Number Theory Notes for 2025 IMO Camp

Phyoe Min Khant, Hsu Wutt Yee Linn

April 2025

Contents

1 Divisibility

For integers a and b, we say that a **divides** b, or that a is a **divisor** (or **factor**) of b, or that b is a **multiple** of a, if there exists an integer c such that $b = ca$, and we denote this by $a \mid b$. Otherwise, a does not divide b, and we denote this by $a \nmid b$.

A positive integer p is a **prime** if the only divisors of p are 1 and p. If $p^k \mid a$ and $p^{k+1} \nmid a$, where p is a prime—i.e., p^k is the highest power of p dividing a—we denote this by $p^k \parallel a$.

Useful Facts

- If $a, b > 0$ and $a \mid b$, then $a \leq b$.
- If $a \mid b_1, a \mid b_2, \ldots, a \mid b_n$, then for any integers $c_1, c_2, \ldots, c_n$,

$$a \Big| \sum_{i=1}^{n} b_i c_i.$$

Useful Identities

- If n is a positive integer, then

$$x^n - y^n = (x - y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right)$$

- If n is a positive odd number, then

$$x^n + y^n = (x + y)\left(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}\right)$$

- If p is a prime and $0 < k < p$, then

$$\binom{p}{k} \text{ is divisible by } p.$$

Theorem 1.1 The Division Algorithm

For any positive integer a and integer b, there exist unique integers q and r such that $b = qa + r$ and $0 \leq r < a$, with $r = 0$ iff $a \mid b$.

Theorem 1.2 The Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely in the form

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

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

Theorem 1.3 Euclid

There exist an infinite number of primes.

Proof. Suppose there are only finitely many primes $p_1, p_2, \ldots, p_n$. Let

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

By the Fundamental Theorem of Arithmetic, N must be divisible by some prime p. However, none of the p_i divide N (since $N \equiv 1 \mod p_i$), a contradiction. $\square$

Example 1.1. Let k be an even number. Is it possible to write 1 as the sum of the reciprocals of k odd integers?

Example 1.2. Let $k \geq 1$ be an odd integer. Prove that for any positive integer n, the sum

$$1^k + 2^k + \cdots + n^k$$

is not divisible by $n + 2$.

Example 1.3. Find all pairs (a, b) of positive integers such that

$$ab \mid a^{2025} + b.$$

Example 1.4. Show that for all prime numbers p,

$$Q(p) = \prod_{k=1}^{p-1} k^{2k-p-1}$$

is an integer.

Example 1.5. (1984 IMO Shortlist) Suppose that $a_1, a_2, \ldots, a_{2n}$ are distinct integers such that the equation

$$(x - a_1)(x - a_2) \cdots (x - a_{2n}) - (-1)^n (n!)^2 = 0$$

has an integer solution r. Show that

$$r = \frac{a_1 + a_2 + \cdots + a_{2n}}{2n}.$$

2 GCD and LCM

The **greatest common divisor** of two positive integers a and b is the greatest positive integer that divides both a and b, which we denote by $\gcd(a, b)$. Similarly, the **lowest common multiple** of a and b is the least positive integer that is a multiple of both a and b, which we denote by $\text{lcm}(a, b)$.

We say that a and b are **relatively prime** if $\gcd(a, b) = 1$. For integers $a_1, a_2, \ldots, a_n$, $\gcd(a_1, a_2, \ldots, a_n)$ is the greatest positive integer that divides all of $a_1, a_2, \ldots, a_n$, and $\text{lcm}(a_1, a_2, \ldots, a_n)$ is defined similarly.

Useful Facts

- For all a, b,
$$\gcd(a,b)\cdot\operatorname{lcm}(a,b)=ab.$$
- For all a, b, and m,
$$\gcd(ma,mb)=m\cdot\gcd(a,b)\quad\text{and}\quad\operatorname{lcm}(ma,mb)=m\cdot\operatorname{lcm}(a,b).$$
- If $d\mid\gcd(a,b)$, then
$$\gcd\left(\frac{a}{d},\frac{b}{d}\right)=\frac{\gcd(a,b)}{d}.$$
In particular, if $d=\gcd(a,b)$, then $\gcd(a/d,b/d)=1$; that is, a/d and b/d are relatively prime.
- If $a\mid bc$ and $\gcd(a,c)=1$, then $a\mid b$.
- For positive integers a and b, if d is a positive integer such that $d\mid a$, $d\mid b$, and for any d', $d'\mid a$ and $d'\mid b$ implies that $d'\mid d$, then $d=\gcd(a,b)$. This asserts that any common divisor of a and b divides $\gcd(a,b)$.
- If $a_1a_2\ldots a_n$ is a perfect k^{th} power and the a_i are pairwise relatively prime, then each a_i is a perfect k^{th} power.
- Any two consecutive integers are relatively prime.

Useful Identities

- For natural numbers a, m, and n,
$$\gcd(a^m-1,\ a^n-1)=a^{\gcd(m,n)}-1.$$

Theorem 2.1 GCD and LCM

Let the prime factorizations of two integers a,b be
$$a=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}=\prod_{i=1}^{k}p_i^{e_i}=\prod p_k^{e_k}$$
$$b=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}=\prod_{i=1}^{k}p_i^{f_i}=\prod p_k^{f_k}$$
The exponents above can be zero and the p_i's are distinct. Then,
$$gcd(a,b)=p_1^{min(e_1,f_1)}p_2^{min(e_2,f_2)}\cdots p_k^{min(e_k,f_k)}$$
$$lcm(a,b)=p_1^{max(e_1,f_1)}p_2^{max(e_2,f_2)}\cdots p_k^{max(e_k,f_k)}$$

Theorem 2.2 Number and Sum of Divisors

Let $n \in \mathbb{N}$ such that its prime factorization is

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

where $p_1, \cdots, p_k$ are distinct primes and $\alpha_1, \cdots, \alpha_k$ are positive integers.

- The number of (positive) divisors of n,

$$\tau(n) = (1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_k).$$

Note. The function $\tau(n)$ is odd if and only if n is a square.

- The sum of (positive) divisors of n,

$$\sigma(n) = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right) \cdots \left(\sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k}\right) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right)$$

Theorem 2.3 Euclidean Algorithm

For natural numbers a and b, $a > b$,

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

where, k is a positive integer.

Theorem 2.4 GCD using Euclidean Algorithm

For natural numbers a and b, $a > b$, we use division algorithm to determine a quotient and remainder q, r, such that $a = bq + r$. Then

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

We use division algorithm repeatedly

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\cdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

We have

$$\gcd(a,b) = \gcd(r_1,b) = \gcd(r_1,r_2) = \cdots = \gcd(r_{n-1},r_n) = r_n$$

Theorem 2.5 Bezout's Identity

For natural numbers a, b, there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$.

Proof. Run the Euclidean Algorithm backwards.

$$\begin{aligned}\gcd(a,b) &= r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = r_{n-2}(1 + q_n q_{n-1}) - r_{n-3}q_n \\ &= \cdots = ax + by\end{aligned}$$

Theorem 2.6 General Bezout's Identity

For integers $a_1, a_2, \ldots, a_n$, there exist $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \sum_{i=1}^{n} a_ix_i = \gcd(a_1, a_2, \ldots, a_n).$$

Proof. Using induction, moving from 2 to 3 variables.

