^2.

Similarly, multiples of p^3 contribute yet another factor of p, and so on.

Example: Power of 2 in 100!

Example

Find:

$$v_2(100!).$$

Solution. By Legendre's Formula:

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

Thus:

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

□

Example: Power of 5 in 1000!

Example

Find:

$$v_5(1000!).$$

Solution.

$$v_5(1000!) = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor.$$

So:

$$v_5(1000!) = 200 + 40 + 8 + 1 = 249.$$

□

Trailing Zeros and Factorials

A trailing zero comes from a factor of 10.

Since:

$$10 = 2 \cdot 5,$$

the number of trailing zeros in a positive integer is:

$$\min(v_2(n), v_5(n)).$$

For factorials, there are usually many more factors of 2 than factors of 5. Therefore the number of trailing zeros in $n!$ is usually:

$$v_5(n!).$$

Example

Example

How many trailing zeros does 100! have?

Solution. The number of trailing zeros is:

$$v_5(100!).$$

Using Legendre's Formula:

$$v_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 20 + 4 = 24.$$

Thus 100! has:

$$24$$

trailing zeros. □

Finding the Smallest Factorial with Many Zeros

Example

Find the smallest positive integer n such that $n!$ has at least 30 trailing zeros.

Solution. We need:

$$v_5(n!) \geq 30.$$

Try $n = 125$:

$$v_5(125!) = 25 + 5 + 1 = 31.$$

Try smaller near 120:

$$v_5(120!) = 24 + 4 = 28.$$

Try 125 is the first multiple giving the extra contribution from 125.
Check:

$$v_5(124!) = 24 + 4 = 28.$$

Thus the smallest n is:

$$125.$$

□

Common Mistake

A multiple of 25 contributes two factors of 5, and a multiple of 125 contributes three. Do not count only multiples of 5.

Factorials and Divisibility

Legendre's Formula helps determine whether one number divides a factorial.

Example

Determine whether:

$$2^{10}3^4 5^2 \mid 50!.$$

Solution. Compute the needed prime exponents in 50!.

$$v_2(50!) = 25 + 12 + 6 + 3 + 1 = 47.$$

$$v_3(50!) = 16 + 5 + 1 = 22.$$

$$v_5(50!) = 10 + 2 = 12.$$

Since:

$$47 \geq 10, \qquad 22 \geq 4, \qquad 12 \geq 2,$$

the divisibility holds. □

Highest Power Dividing a Factorial

Example

Find the largest integer k such that:

$$12^k \mid 100!.$$

Solution. First factor:

$$12 = 2^2 \cdot 3.$$

We need:

$$(2^2 \cdot 3)^k = 2^{2k}3^k$$

to divide 100!.

Now:

$$v_2(100!) = 97.$$

$$v_3(100!) = 33 + 11 + 3 + 1 = 48.$$

The conditions are:

$$2k \leq 97$$

and:

$$k \leq 48.$$

Thus:

$$k \leq 48$$

from the second condition, and:

$$k \leq 48$$

from the first since $\lfloor 97/2 \rfloor = 48$.

Therefore:

$$k = 48.$$

□

Binomial Coefficients and Prime Powers

Binomial coefficients often contain hidden prime divisibility.

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

Valuations allow us to compute prime exponents in binomial coefficients:

Key Idea

$$v_p\left(\binom{n}{k}\right) = v_p(n!) - v_p(k!) - v_p((n-k)!).$$

Example

Example

Find:

$$v_2\left(\binom{100}{50}\right).$$

Solution.

$$v_2\left(\binom{100}{50}\right) = v_2(100!) - 2v_2(50!).$$

We already know:

$$v_2(100!) = 97.$$

Also:

$$v_2(50!) = 25 + 12 + 6 + 3 + 1 = 47.$$

Thus:

$$v_2\left(\binom{100}{50}\right) = 97 - 2(47) = 3.$$

□

Kummer's Theorem

Kummer's Theorem gives a beautiful interpretation of prime powers in binomial coefficients.

Key Idea

The exponent of a prime p in:

$$\binom{n}{k}$$

equals the number of carries that occur when adding k and $n-k$ in base p.

This theorem is especially useful for parity and divisibility questions.

Parity of Binomial Coefficients

A binomial coefficient:

$$\binom{n}{k}$$

is odd exactly when there are no carries in adding k and $n-k$ in base 2.

