Prime Numbers and Factorization

Advanced Techniques in Olympiad Number Theory

Aryan Ayyanger

Contents

1 Introduction

Prime numbers form the structural foundation of arithmetic. While foundational number theory focuses on divisibility, greatest common divisors, and modular remainders, this handout examines the structures at a deeper level.

The focus here is not to repeat elementary divisibility rules. Instead, this guide studies how primes behave inside products, factorials, binomial coefficients, exponential expressions, and olympiad-style equations.

> *"A prime number is one measured by a unit alone."* — **Euclid**, *Elements*, Book VII, Definition 11

Like Euclid stated, prime numbers are simply the building blocks or basic units of number theory. This handout continues continues with the first number theory handout and discovers the power that primes entail. Definitions are stated concisely, with primary emphasis placed on pattern recognition, structural proofs, and contest applications.

Key Question

Advanced number theory frequently reduces to a single structural question:

What is the exact prime valuation $v_p(N)$ of the given expression?

2 Prime Numbers as Arithmetic Atoms

A prime number is an integer greater than 1 with exactly two positive divisors: 1 and itself. Prime numbers cannot be decomposed into smaller positive integer factors.

The initial sequence of primes is:

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

Composite numbers are constructed from prime factors. For example:

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

The utility of prime numbers stems from the uniqueness of integer prime decomposition.

2.1 Why Primes Matter in Olympiad Problems

Many olympiad number theory problems appear distinct on the surface:

- factorial divisibility,
- binomial coefficient valuation,
- exponential congruences,
- Diophantine equations involving powers,
- prime-generating polynomial evaluations,
- structural integer bounds.

Beneath surface variations, these problem types consistently depend on analyzing prime exponents.

Example 2.1

Determine whether $72 \mid 10!$ without evaluating $10!$.

Solution. Factor the divisor into prime powers:

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

Expanding $10!$:

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

Counting factors directly, the product contains at least three factors of 2 (from $2, 4, 6, 8, 10$) and at least two factors of 3 (from $3, 6, 9$). Therefore:

$$72 \mid 10!.$$

□

3 Euclid's Proof of Infinitely Many Primes

Euclid's proof of the infinitude of primes illustrates a fundamental constructive technique in number theory.

Theorem

There are infinitely many prime numbers.

Proof. Assume for contradiction that only finitely many primes exist:

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

Construct the integer:

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

Dividing N by any listed prime p_i yields a remainder of 1. Consequently, no prime in the set $\{p_1, p_2, \ldots, p_n\}$ divides N.

However, every integer greater than 1 possesses at least one prime factor. Thus N must be divisible by a prime not included in the original set, contradicting the assumption that the set contained all primes.

Therefore, the set of prime numbers is infinite. □

3.1 Constructive Extensions

Example 3.1

Show that no finite set of primes can divide all integers constructed by adding 1 to a product of distinct primes.

Solution. Let S be any finite set of prime numbers. Define:

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

No prime $p \in S$ can divide N, because $N \equiv 1 \pmod{p}$. Any prime divisor of N must lie outside S, demonstrating that S cannot contain all prime factors occurring across the integers. □

4 The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic establishes that every integer greater than 1 factors uniquely into a product of prime powers.

Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be expressed in the form:

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

where $p_1 < p_2 < \cdots < p_k$ are distinct primes and each exponent a_i is a positive integer. This representation is unique up to the order of factors.

4.1 Existence

If an integer $n > 1$ is not prime, it splits into a product ab with $1 < a, b < n$. Applying this step iteratively to composite factors must terminate because positive integers strictly decrease. The resulting factors are necessarily prime.

4.2 Uniqueness and Euclid's Lemma

Uniqueness depends on Euclid's Lemma, which establishes that prime factors cannot split across coprime components.

Euclid's Lemma

If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

This property fails for composite numbers. For example, $6 \mid (2 \cdot 3)$, yet $6 \nmid 2$ and $6 \nmid 3$.