Note. Bézout's Identity for polynomials works in exactly the same way as it does for integers. Assume $f(x), g(x) \in \mathbb{Z}[x]$. Then, using Euclid's Algorithm, we can find $u(x), v(x) \in \mathbb{Q}[x]$ such that

$$f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x)).$$

Theorem 2.7 Four Number Lemma

Let a, b, c, and d be positive integers such that

$$ab = cd.$$

Then there exist positive integers p, q, r, and s such that

$$a = pq, \quad b = rs, \quad c = ps, \quad d = qr.$$

Example 2.1. **(1959 IMO)** Prove that the fraction

$$\frac{21n + 4}{14n + 3}$$

is irreducible for every natural number n.

Example 2.2. **(1979 IMO)** Let p and q be natural numbers such that

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Prove that p is divisible by 1979.

Example 2.3. **(1972 USAMO)** Let a, b, and c be integers. Prove that

$$\frac{\text{lcm}[a,b,c]^2}{\text{lcm}[a,b] \cdot \text{lcm}[b,c] \cdot \text{lcm}[c,a]} = \frac{\gcd(a,b,c)^2}{\gcd(a,b) \cdot \gcd(b,c) \cdot \gcd(c,a)}.$$

Example 2.4. (1970 Canada NO) Given the polynomial

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

with integer coefficients $a_1, a_2, \ldots, a_n$, and given that there exist four distinct integers a, b, c, and d such that

$$f(a) = f(b) = f(c) = f(d) = 5,$$

show that there is no integer k such that $f(k) = 8$.

Example 2.5. (2002 Romanian MO) Let p, q be distinct primes. Prove that there are positive integers a, b such that the arithmetic mean of all the divisors of the number $n = p^a \cdot q^b$ is also an integer.

Example 2.6. (1989 Russian MO) Find the positive integers n with exactly 12 divisors $1 = d_1 < d_2 < \cdots < d_{12} = n$ such that the divisor with index $d_4 - 1$ (that is, d_{d_4-1}) is $(d_1 + d_2 + d_4)d_8$.

Example 2.7. (1996 Spanish MO) The natural numbers a and b are such that

$$\frac{a+1}{b} + \frac{b+1}{a}$$

is an integer. Show that the greatest common divisor of a and b is not greater that $\sqrt{a+b}$.

Example 2.8. (2017 India Practice TST) Let a, b, c, d be pairwise distinct positive integers such that

$$\frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+d} + \frac{d}{d+a}$$

is an integer. Prove that $a + b + c + d$ is not a prime number.

Example 2.9. (1970 IMO) Find all positive integers n such that the set

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

can be split into two disjoint subsets such that the products of elements in these subsets are the same.

Example 2.10. (2023 IMO) Determine all composite integers $n > 1$ that satisfy the following property: if $d_1, d_2, \ldots, d_k$ are all the positive divisors of n with $1 = d_1 < d_2 < \cdots < d_k = n$, then d_i divides $d_{i+1} + d_{i+2}$ for every $1 \le i \le k-2$.

Example 2.11. (1992 IMO) Find all integers a, b, c satisfying $1 < a < b < c$ such that $(a-1)(b-1)(c-1)$ is a divisor of $abc - 1$.

Example 2.12. (1998 IMO) Determine all pairs (a, b) of positive integers such that $ab^2 + b + 7$ divides $a^2b + a + b$.

Example 2.13. (1984 IMO) Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Prove that if $a + d = 2^k$ and $b + c = 2^m$ for some integers k and m, then $a = 1$.

3 Modular Arithmetic

- *(Modulus)* A modulus is a system for counting using only the fixed set of integers $0, 1, 2, \ldots, m-1$. When working in this modulus of m integers, we say that we are working with the integers modulo m.
- *(Congruence)* For a positive integer m and integers a and b, the following 3 statements are equivalent.
  1. a is congruent to b modulo m, i.e., $a \equiv b \pmod m$
  2. The difference between a and b is a multiple of m, i.e., $m \mid a - b$.
  3. a leaves the same remainder as b when divided by m, i.e., $a = mk + b$ for some integer k.
- *(Residue)* We say that r is the modulo m residue of a when $a \equiv r \pmod m$ and $0 \leq r < n$.

Theorem 3.1 Congruence Rules

Let a, b, c, d, x be integers and m, n be positive integers.

- *(Reflexivity)* $a \equiv a \pmod m$.
- *(Transitivity)* If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.
- *(Symmetry)* If $a \equiv b \pmod m$, then $b \equiv a \pmod m$.
- *(Addition)* If $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then $a+c \equiv b+d \pmod m$ and $a - c \equiv b - d \pmod m$.
- *(Multiplication)* If $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$.
- *(Exponentiation)* If $a \equiv b \pmod m$, then $a^n \equiv b^n \pmod m$.
- *(Division)* If $ac \equiv bc \pmod m$, then $a \equiv b \pmod{\frac{m}{gcd(m,c)}}$.
  In particular, if $ac \equiv bc \pmod m$ and $gcd(m, c) = 1$, then $a \equiv b \pmod m$.

Useful Facts

- If f is a polynomial with integer coefficients and $a \equiv b \pmod m$, then
$$f(a) \equiv f(b) \pmod m.$$
- If f is a polynomial with integer coefficients of degree n, not identically zero, and p is a prime, then the congruence
$$f(x) \equiv 0 \pmod p$$
has at most n solutions modulo p, counting multiplicity.

Theorem 3.2 Euler's Totient Theorem

Let a, m be integers. If $gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

where, $\phi(m) =$ *Euler's Totient Function.*
If prime factorization of m is

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

$$\begin{aligned}\phi(m) &= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\\ &= p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}\cdot(p_1-1)(p_2-1)\cdots(p_k-1).\end{aligned}$$

Theorem 3.3 Gauss

For any positive integer n, we have

$$\sum_{d|n}\phi(d) = n.$$

For instance, if $n = 10$, then

$$\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10.$$

Theorem 3.4 Fermat's Little Theorem

Let a be any integer relatively prime to a prime p. Then

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

Alternatively,
Let a be any integer. Then

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

Theorem 3.5 Modular Inverses

Let a, b, c, d, x be integers and m be positive integers.

- *(Definition)* A modular inverse of an integer a (modulo m) is an integer a^{-1} such that
$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$
- *(Existence)* Inverses do not exist when $gcd(a, m) > 1$. If $ax \equiv b \pmod{m}$ and $gcd(a, m) = 1$, then
$$x \equiv \frac{b}{a} \equiv b \cdot a^{-1} \pmod{m}.$$
- *(Inverses add like fractions)*
$$a \cdot c^{-1} + b \cdot d^{-1} \equiv \frac{a}{c} + \frac{b}{d} \equiv \frac{ad + bc}{cd} \equiv (ad + bc) \cdot (cd)^{-1}$$
- *(Inverses multiply like fractions)*
$$(a \cdot c^{-1}) \cdot (b \cdot d^{-1}) \equiv \frac{a}{c} \cdot \frac{b}{d} \equiv \frac{ab}{cd} \equiv ab \cdot (cd)^{-1}$$

Theorem 3.6 Wilson's Theorem

Let p be a prime.
$$(p - 1)! \equiv -1 \pmod{p}.$$

Theorem 3.7 Chinese Remainder Theorem

If a positive integer x satisfies
$$\begin{aligned} x &\equiv a_1 \quad (\text{mod } m)_1 \\ x &\equiv a_2 \quad (\text{mod } m)_2 \\ &\vdots \\ x &\equiv a_k \quad (\text{mod } m)_k \end{aligned}$$
where all m_i are relatively prime, then x has a unique solution $\pmod{m_1 \cdot m_2 \cdot m_k}$.