Olympiad Insight. Pascal's Triangle contains many hidden divisibility patterns. Looking at binomial coefficients modulo primes reveals deep structure.

Advanced Factorization Techniques

Many olympiad problems become easy once the correct factorization is recognized.

Difference of Powers

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

This shows:

$$a - b \mid a^n - b^n.$$

Sum of Odd Powers

If n is odd:

$$a^n + b^n$$

is divisible by:

$$a + b.$$

For example:

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

Difference of Squares

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

Sophie Germain Identity

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

This identity is especially useful because expressions of the form:

$$x^4 + 4$$

often look prime at first glance but secretly factor.

Example

Example

Factor:

$$x^4 + 4.$$

Solution. Use Sophie Germain with $a = x$ and $b = 1$:

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

□

Cyclotomic Flavor

A full treatment of cyclotomic polynomials is beyond this handout, but some basic patterns are useful.

$$a^n - b^n$$

has factors corresponding to divisors of n.

For example:

$$a^6 - b^6 = (a^3 - b^3)(a^3 + b^3).$$

Also:

$$a^6 - b^6 = (a - b)(a + b)(a^2 + ab + b^2)(a^2 - ab + b^2).$$

Olympiad Insight. When an exponent is composite, try factoring using its divisors.

Mersenne Numbers

Numbers of the form:

$$2^n - 1$$

are called Mersenne numbers.

Key Idea

If $2^n - 1$ is prime, then n must be prime.

Proof. Suppose n is composite, so:

$$n = ab$$

with $a, b > 1$.

Then:

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1.$$

Since:

$$x^b - 1$$

is divisible by:

$$x - 1,$$

we get:

$$2^a - 1 \mid 2^{ab} - 1.$$

Thus $2^n - 1$ is composite.

Therefore, if $2^n - 1$ is prime, n must be prime. □

Common Mistake

The converse is false. If n is prime, $2^n - 1$ does not have to be prime. For example:

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

Fermat Numbers

Numbers of the form:

$$F_n = 2^{2^n} + 1$$

are called Fermat numbers.

The first few are:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

These are prime, but not all Fermat numbers are prime.

Example. Euler proved that:

$$F_5 = 2^{32} + 1$$

is composite.

A Useful Identity

Fermat numbers satisfy:

$$F_0 F_1 \cdots F_{n-1} = F_n - 2.$$

This identity gives another proof that infinitely many primes exist, since Fermat numbers are pairwise coprime.

Multiplicative Order

The multiplicative order of a modulo n is the smallest positive integer k such that:

$$a^k \equiv 1 \pmod{n}.$$

This is defined when:

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

Definition 16.1. *If* $\gcd(a, n) = 1$*, then the order of* a *modulo* n*, denoted* $\mathrm{ord}_n(a)$*, is the smallest positive integer* k *satisfying:*

$$a^k \equiv 1 \pmod{n}.$$

Example

Example

Find the order of 2 modulo 7.

Solution. Compute:

$$2^1 \equiv 2 \pmod{7},$$
$$2^2 \equiv 4 \pmod{7},$$
$$2^3 \equiv 8 \equiv 1 \pmod{7}.$$

Thus:

$$\mathrm{ord}_7(2) = 3.$$

□

Order Divides Phi

Key Idea

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

$$\mathrm{ord}_n(a) \mid \phi(n).$$

In particular, if p is prime:

$$\mathrm{ord}_p(a) \mid p - 1.$$

Olympiad Insight. When solving exponential congruences, orders are often more precise than simply applying Fermat's Little Theorem.

Repeating Decimals and Orders

Repeating decimals are connected to multiplicative order.

For example:

$$\frac{1}{7} = 0.\overline{142857}.$$

The repeating block has length 6 because:

$$10^6 \equiv 1 \pmod 7$$

and no smaller positive exponent works.

Thus:

$$\operatorname{ord}_7(10) = 6.$$

Example

Example

Find the length of the repeating decimal of $\frac{1}{13}$.

