MSM Olympiad Training Course (Number Theory)

Phyoe Min Khant

2023 December

Contents

Chapter 1

Divisibility

Contradiction

Contradiction is an important tool in solving number theory problems. Some examples are minimality contradiction, parity (even or odd) contradiction and modular contradiction.

Well Ordering Axiom
Every non-empty set of natural numbers contains a smallest element.

Example 1. Prove that there is no integer in the interval $(0, 1)$.
(Setup: assume that the set A of integers in (0,1) is non-empty and find contradiction.)

Example 2. Prove that $\sqrt{p}$ is irrational for any prime p.
Hint: assume that $\sqrt{p}$ is rational and can be expressed as $\sqrt{p} = \frac{a}{b}$, where $gcd(a, b) = 1, a, b$ are integers.

Theorem 1.1 (Division Algorithm)
For every integer pair a, b, there exists distinct integer quotient and remainders, q and r, that satisfy

$$a = bq + r, 0 \leq r < b$$

Proof.

1. *Existence.* To prove, for every pair (a, b), we can find a corresponding quotient and remainder.
   Setup: Given 2 integers a and b with varying q, consider the set $\{a - bq$ with q an integer and $a - bq \geq 0\}$ and prove that there is quotient q_1 such that $a - bq_1 = r < b$.

2. *Uniqueness.* To prove this quotient and remainder pair is unique.
   Setup: Assume that a can be represented in two ways, $a = bq_1 + r = bq_2 + r_2$, and find contradiction.

Example 3. *(Elements)* Prove that there are infinitely many primes.
(Setup: Assume that the number of primes is finite and find contradiction.)

Example 4. Find 20 consecutive composite numbers.

Theorem 1.2 (Euclidean Algorithm)
For natural numbers a and b, $a > b$,

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

where, k is a positive integer.

Corollary 1.2.1 (Finding 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

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\cdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} \end{aligned}$$

We have

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

Example 5. *(IMO 1959 P1)* Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.

Example 6. Let the integers a_n and b_n be defined by the relationship

$$a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n$$

for all integers $n \geq 1$. Prove that $gcd(a_n, b_n) = 1$ for all integers $n \geq 1$.

Example 7. *(AIME 1985 P13)* The numbers in the sequence $101, 104, 109, 116, \cdots$ are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \cdots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

Example 8. *(AIME 1986 P5)* What is that largest positive integer n for which $n^3 + 100$ is divisible by $n + 10$?

Example 9. *(MMO 2016 Regional)* The sum of the two smallest positive divisors of a positive integer N is 6, while the sum of the largest positive divisors of N is 1122. Find N.

Example 10. *(IMO 2023 P1)* 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 $1 \leq i \leq k-2$.

Theorem 1.3 (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.

Example 11. (a) Express 5 as a linear combination of 45 and 65.

(b) Express 10 as a linear combination of 110 and 380.

Example 12. Suppose you have a 5-liter jug and a 7-liter jug. We can perform any of the following moves:

- Fill a jug completely with water.
- Transfer water from one jug to another, stopping if the other jug is filled
- Empty a jug of water.

The goal is to end up with one jug having exactly 1 liter of water. How do you do this?

Example 13. *(Putnam 2000)* Prove that the expression

$$\frac{gcd(m, n)}{n} \binom{n}{m}$$

is an integer for all pairs of integers $n \geq m \geq 1$.

Divisibility Rules
Let a, b, c be integers.

- The following 5 statements are equivalent.
  1. a divides b.
  2. a is a divisor of b.
  3. a is a factor of b.
  4. $a \mid b$.
  5. $a \cdot k = b$ for some integer k.
- If $c \mid a, b$, then $c \mid ax + by$ for any integers x, y. (possibly negative).
- If $a \mid b$, then either $b = 0$, or $|a| \leq |b|$.
- If $a \mid b$, and $a \mid b$, then $a = \pm b$, i.e., $|a| = |b|$.
- If a prime, $p \mid ab$, then p divides either a or b.
- *(Euclid's Lemma)* If $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.