Theorem 3.8 Modular Contradictions

Let n be an integer.

1. $n^2 \equiv 0 \text{ or } 1 \pmod{3} \equiv 0 \text{ or } 1 \pmod{4} \equiv 0 \text{ or } \pm 1 \pmod{5}$
$n^2 \equiv 0 \text{ or } 1 \text{ or } 4 \pmod{8}$
2. $n^3 \equiv 0 \text{ or } \pm 1 \pmod{7} \equiv 0 \text{ or } \pm 1 \pmod{9}$
3. $n^4 \equiv 0 \text{ or } 1 \pmod{16}$

Example 3.1. **(Fermat Prime Conjecture)** Pierre de Fermat (1601-1665) stated that all integers in the form $2^{2^n} + 1$ are primes. About a century after Fermat's conjecture,

Leonhard Euler (1707-1783) showed that this conjecture was not true. If you were Euler, how would you prove it?
(Hint: It fails at $n = 5$. Prove that $641 \mid 2^{2^5} + 1$.)

Example 3.2. (2000 Russian MO) Evaluate the sum

$$\left\lfloor \frac{2^0}{3} \right\rfloor + \left\lfloor \frac{2^1}{3} \right\rfloor + \left\lfloor \frac{2^2}{3} \right\rfloor + \cdots + \left\lfloor \frac{2^{1000}}{3} \right\rfloor.$$

Example 3.3. (2008 PuMAC) Calculate the last 3 digits of

$$2008^{2007^{2006^{\cdots^{2^1}}}}.$$

Example 3.4. (2003 Romania) Consider the prime numbers $n_1 < n_2 < \cdots < n_{31}$. Prove that if $30 \mid (n_1^4 + n_2^4 + \cdots + n_{31}^4)$, then among these numbers one can find three consecutive primes.

Example 3.5. (2008 St. Petersburg) Given three distinct natural numbers a, b, c, show that

$$\gcd(ab+1, bc+1, ca+1) \le \frac{a+b+c}{3}.$$

Example 3.6. (1986 IMO) Let d be any positive integer not equal to $2, 5$, or 13. Show that one can find distinct a, b in the set $\{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square.

Example 3.7. (2004 APMO) Prove that

$$\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor$$

is even for every positive integer n.

Example 3.8. (2005 IMO) Consider the sequence $a_1, a_2, \ldots$ defined by

$$a_n = 2^n + 3^n + 6^n - 1$$

for all positive integers n. Determine all positive integers that are relatively prime to every term of the sequence.

4 Diophantine Equations

Useful Techniques

- Parity (Even or Odd)
- Factoring Equations

- Bounding (Using Inequalities)
- Modular Contradictions
- Minimality Contradictions (Infinite Descent, Vieta Jumping)

Example 4.1. (2005 JBMO) Find all positive integers x, y satisfying the equation

$$9(x^2 + y^2 + 1) + 2(3xy + 2) = 2005.$$

Example 4.2. (2008 IMO Shortlist) Let n be a positive integer and let p be a prime number. Prove that if a, b, c are integers (not necessarily positive) satisfying the equations

$$a^n + pb = b^n + pc = c^n + pa,$$

then $a = b = c$.

Example 4.3. (2023 IMO Shortlist) Determine all pairs (a, p) of positive integers with p prime such that $p^a + a^4$ is a perfect square.

Example 4.4. (INMO) Determine all non-negative integral pairs (x, y) for which

$$(xy - 7)^2 = x^2 + y^2.$$

Example 4.5. (Russia) Find all natural pairs of integers (x, y) such that

$$x^3 - y^3 = xy + 61.$$

Example 4.6. (2010 IMO Shortlist) Find the least positive integer n for which there exists a set $\{s_1, s_2, \ldots, s_n\}$ consisting of n distinct positive integers such that

$$\left(1 - \frac{1}{s_1}\right)\left(1 - \frac{1}{s_2}\right)\ldots\left(1 - \frac{1}{s_n}\right) = \frac{51}{2010}.$$

Example 4.7. (2019 IMO Shortlist) Find all triples (a, b, c) of positive integers such that

$$a^3 + b^3 + c^3 = (abc)^2.$$

Example 4.8. Find all pairs of integers (x, y) that satisfy the equation

$$x^2 - y! = 2001.$$

Example 4.9. (2021 JBMO Shortlist) Find all positive integers a, b, c such that

$$ab + 1, \quad bc + 1, \quad ca + 1$$

are all equal to the factorial of some positive integer.

Example 4.10. **(2002 IMO Shortlist)** Find the smallest positive integer t such that there exist integers $x_1, x_2, \ldots, x_t$ with

$$x_1^3 + x_2^3 + \cdots + x_t^3 = 2002^{2002}.$$

Example 4.11. Let a, b, c be integers such that

$$a^6 + 2b^6 = 4c^6.$$

Show that $a = b = c = 0$.

Example 4.12. **(Fermat)** Show that the only solution to the equation

$$x^3 + 2y^3 + 4z^3 = 0$$

in integers is $(0, 0, 0)$.

Example 4.13. **(2007 IMO)** Let a and b be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)^2$, then $a = b$.

Example 4.14. **(1988 IMO)** If a, b are positive integers such that

$$\frac{a^2 + b^2}{1 + ab}$$

is an integer, then it is a perfect square.

Example 4.15. Let a and b be positive integers such that ab divides $a^2 + b^2 + 1$. Show that

$$\frac{a^2 + b^2 + 1}{ab} = 3.$$

Example 4.16. Let k be a positive integer not equal to 1 or 3. Prove that the only solution to

$$x^2 + y^2 + z^2 = kxyz$$

over integers is $(0, 0, 0)$.

5 Solutions to the Problems

Example 1.1

Let k be an even number. Is it possible to write 1 as the sum of the reciprocals of k odd integers?

Solution. Assume that it is possible to write 1 as the sum of the reciprocals of k odd integers, i.e.,

$$1 = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$$

for odd integers $n_1, n_2, \cdots, n_k$. Then,

$$1 = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k} = \frac{n_2n_3n_4\cdots n_k + n_1n_3n_4\cdots n_k + n_1n_2n_4\cdots n_k + \cdots + n_1n_2n_3\cdots n_{k-1}}{n_1n_2n_3\cdots n_k}$$

The denominator of the resulting fraction is an odd number, since it is a product of only odd integers. On the other hand, the numerator of the resulting fraction is the sum of k odd numbers, making it an even number. (Note that k is an even number.)