5 Prime Exponents and Valuation

Prime valuation provides a systematic framework for translating divisibility questions into arithmetic equations.

Definition 5.1. *For a prime p and a positive integer n, the p-adic valuation $v_p(n)$ denotes the exponent of the highest power of p dividing n.*

For example, $48 = 2^4 \cdot 3^1$, which gives:

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

5.1 Properties of Valuations

Valuation Properties

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 properties convert multiplicative relationships into additive relations.

5.2 Computational Application

Example 5.1

Compute $v_3(5400)$.

Solution. Decompose 5400 into prime components:

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

Extracting the exponent of 3:

$$v_3(5400) = 3.$$

□

5.3 Divisibility via Valuations

The divisibility statement $a \mid b$ is logically equivalent to:

$$v_p(a) \le v_p(b) \quad \text{for every prime } p.$$

Example 5.2

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

Solution. Compare prime valuations individually:

- For $p = 2$: $v_2(\text{left}) = 5 \le 7 = v_2(\text{right})$.
- For $p = 3$: $v_3(\text{left}) = 2 > 1 = v_3(\text{right})$.

Because the valuation inequality fails for $p = 3$, divisibility does not hold. □

6 Valuations of GCD and LCM

Valuations simplify the behavior of greatest common divisors and least common multiples.

GCD and LCM Valuations

For positive integers a, b and prime p:

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

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

6.1 Application Example

Let $a = 2^4 \cdot 3^2 \cdot 5$ and $b = 2^2 \cdot 3^5 \cdot 7$. Evaluating prime by prime:

$$\gcd(a,b) = 2^{\min(4,2)} \cdot 3^{\min(2,5)} \cdot 5^{\min(1,0)} \cdot 7^{\min(0,1)} = 2^2 \cdot 3^2,$$

$$\operatorname{lcm}(a,b) = 2^{\max(4,2)} \cdot 3^{\max(2,5)} \cdot 5^{\max(1,0)} \cdot 7^{\max(0,1)} = 2^4 \cdot 3^5 \cdot 5 \cdot 7.$$

7 Legendre's Formula

Legendre's Formula determines the exact valuation of a prime inside a factorial.

Legendre's Formula

For any prime p and positive integer n:

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

The sum contains finitely many non-zero terms once $p^k > n$.

7.1 Structural Justification

The expansion $n! = 1 \cdot 2 \cdot 3 \cdots n$ receives one factor of p from each multiple of p, contributing $\lfloor n/p \rfloor$ factors.

Multiples of p^2 contribute an additional factor of p, adding $\lfloor n/p^2 \rfloor$ factors. Each higher prime power p^k similarly contributes one extra factor beyond those counted in earlier terms.

7.2 Examples

Example 7.1

Find $v_2(100!)$.

Solution. Apply Legendre's Formula for $p = 2$:

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

Summing the floor terms:

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

□

Example 7.2

Find $v_5(1000!)$.

Solution. Apply Legendre's Formula for $p = 5$:

$$v_5(1000!) = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor = 200 + 40 + 8 + 1 = 249.$$

□

8 Trailing Zeros in Factorials

Trailing zeros in a decimal integer correspond to factors of $10 = 2 \cdot 5$. The number of trailing zeros in N equals:

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

In factorial expansions $n!$, prime factors of 2 occur more frequently than factors of 5. Therefore, the count of trailing zeros in $n!$ is determined by $v_5(n!)$.

8.1 Examples

Example 8.1

Calculate the number of trailing zeros in 100!.

Solution. Evaluate $v_5(100!)$ via Legendre's Formula:

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

Hence 100! ends in 24 trailing zeros. □

Example 8.2

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

Solution. We require $v_5(n!) \geq 30$. Testing multiples of 5:

- For $n = 120$: $v_5(120!) = \lfloor 120/5 \rfloor + \lfloor 120/25 \rfloor = 24 + 4 = 28$.
- For $n = 124$: $v_5(124!) = 28$.
- For $n = 125$: $v_5(125!) = \lfloor 125/5 \rfloor + \lfloor 125/25 \rfloor + \lfloor 125/125 \rfloor = 25 + 5 + 1 = 31$.