Solution. We need the smallest k such that:

$$10^k \equiv 1 \pmod{13}.$$

Compute:

$$10^1 \equiv 10,$$
$$10^2 \equiv 100 \equiv 9,$$
$$10^3 \equiv 90 \equiv 12,$$
$$10^4 \equiv 120 \equiv 3,$$
$$10^5 \equiv 30 \equiv 4,$$
$$10^6 \equiv 40 \equiv 1 \pmod{13}.$$

Therefore the repeating block length is:

$$6.$$

□

Lifting the Exponent

Lifting the Exponent, often abbreviated LTE, is an advanced olympiad technique for computing valuations of expressions like:

$$a^n - b^n.$$

Key Idea

A common LTE form:
If p is an odd prime, $p \mid a - b$, and $p \nmid ab$, then:

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

This theorem is powerful because it converts a difficult exponential valuation into two smaller valuations.

Example

Example

Find:

$$v_3(10^{12} - 1).$$

Solution. We write:

$$10^{12} - 1 = 10^{12} - 1^{12}.$$

Since:

$$3 \mid 10 - 1,$$

and:

$$3 \nmid 10,$$

LTE gives:

$$v_3(10^{12} - 1) = v_3(10 - 1) + v_3(12).$$

Now:

$$v_3(9) = 2$$

and:

$$v_3(12) = 1.$$

Therefore:

$$v_3(10^{12} - 1) = 3.$$

□

Another Example

Example

Find:

$$v_5(6^{50} - 1).$$

Solution. Since:

$$5 \mid 6 - 1,$$

LTE gives:

$$v_5(6^{50} - 1) = v_5(6 - 1) + v_5(50).$$

Thus:

$$v_5(6^{50} - 1) = v_5(5) + v_5(50) = 1 + 2 = 3.$$

□

The Special Case for 2

LTE has special forms for $p = 2$.

One common version is:

Key Idea

If a and b are odd and n is even, then:

$$v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1.$$

Example

Find:

$$v_2(3^{20} - 1).$$

Solution. Use the special LTE form with:

$$a = 3, \quad b = 1, \quad n = 20.$$

Then:

$$v_2(3^{20} - 1) = v_2(3 - 1) + v_2(3 + 1) + v_2(20) - 1.$$

Compute:

$$v_2(2) = 1, \quad v_2(4) = 2, \quad v_2(20) = 2.$$

Therefore:

$$v_2(3^{20} - 1) = 1 + 2 + 2 - 1 = 4.$$

□

Common Mistake

LTE has hypotheses. Before applying it, check divisibility conditions and whether the prime is odd or equal to 2.

Prime Exponents in Products

Valuations are not only for factorials and powers. They also help with products.

Example

Find the largest power of 2 dividing:

$$1 \cdot 2 \cdot 3 \cdots 64.$$

Solution. The expression is:

$$64!.$$

Using Legendre's Formula:

$$v_2(64!) = 32 + 16 + 8 + 4 + 2 + 1 = 63.$$

Therefore the largest power of 2 dividing the product is:

$$2^{63}.$$

□

Product of Consecutive Integers

The product:

$$n(n+1)(n+2)\cdots(n+k-1)$$

always has strong divisibility properties because it contains k consecutive integers.

For example, the product of any k consecutive integers is divisible by:

$$k!.$$

Key Idea

The product of k consecutive integers is divisible by $k!$.

This can be seen from binomial coefficients:

$$\binom{n+k-1}{k} = \frac{n(n+1)\cdots(n+k-1)}{k!}.$$

Since binomial coefficients are integers, the numerator is divisible by $k!$.

Prime Counting and the Sieve of Eratosthenes

The Sieve of Eratosthenes is an ancient method for finding primes.

To find all primes up to N:

1. List all integers from 2 to N.
2. Circle the smallest uncrossed number.
3. Cross out all of its multiples.
4. Repeat until all composite numbers are crossed out.

Why It Works

Every composite number has a prime factor less than or equal to its square root.

Key Idea

If n is composite, then n has a prime divisor p satisfying:

$$p \leq \sqrt{n}.$$

Proof. If:

$$n = ab$$

with $1 < a \leq b < n$, then:

$$a^2 \leq ab = n.$$

Thus:

$$a \leq \sqrt{n}.$$

The number a has a prime divisor $p \leq a$, so:

$$p \leq \sqrt{n}.$$

□

Testing Primality

To test whether n is prime, it is enough to check divisibility by primes up to:

$$\sqrt{n}.$$

Example

Determine whether 221 is prime.