Since the numerator does not equal the denominator, the fraction does not equal 1. $\therefore$ Impossible.

Motivation

Parity arguments are most naturally applied to integers although we are only given fractions. Therefore, we try to manipulate the given expression into integer terms.

□

Example 1.2

Let $k \geq 1$ be an odd integer. Prove that for any positive integer n, the sum

$$1^k + 2^k + \cdots + n^k$$

is not divisible by $n + 2$.

Solution. Note that, for a positive odd number k,

$$x^k + y^k = (x + y)(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1})$$

Therefore, $x + y | x^k + y^k$ for an odd k.

Case 1: n is an odd number. Then,
$1^k + 2^k + \cdots + n^k$
$= 1^k + (2^k + n^k) + (3^k + (n-1)^k) + (4^k + (n-2)^k) + \cdots + ((\frac{n+1}{2})^k + (\frac{n+3}{2})^k)$

When paired as above, we can write $1^k + 2^k + \cdots + n^k$ as the sum of 1 + a multiple of $(n+2)$. By Euclid's Division Lemma, there will be a remainder of 1 when $1^k+2^k+\cdots+n^k$ is divided by $n+2$.

$\therefore$ The sum is not divisible by $n+2$.

Case 2: n is an even number. Then,
$1^k + 2^k + \cdots + n^k$
$= 1^k + (2^k + n^k) + (3^k + (n-1)^k) + (4^k + (n-2)^k) + \cdots + ((\frac{n}{2})^k + (\frac{n+4}{2})^k) + (\frac{n+2}{2})^k$

When paired as above, we can write $1^k + 2^k + \cdots + n^k$ as $1 + (\frac{n+2}{2})^k+$ a multiple of $(n+2)$. Then, $1^k + 2^k + \cdots + n^k$ is divisible by $n+2$ if and only if $1 + (\frac{n+2}{2})^k$ is divisible by $n+2$. Let $n = 2m$ for a positive integer m. Then

$$1 + (\frac{n+2}{2})^k = 1 + (m+1)^k$$

By Euclid's Division Lemma, we know that there will be a remainder of 1 when $1+(\frac{n+2}{2})^k$ is divided by $m+1$. Since $1 + (\frac{n+2}{2})^k$ is not divisible by $m+1$, it will not be divisible by $2(m+1)$, that is $n+2$.

$\therefore$ For any case, the sum is not divisible by $n+2$.

Motivation

The main challenge lies in recognizing $x+y$ divides x^k+y^k for all (x,y) and an odd number k. In fact, you should always think of the two useful factorization formulae (check NTL1) when exponents and divisibility are involved! It is then easy to pair numbers whose base-numbers add up to $n+2$. The rest comes naturally working the terms out.

$\square$

Example 1.3

Find all pairs (a, b) of positive integers such that

$$ab \mid a^{2025} + b.$$

Solution.

$$ab|a^{2025} + b \Rightarrow a|a^{2025} + b \Rightarrow a|b.$$

Let $b = ak_1$. Then, we get

$$a^2k_1|a^{2025} + ak_1 \Rightarrow ak_1|a^{2024} + k_1$$

What we got here is indeed a similar statement to the given statement. The differences are just a^{2024} and k_1. Then, let $k_1 = ak_2$.

$$a^2k_2|a^{2024} + ak_2 \Rightarrow ak_2|a^{2023} + k_2$$

let $k_i = ak_{i+1}$. Continuing the pattern, we get

$$a^2k_3|a^{2023} + ak_3 \Rightarrow ak_3|a^{2022} + k_3$$

$$.$$

$$.$$

$$.$$

$$a^2k_{2025}|a + ak_{2025} \Rightarrow ak_{2025}|1 + k_{2025}$$

$$ak_{2025}|1 + k_{2025} \Rightarrow k_{2025}|1 + k_{2025} \Rightarrow k_{2025} = 1$$

$$ak_{2025}|1 + k_{2025} \Rightarrow a|1 + k_{2025} \Rightarrow a|2$$

$$\therefore a = 1 \quad \text{(or)} \quad 2$$

$$b = a \times k_1 = a \times a \times k_2 = \cdots = a^{2025}k_{2025}.$$

Case 1: $a = 1$

$$\therefore b = a^{2025}k_{2025} = 1.$$

Case 2: $a = 2$

$$\therefore b = a^{2025}k_{2025} = 2^{2025}.$$

The two pairs $(1, 1)$ and $(2, 2^{2025})$ are the answers.

Motivation

The key idea is noticing $ab \mid x$ means both $a \mid x$ and $b \mid x$. After that, it's worth it to substitute b as a product of a and a number (which is k_1 in our case). A pattern appears and it becomes easy to work out the answer from there.

□

Example 1.4

Show that for all prime numbers p,

$$Q(p) = \prod_{k=1}^{p-1} k^{2k-p-1}$$

is an integer.

Solution.

$$Q(p) = \prod_{k=1}^{p-1} k^{2k-p-1} = 1^{2-p-1} \times 2^{4-p-1} \times \cdots \times \left(\frac{p+1}{2}\right)^0 \times \left(\frac{p+3}{2}\right)^2 \times \cdots \times (p-1)^{p-3}$$

Let

$$A = 1^{-(2-p-1)} \times 2^{-(4-p-1)} \times \cdots \times \left(\frac{p-1}{2}\right)^2$$

$$\Rightarrow A = (1!)^2 \times (2!)^2 \times (3!)^2 \times \cdots \times \left[\left(\frac{p-3}{2}\right)!\right]^2 \times \left[\left(\frac{p-1}{2}\right)!\right]^2$$

Let

$$B = \left(\frac{p+3}{2}\right)^2 \times \left(\frac{p+5}{2}\right)^4 \times \cdots \times (p-1)^{p-3}$$

$$\Rightarrow B = \left({}^{p-1}P_1\right)^2 \times \left({}^{p-1}P_2\right)^2 \times \cdots \times \left({}^{p-1}P_{\frac{p-3}{2}}\right)^2$$

Note that

$${}^nC_r = \frac{{}^nP_r}{r!}$$

Then,

$$Q(p) = \frac{B}{A} = \frac{\left({}^{p-1}P_1\right)^2}{(1!)^2} \times \frac{\left({}^{p-1}P_2\right)^2}{(2!)^2} \times \cdots \times \frac{\left({}^{p-1}P_{\frac{p-3}{2}}\right)^2}{\left[\left(\frac{p-3}{2}\right)!\right]^2} \times \left[\left(\frac{p-1}{2}\right)!\right]^{-2}$$

$$= \left[\frac{{}^{p-1}C_1 \times {}^{p-1}C_2 \times {}^{p-1}C_3 \times \cdots \times {}^{p-1}C_{\frac{p-3}{2}}}{\left(\frac{p-1}{2}\right)!}\right]^2$$

Let $R(p) = \sqrt{Q(p)}$. Note that $Q(p)$ is an integer if and only if $R(p)$ is an integer since $R(p)$ is rational.