The minimal integer satisfying the requirement is $n = 125$. □

Common Mistake

Multiples of 25 supply two factors of 5, while multiples of 125 supply three. Remember to account for higher powers of 5 when estimating trailing zeros.

9 Factorials and Composite Divisors

Legendre's Formula can determine divisibility conditions for composite values dividing factorials.

Example 9.1

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

Solution. Compute the relevant prime valuations of 50!:

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

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

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

Comparing exponents: $47 \geq 10$, $22 \geq 4$, and $12 \geq 2$. Divisibility holds. □

9.1 Maximizing Composite Divisors

Example 9.2

Find the largest integer k such that $12^k \mid 100!$.

Solution. Factor the base into prime components: $12 = 2^2 \cdot 3^1$, so $12^k = 2^{2k} \cdot 3^k$. Divisibility requires:

$$2k \leq v_2(100!) \quad \text{and} \quad k \leq v_3(100!).$$

Using Legendre's Formula:

$$v_2(100!) = 97, \qquad v_3(100!) = 33 + 11 + 3 + 1 = 48.$$

The conditions yield $k \leq \lfloor 97/2 \rfloor = 48$ and $k \leq 48$. The maximum integer is $k = 48$. □

10 Binomial Coefficients and Prime Powers

Prime exponents in binomial coefficients are computed by taking valuation differences:

Binomial Valuation Formula

For prime p and integers $0 \leq k \leq n$:

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

10.1 Valuation Example

Example 10.1

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

Solution. Using the valuation difference identity:

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

From earlier calculations, $v_2(100!) = 97$ and $v_2(50!) = 47$. Substituting these values:

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

□

11 Kummer's Theorem

Kummer's Theorem provides a base-p carry interpretation for prime valuations of binomial coefficients.

Kummer's Theorem

The exponent $v_p\left(\binom{n}{k}\right)$ equals the number of carries that occur when adding k and $n-k$ in base p.

11.1 Parity Criterion

A binomial coefficient $\binom{n}{k}$ is odd ($v_2 = 0$) if and only if no carries occur when adding k and $n-k$ in base 2. This is equivalent to requiring that the binary representation of k be a sub-mask of n (Lucas' Theorem).

12 Advanced Factorization Techniques

Standard algebraic factorizations frequently isolate prime components in contest settings.

12.1 Difference and Sum of Powers

For all positive integers n:

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

This implies $(a-b) \mid (a^n - b^n)$.

If n is odd:

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

12.2 Sophie Germain Identity

Sophie Germain Identity

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

This identity factors expressions of the form $x^4 + 4b^4$ into smaller quadratic terms.

Example 12.1

Factor $x^4 + 4$.

Solution. Setting $a = x$ and $b = 1$ in Sophie Germain's Identity:

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

□

13 Cyclotomic Polynomial Patterns

Expressions of the form $a^n - b^n$ factor systematically using the divisors of n.

For example, using $n = 6$:

$$a^6 - b^6 = (a^3 - b^3)(a^3 + b^3) = (a - b)(a^2 + ab + b^2)(a + b)(a^2 - ab + b^2).$$

Olympiad Insight

When encountering composite exponents in equations of the form $a^n \pm b^n$, factor the expression using proper divisors of n.

14 Mersenne Numbers

Mersenne numbers take the form $M_n = 2^n - 1$.

Theorem

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

Proof. Suppose n is composite, so $n = ab$ for integers $a, b > 1$. Then:

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

Because $(x - 1) \mid (x^b - 1)$, setting $x = 2^a$ yields:

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

Since $1 < 2^a - 1 < 2^n - 1$, $2^n - 1$ has a non-trivial factor and is composite. □

Common Mistake

The converse is false: if n is prime, $2^n - 1$ is not guaranteed to be prime. For instance, $2^{11} - 1 = 2047 = 23 \cdot 89$.