Solution. Since:

$$\sqrt{221} < 15,$$

we only need to test primes:

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

It is not divisible by $2, 3$, or 5.
Check:

$$221 = 13 \cdot 17.$$

Therefore 221 is composite. □

Prime Gaps and Patterns

Primes do not appear regularly, but some patterns are useful.
Except for 2, all primes are odd.
Except for 2 and 3, every prime is congruent to:

$$1 \quad \text{or} \quad 5 \pmod 6.$$

Why?
Every integer is congruent to:

$$0, 1, 2, 3, 4, 5 \pmod 6.$$

Numbers congruent to $0, 2, 4$ are even.
Numbers congruent to 3 are divisible by 3.

So primes greater than 3 must be:

$$1 \quad \text{or} \quad 5 \pmod 6.$$

Common Mistake

The condition $n \equiv 1$ or $5 \pmod 6$ is necessary for primes greater than 3, but it is not sufficient. For example, $25 \equiv 1 \pmod 6$ but is not prime.

Advanced Worked Examples

Example

Find the largest integer k such that:

$$18^k \mid 100!.$$

Solution. Factor:

$$18 = 2 \cdot 3^2.$$

So:

$$18^k = 2^k 3^{2k}.$$

We need:

$$k \leq v_2(100!)$$

and:

$$2k \leq v_3(100!).$$

Compute:

$$v_2(100!) = 97.$$

Also:

$$v_3(100!) = 33 + 11 + 3 + 1 = 48.$$

Thus:

$$2k \leq 48,$$

so:

$$k \leq 24.$$

Therefore:

$$k = 24.$$

□

Example

Find the highest power of 5 dividing:

$$\binom{100}{25}.$$

Solution. We compute:

$$v_5\left(\binom{100}{25}\right) = v_5(100!) - v_5(25!) - v_5(75!).$$

Now:

$$v_5(100!) = 20 + 4 = 24.$$

$$v_5(25!) = 5 + 1 = 6.$$

$$v_5(75!) = 15 + 3 = 18.$$

Therefore:

$$v_5\left(\binom{100}{25}\right) = 24 - 6 - 18 = 0.$$

So 5 does not divide:

$$\binom{100}{25}.$$

□

Example

Prove that if $a^2 \mid b^3$ and $b^3 \mid a^4$, then $a \mid b^2$.

Solution. Let p be any prime.

From:

$$a^2 \mid b^3,$$

we get:

$$2v_p(a) \leq 3v_p(b).$$

From:

$$b^3 \mid a^4,$$

we get:

$$3v_p(b) \leq 4v_p(a).$$

We want to prove:

$$a \mid b^2,$$

which is equivalent to:

$$v_p(a) \leq 2v_p(b)$$

for every prime p.

But this follows immediately from:

$$2v_p(a) \leq 3v_p(b),$$

since:

$$v_p(a) \leq \frac{3}{2}v_p(b) \leq 2v_p(b).$$

Therefore:

$$a \mid b^2.$$

□

Example

Show that:

$$7 \mid 2^{3n} - 1$$

for every positive integer n.

Solution. Since:

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

we get:

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

Thus:

$$2^{3n} - 1 \equiv 0 \pmod 7,$$

so:

$$7 \mid 2^{3n} - 1.$$

□

Common Patterns

Pattern 1: Factorials

If the problem contains:

$$n!,$$

think about Legendre's Formula and prime exponents.

Pattern 2: Binomial Coefficients

If the problem contains:

$$\binom{n}{k},$$

think about:

$$v_p(n!) - v_p(k!) - v_p((n-k)!).$$

Pattern 3: Difference of Powers

If the problem contains:

$$a^n - b^n,$$

think about:

$$a - b \mid a^n - b^n$$

and possibly LTE.

Pattern 4: Mersenne Expressions

If the problem contains:

$$2^n - 1,$$

check whether n is composite.

Pattern 5: Repeating Powers

If powers repeat modulo m, think about multiplicative order.

Problem Set

Introductory Problems

1. Prove that there are infinitely many primes.
2. Find the prime factorization of 2520.
3. Compute $v_2(1440)$.
4. Compute $v_3(3^7 \cdot 5^2 \cdot 11)$.
5. Determine whether $2^4 \cdot 3^2 \mid 20!$.
6. Find $v_5(200!)$.
7. Find the number of trailing zeros in 150!.
8. Determine whether 13 is prime.
9. Determine whether 391 is prime.
10. Prove that every composite number n has a prime divisor at most $\sqrt{n}$.