$$R(p) = \frac{{}^{p-1}C_1 \times {}^{p-1}C_2 \times {}^{p-1}C_3 \times \cdots \times {}^{p-1}C_{\frac{p-3}{2}}}{\left(\frac{p-1}{2}\right)!}$$

$$= \frac{{}^{p-1}C_1 \times {}^{p-1}C_2 \times {}^{p-1}C_3 \times \cdots \times {}^{p-1}C_{\frac{p-3}{2}}}{\left(\frac{p-1}{2}\right)!} \times \frac{{}^{p-1}P_{\frac{p-1}{2}}}{{}^{p-1}P_{\frac{p-1}{2}}}$$

$$= \frac{{}^{p-1}C_1 \times {}^{p-1}C_2 \times {}^{p-1}C_3 \times \cdots \times {}^{p-1}C_{\frac{p-3}{2}} \times {}^{p-1}C_{\frac{p-1}{2}}}{{}^{p-1}P_{\frac{p-1}{2}}}$$

Note that $\frac{{}^{p-1}C_i}{p-i} \times p = {}^pC_i$ for $i = 1, 2, 3, \cdots, \frac{p-1}{2}$. Then,

$$R(p) = \frac{{}^{p-1}C_1 \times {}^{p-1}C_2 \times {}^{p-1}C_3 \times \cdots \times {}^{p-1}C_{\frac{p-3}{2}} \times {}^{p-1}C_{\frac{p-1}{2}}}{{}^{p-1}P_{\frac{p-1}{2}}} \times \frac{p^{\frac{p-1}{2}}}{p^{\frac{p-1}{2}}}$$

$$= \frac{{}^pC_1 \times {}^pC_2 \times {}^pC_3 \times \cdots \times {}^pC_{\frac{p-3}{2}} \times {}^pC_{\frac{p-1}{2}}}{p^{\frac{p-1}{2}}}$$

We know that $p \mid {}^pC_i$, for $i = 1, 2, \cdots, p-1$. $\therefore R(p)$ must be an integer.

Motivation

We first expand the product and find that the exponent of the terms increases by 2. This leads us to rephrase the terms nicely — with factorials and permutations. The fact that we are working on a prime p eliminates attempting recursion-involved techniques like induction. Instead, we find a truth that is only true for prime numbers: $p \mid {}^pC_i$, for $i = 1, 2, \cdots, p-1$. (You will also see this in NTP1 Problem 10.)
By integrating these two key ideas, we rephrase Q(p) throughout the solution, ultimately establishing that it is an integer.

□

Example 1.5

(1984 IMO Shortlist) Suppose that $a_1, a_2, \ldots, a_{2n}$ are distinct integers such that the equation
$$(x-a_1)(x-a_2)\cdots(x-a_{2n}) - (-1)^n(n!)^2 = 0$$
has an integer solution r. Show that
$$r = \frac{a_1 + a_2 + \cdots + a_{2n}}{2n}.$$

Solution. Let r be the integer solution to the equation and $S = (r-a_1)(r-a_2)\cdots(r-a_n) = (-1)^n(n!)^2$.

Note that $r - a_i$ are distinct non-negative integers for $i = 1, 2, \cdots, 2n$.

WLOG, let $|r-a_1| \le |r-a_2| \le \cdots \le |r-a_n|$.

$$|r-a_1| \ge 1$$

$$|r-a_2| \ge 1$$

(minimum values of $r-a_1$ and $r-a_2$ are -1 and 1 each)

$$|r-a_3| \ge 2$$

$$|r-a_4| \ge 2$$

(minimum values of $r-a_3$ and $r-a_4$ are -2 and 2 each)

$$\cdots$$

$$|r-a_{2n-1}| \ge n$$

$$|r-a_{2n}| \ge n$$

Therefore,

$$\begin{aligned}|S| &= |r-a_1|\times|r-a_2|\times\cdots\times|r-a_n|\\ &\geq (n!)^2\end{aligned}$$

However, we know that $|S|=(n!)^2$. $\therefore$ It must be the case of equality for the inequalities above, i.e.,

$$|r-a_1|=1$$
$$|r-a_2|=1$$
$$|r-a_3|=2$$
$$|r-a_4|=2$$
$$\cdots$$
$$|r-a_{2n-1}|=n$$
$$|r-a_{2n}|=n$$

Taking the vertical bars off,

$$r-a_1=-1$$
$$r-a_2=1$$
$$r-a_3=-2$$
$$r-a_4=2$$
$$\cdots$$
$$r-a_{2n-1}=-n$$
$$r-a_{2n}=n$$

Adding the above equations leaves us with

$$2nr-(a_1+a_2+\cdots+a_{2n})=0$$
$$\therefore r=\frac{a_1+a_2+\cdots+a_{2n}}{2n}$$

Motivation

The key idea is expanding $(-1)^n(n!)^2=(-n)\times(-(n-1))\times\cdots\times(-1)\times1\times2\times\cdots\times n$. It conveniently expands to $2n$ terms and they are all distinct. This leads us to assuming that these $2n$ terms could equal to $(r-a_i)$ terms and focus on proving why so. Also, $(r-a_i)$ being *distinct* integers implies bounding — which we utilize to get to our goal.

$\square$

Example 2.2

(1979 IMO) Let p and q be natural numbers such that

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Prove that p is divisible by 1979.

Solution.

$$\begin{aligned}\frac{p}{q} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{1318} + \frac{1}{1319} - 2\left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{1318}\right)\\ &= \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{1318} + \frac{1}{1319}\right) - \left(1 + \frac{1}{2} + \cdots + \frac{1}{659}\right)\\ &= \frac{1}{660} + \frac{1}{661} + \cdots + \frac{1}{1319}\end{aligned}$$

Now consider pairing the terms symmetrically,

$$\frac{1}{660} + \frac{1}{1319} = \frac{1979}{660 \times 1319}, \quad \frac{1}{661} + \frac{1}{1318} = \frac{1979}{661 \times 1318}, \quad \ldots$$

Thus,

$$\frac{p}{q} = \frac{1979}{660 \times 1319} + \frac{1979}{661 \times 1318} + \cdots + \frac{1979}{989 \times 990} = 1979 \cdot \frac{r}{s}$$

Since 1979 is a prime and coprime to s, it follows that p is divisible by 1979. $\square$

Example 2.3

(1972 USAMO) Let a, b, and c be integers. Prove that

$$\frac{\operatorname{lcm}[a,b,c]^2}{\operatorname{lcm}[a,b] \cdot \operatorname{lcm}[b,c] \cdot \operatorname{lcm}[c,a]} = \frac{\gcd(a,b,c)^2}{\gcd(a,b) \cdot \gcd(b,c) \cdot \gcd(c,a)}.$$

Solution. Let p be a random prime. Let x, y, z be the amount of p's in the factorization of a, b, c respectively.

WLOG, let $x \geq y \geq z$. Then, the number of factor's of p on LHS is $\frac{x^2}{x^2 \times y}$, while on the RHS, $\frac{z^2}{z^2 \times y}$, which are clearly equal. As this is true for all primes, LHS = RHS.