15 Fermat Numbers

Fermat numbers take the form $F_n = 2^{2^n} + 1$. The first five terms are:

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

all of which are prime. However, $F_5 = 2^{32} + 1 = 641 \cdot 6700417$ is composite.

15.1 Recurrence Property

Fermat Identity

For $n \geq 1$:

$$\prod_{k=0}^{n-1} F_k = F_n - 2.$$

This identity implies that any two distinct Fermat numbers F_m, F_n are relatively prime, providing another proof of the infinitude of primes.

16 Multiplicative Order

Definition 16.1. *Let* $\gcd(a, n) = 1$. *The multiplicative order of* a *modulo* n, *denoted* $\operatorname{ord}_n(a)$, *is the smallest positive integer* k *such that:*

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

Example 16.1

Find $\operatorname{ord}_7(2)$.

Solution. Compute successive powers modulo 7:

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

The smallest positive exponent yielding 1 is $k = 3$, so $\operatorname{ord}_7(2) = 3$. □

16.1 Fundamental Order Theorem

Order Division Theorem

If $\gcd(a, n) = 1$, then $a^m \equiv 1 \pmod{n}$ if and only if $\operatorname{ord}_n(a) \mid m$. In particular:

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

17 Repeating Decimals and Orders

The period length of a repeating decimal $\frac{1}{m}$ (with $\gcd(10, m) = 1$) equals $\operatorname{ord}_m(10)$.

Example 17.1

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

Solution. Compute powers of 10 modulo 13:

$$10^1 \equiv 10, \quad 10^2 \equiv 9, \quad 10^3 \equiv 12, \quad 10^4 \equiv 3, \quad 10^5 \equiv 4, \quad 10^6 \equiv 1 \pmod{13}.$$

Since $\text{ord}_{13}(10) = 6$, the repeating block length is 6. □

18 Lifting the Exponent Lemma (LTE)

Lifting the Exponent Lemma determines valuations of expressions of the form $a^n \pm b^n$.

LTE Lemma (Odd Primes)

Let p be an odd prime. If $p \mid (a-b)$ and $p \nmid a, p \nmid b$, then:

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

18.1 Application Examples

Example 18.1

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

Solution. Check LTE conditions: $p = 3$ is odd, $3 \mid (10-1)$, and $3 \nmid 10$. Applying LTE:

$$v_3(10^{12} - 1) = v_3(10-1) + v_3(12) = v_3(9) + v_3(12) = 2 + 1 = 3.$$

□

Example 18.2

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

Solution. Check conditions: $p = 5$ is odd, $5 \mid (6-1)$, and $5 \nmid 6$. Applying LTE:

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

□

19 The Special Case for $p = 2$

The valuation behavior for $p = 2$ requires a modified identity when the exponent is even.

LTE Lemma (p

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 19.1

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

Solution. Apply the base $p = 2$ LTE formula with $a = 3, b = 1, n = 20$:

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

Evaluating each valuation: $v_2(2) = 1$, $v_2(4) = 2$, and $v_2(20) = 2$. Thus:

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

□

Hypothesis Check

Verify all hypotheses ($p \mid a - b$, prime parity, and coprimality) before applying Lifting the Exponent.

20 Prime Exponents in Consecutive Products

The product of k consecutive integers contains predictable prime power contributions.

Consecutive Product Divisibility

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

This follows directly from the integrality of binomial coefficients:

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

21 Prime Counting and Primality Bounds

Square Root Bound

If n is composite, it has a prime divisor $p \leq \sqrt{n}$.

Proof. Let $n = ab$ with $1 < a \leq b < n$. Then $a^2 \leq ab = n$, which implies $a \leq \sqrt{n}$. Selecting any prime divisor p of a yields $p \leq a \leq \sqrt{n}$. □

Example 21.1

Determine whether 221 is prime.

Solution. Because $\sqrt{221} < 15$, check prime divisors up to 13: $\{2, 3, 5, 7, 11, 13\}$. Testing divisibility:

$$221 = 13 \cdot 17.$$

Thus 221 is composite. □

22 Prime Gaps and Modulo 6 Patterns

Every prime $p > 3$ satisfies $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.