Intermediate Problems

11. Find the largest k such that:
$$8^k \mid 100!.$$
12. Find the largest k such that:
$$45^k \mid 200!.$$
13. Compute:
$$v_2\left(\binom{50}{25}\right).$$
14. Compute:
$$v_3\left(\binom{90}{30}\right).$$
15. Prove that:
$$2^n - 1$$
is composite whenever n is composite.

16. Factor:
$$x^6 - y^6.$$

17. Use Sophie Germain's identity to factor:
$$x^4 + 4y^4.$$

18. Find:
$$v_3(10^{18} - 1).$$

19. Find:
$$v_5(11^{25} - 1).$$

20. Find the order of 3 modulo 7.

Advanced Problems

21. Prove that:
$$F_0F_1 \cdots F_{n-1} = F_n - 2$$
for Fermat numbers $F_n = 2^{2^n} + 1$.

22. Prove that Fermat numbers are pairwise coprime.

23. Find the length of the repeating decimal of:
$$\frac{1}{17}.$$

24. Determine all primes p such that:
$$p \mid 2^p - 2.$$

25. Prove that:
$$\text{ord}_p(a) \mid p - 1$$
for prime p and $\gcd(a, p) = 1$.

26. Compute:
$$v_2(5^{32} - 1).$$

27. Compute:
$$v_7(8^{49} - 1).$$

28. Show that:
$$\binom{2p}{p}$$
is divisible by 2 but not by p^2 for prime $p > 2$.

29. Prove that the product of k consecutive integers is divisible by $k!$.

30. Find the largest power of 12 dividing:
$$\frac{100!}{50!}.$$

31. Prove that if p is prime and $p \mid a^2$, then $p \mid a$.

32. Show that if ab is a perfect square and $\gcd(a, b) = 1$, then both a and b are perfect squares.

33. Find all positive integers n such that:
$$n! + 1$$
is prime for small n, and explain why this question becomes difficult.

34. Prove that if p is an odd prime and $p \mid a - b$, then:
$$p \mid a^n - b^n.$$

35. Create and solve your own valuation problem involving a factorial and a binomial coefficient.

Problem-Solving Guidance

For introductory problems, focus on definitions, prime factorization, and direct use of Legendre's Formula.

For intermediate problems, expect to combine valuations with factorials, binomial coefficients, and factorization.

For advanced problems, the main challenge is often recognizing which tool applies: LTE, multiplicative order, prime exponent comparison, or special factorization.

Strategies for Olympiad Success

- Do not expand large products. Factor them.
- When divisibility involves powers, use valuations.
- When factorials appear, use Legendre's Formula.
- When binomial coefficients appear, subtract valuations.
- When expressions look like $a^n - b^n$, try factorization or LTE.
- When powers repeat modulo a number, use multiplicative order.
- When testing primality, only check primes up to the square root.
- When a prime expression looks suspicious, try proving it is composite by finding a factor.

Common Mistake

Many students try to compute numbers that are far too large. Olympiad number theory usually rewards structure, not brute force.

Section Strategy Summary

When facing a prime factorization problem, try the following sequence:

1. Factor all small numbers.
2. Identify the important prime.
3. Translate divisibility into valuation inequalities.
4. Use Legendre's Formula for factorials.
5. Use binomial valuation formulas for combinations.
6. Use $a^n - b^n$ factorization when exponents appear.
7. Use LTE if the expression is an exponential difference.
8. Use multiplicative order if the problem asks about repeating powers.

Closing Thoughts

Prime numbers aren't isolated objects, but rather the structures beneath all integers. The deeper a student goes into number theory, the more often problems become hidden tasks rooted in prime factorizations and divisibility.

Resources and References

1. Art of Problem Solving - `https://artofproblemsolving.com/`
2. HMMT Problem Sets - `https://www.hmmt.org/www/archive/problems`
3. Yufei Zhao's Notes - `https://yufeizhao.com/olympiad/`
4. Evan Chen's Olympiad Resources - `https://web.evanchen.cc/`
5. David Altizio's Web Page - `https://davidaltizio.web.illinois.edu/mathlinks.html`