Motivation

We know that all numbers are composed of primes. We also know that if a prime p is present on LHS, it must also be present on RHS through the definitions of GCD and LCM themselves. But it's not so obvious that the factor's of p on LHS and RHS are actually equal; so, we focus on that.
Unrelated to the solution above, you can also use the technique of writing a, b, c in terms of their GCD's that we used on many other NT problems previously. Since we are dealing with a, b, c here, there are some more extra steps than dealing with just a, b. This method also solves this problem. (This was my initial solution.)

□

Example 2.4

(1970 Canada NO) Given the polynomial

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

with integer coefficients $a_1, a_2, \ldots, a_n$, and given that there exist four distinct integers a, b, c, and d such that

$$f(a) = f(b) = f(c) = f(d) = 5,$$

show that there is no integer k such that $f(k) = 8$.

Solution. Let $g(x) = f(x) - 5$. Then

$$g(a) = g(b) = g(c) = g(d) = 0$$

This implies a, b, c, and d are zeroes of g(x). Hence, let

$$g(x) = (x - a)(x - b)(x - c)(x - d)h(x)$$

where $h(x)$ is a polynomial with integer coefficient .

For the sake of contradiction, assume that there exist one k such that $f(k) = 8$. This means $g(k) = (k - a)(k - b)(k - c)(k - d)h(k) = f(k) - 5 = 3$

But, $(k - a)(k - b)(k - c)(k - d)h(k) = 3$ is impossible: at least four out of the five terms on LHS must be distinct. However the smallest absolute value you can obtain by a product of four distinct integers is $|1 \times (-1) \times 2 \times (-2)| = 4$ In other words, $|(k - a)(k - b)(k - c)(k - d)h(k)| \geq 4$. $\therefore$ Contradiction!

Motivation

It is important to note the two facts: a, b, c, d are distinct integers AND the given polynomial is one with integer coefficients. This means there should be limited options to factorize an integer as small as numbers around 5 and 8 and frame these small numbers under some polynomials with integer coefficients.

□

Example 2.5

(2002 Romanian MO) Let p, q be distinct primes. Prove that there are positive integers a, b such that the arithmetic mean of all the divisors of the number $n = p^a \cdot q^b$ is also an integer.

Solution. The sum of all divisors of n is given by the formula

$$(1+p+p^2+\cdots+p^a)(1+q+q^2+\cdots+q^b),$$

The number n has $(a+1)(b+1)$ positive divisors and their arithmetic mean is

$$M = \frac{(1+p+p^2+\cdots+p^a)(1+q+q^2+\cdots+q^b)}{(a+1)(b+1)}.$$

If p and q are both odd, we can take $a = p$ and $b = q$, and it is easy to see that M is an integer because $1+p+p^2+\cdots+p^a \equiv 1-1+1-1\cdots-1 = 0 \pmod{p+1}$. If $p = 2$ and q odd, taking b as q, M becomes

$$M = \frac{(1+p+p^2+\cdots+p^a)(1+q^2+\cdots+q^{b-1})}{(a+1)}.$$

If we take a as $q^2+\cdots+q^{b-1}$, then M is an integer. $\square$

Example 2.6

(1989 Russian MO) Find the positive integers n with exactly 12 divisors $1 = d_1 < d_2 < \cdots < d_{12} = n$ such that the divisor with index $d_4 - 1$ (that is, d_{d_4-1}) is $(d_1+d_2+d_4)d_8$.

Solution. Let $d_i = d_1 + d_2 + d_4$ where $1 \leq i \leq 12$. We will prove that $i = 5$. Since $d_i > d_4$, we have $i \geq 5$. Also, observe that $d_j d_{13-j} = n$ for all j and since $d_i d_8 = d_{d_4-1} \leq n$,, we must have $i \leq 5$., thus $i = 5$ and $d_1 + d_2 + d_4 = d_5$. Also, $d_{d_4-1} = d_5 d_8 = n = d_{12}$, thus $d_4 = 12$ and $d_5 = 14 + d_2$.. Of course, d_2 is the smallest prime divisor of n, and since $d_4 = 13$, we can only have $d_2 \in \{2, 3, 5, 7, 11\}$. Also, since n has 12 divisors, it has at most 3 prime divisors. If $d_2 = 2$ then $d_5 = 16$ and then 4 and 8 are divisors of n smaller than $d_4 = 13$,, impossible. A similar argument shows that $d_2 = 3$ and $d_5 = 17$. Since n has 12 divisors and is a multiple of $3 \cdot 13 \cdot 17$, the only possibilities are $9 \cdot 13 \cdot 17, 3 \cdot 169 \cdot 17, 3 \cdot 13 \cdot 289$. One can easily check that only $9 \cdot 13 \cdot 17 = 1989$ is a solution. $\square$

Example 2.7

(1996 Spanish MO) The natural numbers a and b are such that

$$\frac{a+1}{b} + \frac{b+1}{a}$$

is an integer. Show that the greatest common divisor of a and b is not greater that $\sqrt{a+b}$.

Solution. Let $d = \gcd(a, b)$. Adding 2, we see that

$$\frac{a+1}{b} + \frac{b+1}{a} + 2 = \frac{(a+b)(a+b+1)}{ab}$$

is an integer. Since d^2 divides the denominator and $gcd(d, a+b+1) = 1$, we must have $d^2 \mid a+b$; hence $d \leq \sqrt{a+b}$. □

Example 2.8

(2017 India Practice TST) Let a, b, c, d be pairwise distinct positive integers such that

$$\frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+d} + \frac{d}{d+a}$$

is an integer. Prove that $a + b + c + d$ is not a prime number.

Solution. Let

$$X = \frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+d} + \frac{d}{d+a}$$

Let

$$Y = \frac{b}{a+b} + \frac{c}{b+c} + \frac{d}{c+d} + \frac{a}{d+a}$$

We see that $X + Y = 4$, meaning Y must be an integer just like X. We can also see that $X > 1$ because

$$X = \frac{a}{a+b}+\frac{b}{b+c}+\frac{c}{c+d}+\frac{d}{d+a} > \frac{a}{a+b+c+d}+\frac{b}{a+b+c+d}+\frac{c}{a+b+c+d}+\frac{d}{a+b+c+d} = 1$$

Similarly, $Y > 1$. $X, Y > 1$ means $X, Y \geq 2$, making $X + Y \geq 4$. However, $X + Y = 4$, so $X = Y = 2$.
So far,

$$2 = \frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+d} + \frac{d}{d+a} = \frac{b}{a+b} + \frac{c}{b+c} + \frac{d}{c+d} + \frac{a}{d+a}$$

$$\begin{aligned}
0 &= \frac{a-b}{a+b} + \frac{b-c}{b+c} + \frac{c-d}{c+d} + \frac{d-a}{d+a} \\
&= \frac{ac+ad-bc-bd+ac-ad+bc-bd}{(a+b)(c+d)} + \frac{ab-ac+bd-cd+bd-ab+cd-ac}{(b+c)(a+d)} \\
&= 2(ac-bd)\frac{(b+c)(a+d)-(a+b)(c+d)}{(a+b)(b+c)(c+d)(d+a)} \\
&= 2(ac-bd)\frac{(a-c)(b-d)}{(a+b)(b+c)(c+d)(d+a)}
\end{aligned}$$

This leads us to ac = bd. Using Four Number Lemma, which tells us $a + b + c + d$ is not a prime.