All integers fall into residue classes $0, 1, 2, 3, 4, 5 \pmod 6$. Classes $0, 2, 4$ are even, and class 3 is divisible by 3. Prime values greater than 3 are restricted to 1 or 5 $\pmod 6$.

Common Mistake

$n \equiv 1, 5 \pmod 6$ is a necessary condition for primes greater than 3, but not a sufficient one. For example, $25 \equiv 1 \pmod 6$ is composite.

23 Advanced Worked Examples

Example 23.1

Find the largest integer k such that $18^k \mid 100!$.

Solution. Factor the base: $18 = 2 \cdot 3^2$, so $18^k = 2^k \cdot 3^{2k}$. Divisibility requires:

$$k \leq v_2(100!) \quad \text{and} \quad 2k \leq v_3(100!).$$

Using Legendre's Formula, $v_2(100!) = 97$ and $v_3(100!) = 48$. The second condition requires $2k \leq 48 \implies k \leq 24$, which is more restrictive than $k \leq 97$. Thus $k = 24$. □

Example 23.2

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

Solution. Express conditions in terms of prime valuations for an arbitrary prime p:

$$2v_p(a) \leq 3v_p(b) \quad \text{and} \quad 3v_p(b) \leq 4v_p(a).$$

To show $a \mid b^2$, we must prove $v_p(a) \leq 2v_p(b)$. From the first inequality:

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

Since this holds for all prime factors, $a \mid b^2$. □

24 Common Problem Patterns

- **Factorials ($n!$):** Apply Legendre's Formula to analyze prime valuations.
- **Binomial Coefficients $\binom{n}{k}$:** Use $v_p(n!) - v_p(k!) - v_p((n-k)!)$ or Kummer's Theorem.
- **Difference of Powers ($a^n - b^n$):** Combine algebraic factorizations with LTE.
- **Mersenne Expressions ($2^n - 1$):** Analyze exponent divisibility.
- **Exponential Modular Cycles:** Determine multiplicative orders $\text{ord}_m(a)$.

25 Problem Set

25.1 Introductory Problems

1. Prove that there are infinitely many prime numbers.
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 $\sqrt{n}$.

25.2 Intermediate Problems

11. Find the largest integer k such that $8^k \mid 100!$.
12. Find the largest integer 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 $x^6 - y^6$ into irreducible polynomials over $\mathbb{Z}$.
17. Use Sophie Germain's Identity to factor $x^4 + 4y^4$.
18. Compute $v_3(10^{18} - 1)$.
19. Compute $v_5(11^{25} - 1)$.
20. Find $\text{ord}_7(3)$.

25.3 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 distinct Fermat numbers are pairwise coprime.
23. Find the length of the repeating decimal expansion 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 with $\gcd(a,p)=1$.
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 $n \le 5$ such that $n!+1$ is prime, and explain why testing larger n becomes difficult.
34. Prove that if p is an odd prime and $p \mid (a-b)$, then $p \mid (a^n - b^n)$.
35. Construct and solve a valuation problem involving a factorial and a binomial coefficient.

26 Solutions and Answers

26.1 Introductory Problem Solutions

1. Assume finitely many primes $p_1,\dots,p_n$. The integer $N = p_1\cdots p_n + 1$ leaves remainder 1 when divided by any p_i, so its prime factor lies outside the set. Contradiction.
2. $2520 = 2^3\cdot 3^2\cdot 5\cdot 7$.
3. $1440 = 144\cdot 10 = (2^4\cdot 3^2)(2\cdot 5) = 2^5\cdot 3^2\cdot 5$. Thus $v_2(1440)=5$.
4. The prime exponent of 3 in $3^7\cdot 5^2\cdot 11$ is directly given by the term 3^7, so $v_3 = 7$.
5. $v_2(20!) = 10+5+2+1 = 18 \ge 4$, and $v_3(20!) = 6+2 = 8 \ge 2$. Yes, $2^4\cdot 3^2 \mid 20!$.
6. $v_5(200!) = \lfloor 200/5\rfloor + \lfloor 200/25\rfloor + \lfloor 200/125\rfloor = 40+8+1 = 49$.
7. The number of trailing zeros is $v_5(150!) = \lfloor 150/5\rfloor + \lfloor 150/25\rfloor + \lfloor 150/125\rfloor = 30+6+1 = 37$.
8. $\sqrt{13} < 4$. Checking prime factors 2 and 3: neither divides 13. Thus 13 is prime.
9. $\sqrt{391} < 20$. Testing primes $2,3,5,7,11,13,17$: we find $391 = 17\cdot 23$. Thus 391 is composite.
10. If $n = ab$ with $1 < a \le b < n$, then $a^2 \le ab = n \implies a \le \sqrt{n}$. Any prime factor p of a satisfies $p \le a \le \sqrt{n}$.

26.2 Intermediate Problem Solutions

11. $8^k = 2^{3k}$. By Legendre's Formula, $v_2(100!) = 97$. We require $3k \leq 97 \implies k = \lfloor 97/3 \rfloor = 32$.

12. $45^k = 3^{2k} \cdot 5^k$. Legendre gives $v_3(200!) = 66 + 22 + 7 + 2 = 97$ and $v_5(200!) = 40 + 8 + 1 = 49$. Conditions are $2k \leq 97 \implies k \leq 48$, and $k \leq 49$. Thus $k = 48$.

13. $v_2\left(\binom{50}{25}\right) = v_2(50!) - 2v_2(25!) = 47 - 2(22) = 3$.

14. $v_3\left(\binom{90}{30}\right) = v_3(90!) - v_3(30!) - v_3(60!) = (30 + 10 + 3 + 1) - (10 + 3 + 1) - (20 + 6 + 2) = 44 - 14 - 28 = 2$.

15. If $n = ab$ with $a, b > 1$, then $2^n - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + \cdots + 1)$, yielding non-trivial factors.

16. $x^6 - y^6 = (x - y)(x + y)(x^2 + xy + y^2)(x^2 - xy + y^2)$.

17. $x^4 + 4y^4 = (x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2)$.

18. By LTE for $p = 3$: $v_3(10^{18} - 1) = v_3(10 - 1) + v_3(18) = v_3(9) + v_3(18) = 2 + 2 = 4$.

19. By LTE for $p = 5$: $v_5(11^{25} - 1) = v_5(11 - 1) + v_5(25) = v_5(10) + v_5(25) = 1 + 2 = 3$.

20. Powers of 3 $\pmod 7$: $3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1$. Thus $\text{ord}_7(3) = 6$.

26.3 Advanced Problem Solutions

21. Proof by induction: Base case $n = 1$: $F_0 = 3 = F_1 - 2$. Assuming true for n, $\prod_{k=0}^{n} F_k = (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$.

22. If $d \mid F_m$ and $d \mid F_n$ $(m < n)$, then d divides $\prod_{k=0}^{n-1} F_k = F_n - 2$. Thus $d \mid (F_n - (F_n - 2)) = 2$. Since Fermat numbers are odd, $d = 1$.

23. The period length equals $\text{ord}_{17}(10)$. Testing powers of 10 $\pmod{17}$ shows $10^8 \equiv -1 \pmod{17}$, so $\text{ord}_{17}(10) = 16$.

24. By Fermat's Little Theorem, $p \mid (2^p - 2)$ holds for all prime numbers p.

25. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod p$. By the Order Division Theorem, $\text{ord}_p(a) \mid (p - 1)$.

26. Apply LTE for $p = 2$: $v_2(5^{32} - 1) = v_2(5 - 1) + v_2(5 + 1) + v_2(32) - 1 = v_2(4) + v_2(6) + v_2(32) - 1 = 2 + 1 + 5 - 1 = 7$.