Motivation

We know that X is an integer (SUPER SPECIFIC) and it is smaller than 4 but greater than 1. We also want to bring out X's evil twin brother, Y, to compare their properties, which eventually lead us to solving that $X = Y$. If you have seen proof for $a + b + c + d$ not being prime when $ac = bd$, it is easy to want a, b, c, d to mix with each other. Hence, we try $X - Y = 0$.

$\square$

Example 2.10

(2023 IMO) Determine all composite integers $n > 1$ that satisfy the following property: if $d_1, d_2, \ldots, d_k$ are all the positive divisors of n with $1 = d_1 < d_2 < \cdots < d_k = n$, then d_i divides $d_{i+1} + d_{i+2}$ for every $1 \le i \le k - 2$.

Solution. Let $p < q$ be the two smallest prime divisors of n. Then the three largest divisors of n are either

$$\{n, \frac{n}{p}, \frac{n}{q}\} \quad \text{or} \quad \{n, \frac{n}{p}, \frac{n}{p^2}\}.$$

Case 1. $\dfrac{n}{q}$ divides $n + \dfrac{n}{p}$

$$\frac{n + \frac{n}{p}}{\frac{n}{q}} = \frac{n\left(1 + \frac{1}{p}\right)}{\frac{n}{q}} = q\left(1 + \frac{1}{p}\right) = q + \frac{q}{p}.$$

This is not an integer, leading to a contradiction.

Case 2. $\dfrac{n}{p^2}$ divides $n + \dfrac{n}{p}$

$$\frac{n + \frac{n}{p}}{\frac{n}{p^2}} = \frac{n\left(1 + \frac{1}{p}\right)}{\frac{n}{p^2}} = p^2 + p,$$

which is an integer.

The fourth largest divisor is either $\dfrac{n}{q}$ or $\dfrac{n}{p^3}$. The former is impossible, since

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

This being an integer contradicts the assumption that p^2 is coprime to both q and $p+1$.

Therefore, it can be concluded that n has only one prime divisor, and the solution is $n = p^a$, where p is a prime and a is a positive integer greater than 1. $\square$

Example 2.11

(1992 IMO) Find all integers a, b, c satisfying $1 < a < b < c$ such that $(a-1)(b-1)(c-1)$ is a divisor of $abc - 1$.

Solution. Let $x = a - 1$, $y = b - 1$, and $z = c - 1$. Suppose

$$xyz \mid (x+1)(y+1)(z+1) - 1,$$

where $0 < x < y < z$.

Then,

$$xyz \mid (x+1)(y+1)(z+1) - 1 = xyz + xy + yz + xz + x + y + z.$$

So,

$$xyz \mid xy + yz + xz + x + y + z.$$

Let

$$S = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{xy} + \frac{1}{yz} + \frac{1}{xz} \in \mathbb{Z}.$$

The maximum value of S occurs when $x = 1$, $y = 2$, and $z = 3$:

$$S = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = \frac{17}{6} = 2\frac{5}{6}.$$

Thus,

$$0 < S \leq \frac{17}{6} \Rightarrow S = 1 \text{ or } 2.$$

Let $(x, y, z) = (3, 4, 5)$. Then

$$S = \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{12} + \frac{1}{15} + \frac{1}{20} = \frac{59}{60}.$$

So $S < 1$ in this case. Hence, we must have $x = 1$ or $x = 2$.

Case 1: $x = 1$ Then

$$S = 1 + \frac{1}{y} + \frac{1}{z} + \frac{1}{y} + \frac{1}{z} + \frac{1}{yz} = 1 + \frac{2}{y} + \frac{2}{z} + \frac{1}{yz}.$$

Set $S = 2$ (since $S = 1$ is impossible), we get:

$$\frac{2}{y} + \frac{2}{z} + \frac{1}{yz} = 1.$$

Multiply both sides by yz:

$$2z + 2y + 1 = yz \Rightarrow yz - 2y - 2z = 1 \Rightarrow (y-2)(z-2) = 5.$$

This leads to $(y, z) = (3, 7)$ or $(7, 3)$, but since $y < z$, only $(3, 7)$ is valid. Therefore, $(x, y, z) = (1, 3, 7)$.

Case 2: $x = 2$ Similarly, we can check possible values and it leads to $(x, y, z) = (2, 4, 14)$.

Therefore, the corresponding values of (a, b, c) are:

$$(a, b, c) = (2, 4, 8) \quad \text{and} \quad (3, 5, 15).$$

□

Example 2.12

(1998 IMO) Determine all pairs (a, b) of positive integers such that $ab^2 + b + 7$ divides $a^2b + a + b$.

Solution. Consider the expression:

$$xy^2 + y + 7 \mid (x^2y + x + y)y - (xy^2 + y + 7)x = y^2 - 7x.$$

Case 1: $y^2 - 7x > 0$

$$xy^2 + y + 7 \leq y^2 - 7x.$$

Then,

$$(x - 1)y^2 + y + 7x + 7 \leq 0,$$

which is impossible since the left-hand side is positive for $x, y > 0$.

Case 2: $y^2 - 7x = 0$ Then,

$$y = \sqrt{7x}.$$

Let $x = 7m^2$, then $y = 7m$. So,

$$(x, y) = (7m^2, 7m).$$

Case 3: $y^2 - 7x < 0$ Then,

$$\frac{7x - y^2}{xy^2 + y + 7} = k, \quad \text{where } k \in \mathbb{N}.$$

Rewriting,

$$7x - y^2 = kxy^2 + ky + 7k.$$

Thus,

$$(7 - ky^2)x = y^2 + ky + 7k.$$

If $y \geq 3$, then $ky^2 > 7$ implies $7 - ky^2 < 0$, so LHS is negative while RHS is positive — contradiction. Hence, we only consider $y = 1$ or $y = 2$.

Case (i): $y = 1$

$$(7 - k)x = 1 + k + 7k = 1 + 8k,$$

$$(7 - k)(x + 8) = 57.$$

Try integer factorizations of 57: $57 = 1 \cdot 57 = 3 \cdot 19$ Try $(7-k) = 3$, then $k = 4$, and:

$$x + 8 = 19 \Rightarrow x = 11.$$

Also try $(7-k) = 1$, then $k = 6$:

$$x + 8 = 57 \Rightarrow x = 49.$$

So possible solutions: $(x, y) = (11, 1), (49, 1)$.

Case (ii): $y = 2$

$$(7-4k)x = 4 + 2k + 7k = 4 + 9k,$$
$$(7-4k)(4x+9) = 79.$$

Try integer factorizations of 79: 79 is prime, so only $(1, 79)$ or $(79, 1)$.

Try $(7-4k) = 1 \Rightarrow k = 1.5$ (not integer), Try $(7-4k) = 79 \Rightarrow k < 0$ — no valid integer k. So, no solution.

The solutions are:

$$(x, y) = (11, 1), \quad (49, 1), \quad \text{and } (7m^2, 7m).$$

□

Example 2.13

(1984 IMO) Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Prove that if $a + d = 2^k$ and $b + c = 2^m$ for some integers k and m, then $a = 1$.