27. Apply LTE for $p = 7$: $v_7(8^{49} - 1) = v_7(8 - 1) + v_7(49) = v_7(7) + v_7(49) = 1 + 2 = 3$.

28. $\binom{2p}{p} = \frac{(2p)!}{(p!)^2}$. $v_p((2p)!) = 2 + \lfloor 2/p \rfloor = 2$ for $p > 2$, and $v_p(p!) = 1$, so $v_p\left(\binom{2p}{p}\right) = 2 - 2(1) = 0$. Thus $p^2 \nmid \binom{2p}{p}$. Meanwhile, $v_2\left(\binom{2p}{p}\right) \geq 1$ via Kummer's Theorem (adding $p + p$ creates a carry in base 2), so it is divisible by 2.

29. $\frac{(n+1)(n+2)\cdots(n+k)}{k!} = \binom{n+k}{k} \in \mathbb{Z}$, which implies $k! \mid (n + 1) \cdots (n + k)$.

30. $12^k = 2^{2k} \cdot 3^k$. $v_2(100!/50!) = 97 - 47 = 50 \implies 2k \leq 50 \implies k \leq 25$. $v_3(100!/50!) = 48 - 22 = 26 \implies k \leq 26$. The limiting bound is $k = 25$.

31. $p \mid a^2 \implies v_p(a^2) \geq 1 \implies 2v_p(a) \geq 1 \implies v_p(a) \geq 1 \implies p \mid a$.

32. For any prime p, $v_p(ab) = v_p(a) + v_p(b)$ is even. Since $\gcd(a, b) = 1$, either $v_p(a) = 0$ or $v_p(b) = 0$. Thus $v_p(a)$ and $v_p(b)$ are both even for all p, making a and b perfect squares.

33. For $n = 1, 2, 3, 4, 5$: $1! + 1 = 2$ (prime), $2! + 1 = 3$ (prime), $3! + 1 = 7$ (prime), $4! + 1 = 25$ (composite), $5! + 1 = 121$ (composite). Solutions: $n \in \{1, 2, 3\}$. For $n \geq 5$, $n! + 1$ grows exponentially and requires factoring large numbers without predictable algebraic forms.

34. $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$. Since $p \mid (a - b)$, p divides the first factor, so $p \mid (a^n - b^n)$.

35. Example problem: Find $v_3\left(\binom{30}{15} \cdot 15!\right)$. Solution: $v_3\left(\binom{30}{15} \cdot 15!\right) = v_3\left(\frac{30!}{15!}\right) = v_3(30!) - v_3(15!) = (10 + 3 + 1) - (5 + 1) = 14 - 6 = 8$.

27 Olympiad Problem-Solving Strategies

When facing prime valuation problems, proceed through this strategy sequence:

- **Factor Small Values:** Convert all explicit integers into prime power representations.
- **Isolate Key Primes:** Focus on prime constraints that bound the expression.
- **Apply Valuations:** Translate divisibility statements into $v_p(n)$ inequalities.
- **Use Legendre's Formula:** Evaluate prime exponents inside factorials using floor sums.
- **Binomial Differences:** Compute $v_p\left(\binom{n}{k}\right)$ by subtracting denominator valuations.
- **Polynomial Factorization:** Factor expressions of the form $a^n \pm b^n$ before applying modular checks.
- **Apply LTE Lemma:** Use Lifting the Exponent for exponential differences matching prime hypotheses.
- **Order Analysis:** Utilize multiplicative orders $\text{ord}_m(a)$ when working with power cycles.

Structural Focus

Avoid expanding large numeric expressions. Olympiad number theory rewards structural decomposition over direct computation.

28 Closing Thoughts

Prime numbers are the fundamental structures underlying integer relationships. Mastery in contest number theory develops from recognizing when to apply specific prime factorization, valuation, and algebraic tools.

29 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 Olympiad Notes — https://yufeizhao.com/olympiad/
4. Evan Chen's Mathematical Resources — https://web.evanchen.cc/
5. David Altizio's Contest Archive — https://davidaltizio.web.illinois.edu/mathlinks.html