Solution. Since $ad = bc$, we have

$$a((a+d) - (b+c)) = (a-b)(a-c) > 0.$$

Thus, we have $a+d > b+c, 2^k > 2^m$, and $k > m$. Since $ad = a(2^k - a) = bc = b(2^m - b)$, we obtain $2^m b - 2^k a = b^2 - a^2 = (b-a)(b+a)$. By the equality $2^m(b - 2^{k-m}a) = (b-a)(b+a)$, we infer that $2^m \mid (b-a)(b+a)$. But $b - a$ and $b + a$ differ by $2a$, an odd multiple of 2, so either $b - a$ or $b + a$ is not divisible by 4. Hence, either $2^{m-1} \mid b - a$ or $2^{m-1} \mid b + a$. But $0 < b - a < b < 2^{m-1}$, so it must be that $2^{m-1} \mid b + a$.

Since $0 < b + a < b + c = 2^m$, it follows that $b + a = 2^{m-1}$. That is, $2(a+b) = 2^m = b + c$. Thus, $c = 2a + b$. Furthermore, $\gcd(b, c) = 1$ because both of them are odd and from $b + c = 2^m$, $\gcd(b, c) \mid 2^{m-1}$. If $\gcd(a, b) = k, k \mid c$. Then $k \mid b, c$; but $gcd(b, c) = 1$. Therefore, $k = 1$ and $gcd(a, b) = 1$. Similarly, it can be proved that $gcd(a, c) = 1$. Combining with $ad = bc, a = 1$. □

Example 3.1

(Fermat Prime Conjecture) Pierre de Fermat (1601-1665) stated that all integers in the form $2^{2^n} + 1$ are primes. About a century after Fermat's conjecture, Leonhard Euler (1707-1783) showed that this conjecture was not true. If you were Euler, how would you prove it?
(Hint: It fails at $n = 5$. Prove that $641 \mid 2^{2^5} + 1$.)

Solution. □

Example 3.2

(2000 Russian MO) Evaluate the sum

$$\left\lfloor \frac{2^0}{3} \right\rfloor + \left\lfloor \frac{2^1}{3} \right\rfloor + \left\lfloor \frac{2^2}{3} \right\rfloor + \cdots + \left\lfloor \frac{2^{1000}}{3} \right\rfloor.$$

Solution. □

Example 3.3

(2008 PuMAC) Calculate the last 3 digits of

$$2008^{2007^{2006^{\cdots^{2^1}}}}.$$

Solution. □

Example 3.4

(2003 Romania) Consider the prime numbers $n_1 < n_2 < \cdots < n_{31}$. Prove that if $30 \mid (n_1^4 + n_2^4 + \cdots + n_{31}^4)$, then among these numbers one can find three consecutive primes.

Solution. □

Example 3.5

(2008 St. Petersburg) Given three distinct natural numbers a, b, c, show that

$$\gcd(ab+1, bc+1, ca+1) \leq \frac{a+b+c}{3}.$$

Solution. □

Example 3.6

(1986 IMO) Let d be any positive integer not equal to $2, 5$, or 13. Show that one can find distinct a, b in the set $\{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square.

Solution. □

Example 3.7

(2004 APMO) Prove that
$$\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor$$
is even for every positive integer n.

Solution. Let
$$x = \left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor.$$
For $1 \le n \le 5$, $x = 0$. So, we will consider $n \ge 6$. We will apply **Wilson's Theorem**.

There are three cases:

(i) Both n and $n+1$ are composite Since $\gcd(n, n+1) = 1$, we have $n(n+1) \mid (n-1)!$. Also,
$$v_2((n-1)!) > v_2(n(n+1)),$$
so
$$x = \left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor = \text{even}.$$

(ii) $n = p$ is a prime Then,
$$x = \left\lfloor \frac{(p-1)!}{p(p+1)} \right\rfloor.$$
Obviously, $p+1$ is even and divides $(p-1)!$, and
$$v_2((p-1)!) > v_2(p+1).$$

Let
$$k = \frac{(p-1)!}{p+1} = \text{even}.$$
By Wilson's Theorem:
$$(p-1)! \equiv -1 \pmod{p} \Rightarrow k = \frac{(p-1)!}{p+1} \equiv \frac{-1}{1} \equiv -1 \pmod{p}.$$
Thus,
$$p \mid k+1,$$
which implies $k+1$ is an odd multiple of p. Therefore,
$$\frac{k+1}{p} = \text{odd}.$$
Now observe:
$$\frac{(p-1)!}{p(p+1)} + \frac{1}{p} = \frac{k+1}{p} = \text{odd} \Rightarrow x = \left\lfloor \frac{(p-1)!}{p(p+1)} \right\rfloor = \text{even}.$$

(iii) $p = n + 1$ is a prime Then,

$$x = \left\lfloor \frac{(p-2)!}{(p-1)p} \right\rfloor.$$

Clearly, $p - 1$ is even and divides $(p-2)!$, and

$$v_2((p-2)!) > v_2(p-1).$$

Let

$$k' = \frac{(p-2)!}{p-1} = \text{even}.$$

By Wilson's Theorem:

$$(p-1)! \equiv -1 \pmod p \Rightarrow (p-1)(k') \equiv -1 \pmod p \Rightarrow k' \equiv -1 \pmod p.$$

Thus,

$$p \mid k' + 1 \Rightarrow \frac{k'+1}{p} = \text{odd}.$$

So,

$$\frac{(p-2)!}{(p-1)p} + \frac{1}{p} = \frac{k'+1}{p} = \text{odd} \Rightarrow x = \left\lfloor \frac{(p-2)!}{(p-1)p} \right\rfloor = \text{even}.$$

□

Example 3.8

(2005 IMO) Consider the sequence $a_1, a_2, \ldots$ defined by

$$a_n = 2^n + 3^n + 6^n - 1$$

for all positive integers n. Determine all positive integers that are relatively prime to every term of the sequence.

Solution. By Fermat's Little Theorem, for any prime $p \geq 5$, we have:

$$2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod p$$

Now consider:

$$a_{p-1} \equiv 2^{p-1} + 3^{p-1} + 6^{p-1} - 1 \equiv 1 + 1 + 1 - 1 = 2 \pmod p$$

(This is not congruent to $0 \pmod p$, which is not desirable.)

Next, evaluate:

$$a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$$

Using Fermat's theorem again:

$$= 2^{p-1} \cdot 2^{-1} + 3^{p-1} \cdot 3^{-1} + 6^{p-1} \cdot 6^{-1} - 1 \equiv 1 \cdot 2^{-1} + 1 \cdot 3^{-1} + 1 \cdot 6^{-1} - 1 \pmod p$$

Since:

$$2^{-1} + 3^{-1} + 6^{-1} \equiv \frac{3+2+1}{6} = 1 \pmod p$$
$$a_{p-2} \equiv 1 - 1 = 0 \pmod p$$

Thus, a_{p-2} is divisible by p for all primes $p \geq 5$.

Now consider small terms:

$$a_1 = 10, \quad a_2 = 48, \quad a_3 = 250$$

Note:

$$a_2 = 48 \text{ is divisible by } p = 2, 3$$

Therefore, there is no positive integer that is relatively prime to every term of the sequence. □