Euclid's Lemma Proof. Use Bezout's Identity.

Example 14. *(MMO 2015 National)* Prime numbers p, q and positive integers m, n satisfy the following conditions:

$$m < p, n < q \text{ and } \frac{p}{m} + \frac{q}{n} \text{ is an integer.}$$

Prove that $m = n$.

Example 15. Prove that if p is a prime and $0 < k < p$, then $\binom{p}{k}$ is divisible by p.

Example 16. *(St. Petersburg 1996)* Find all positive integers n such that

$$3^{n-1} + 5^{n-1} \mid 3^n + 5^n.$$

Example 17. *(IMO 1992 P1)* 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 18. *(IMO 1998 P4)* Determine all pairs (a, b) of positive integers such that $ab^2 + b + 7$ divides $a^2b + a + b$.

Chapter 2

Fundamental Theorem of Arithmetic

Theorem 2.1 (Fundamental Theorem of Arithmetic)
Every integer $n \geq 2$ has a unique prime factorization.

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

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

Proof. Both existence and uniqueness can be proved by induction.

Theorem 2.2 (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,

$$gcd(a,b) = p_1^{min(e_1,f_1)} p_2^{min(e_2,f_2)} \cdots p_k^{min(e_k,f_k)}$$

$$lcm(a,b) = p_1^{max(e_1,f_1)} p_2^{max(e_2,f_2)} \cdots p_k^{max(e_k,f_k)}$$

Corollary 2.2.1
For $a, b \in \mathbb{Z}^+, gcd(a,b) \cdot lcm(a,b) = ab$.

Example 1. *(AIME 1998 P1)* For how many values of k is 12^{12} the least common multiple of the positive integers 6^6 and 8^8, and k?

Example 2. *(AIME 1987 P7)* Let $[r, s]$ denote the least common multiple of positive

integers r and s. Find the number of ordered triples (a, b, c) of positive integers for which $[a, b] = 1000$, $[b, c] = 2000$, and $[c, a] = 2000$.

Theorem 2.3 (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,

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

Example 4. *(AMC8 2015 P22)* On June 1, a group of students are standing in rows, with 15 students in each row. On June 2, the same group is standing with all of the students in one long row. On June 3, the same group is standing with just one student in each row. On June 4, the same group is standing with 6 students in each row. This process continues through June 12 with a different number of students per row each day. However, on June 13, they cannot find a new way of organizing the students. What is the smallest possible number of students in the group?

Example 5. A new school has exactly 2023 lockers and 2023 students. On the first day of school, the first student enters the school and opens all the lockers. The second student then enters and closes every locker with an even number. The third student will reverse every third locker. (If the locker is closed, it will be opened and vice versa.) The fourth student will reverse every fourth locker and so on, until all 2023 students have entered and reversed the respective lockers. How many lockers will be open at the end?

Example 6. *(AIME 1988 P5)* Find the probability that a randomly chosen positive divisor of 10^{99} is an integer multiple of 10^{88}.

Example 7. *(AIME 1990 P5)* Let n be the smallest positive integer that is a multiple of 75 and has exactly 75 positive integral divisors, including 1 and itself. Find

$\frac{n}{75}$.

Example 8. *(AIME 1995 P6)* Let $n = 2^{31}3^{19}$. How many positive integer divisors of n^2 are less than n but do not divide n?

Example 9. *(AIME I 2005 P3)* How many positive integers have exactly three proper divisors (positive integral divisors excluding itself), each of which is less than 50?

Example 10. *(AIME I 2005 P12)* For positive integers n, let $\tau(n)$ denote the number of positive integer divisors of n, including 1 and n. For example, $\tau(1) = 1$ and $\tau(6) = 4$. Define $S(n)$ by $S(n) = \tau(1) + \tau(2) + \cdots + \tau(n)$. Let a denote the number of positive integers $n \leq 2005$ with $S(n)$ odd, and let b denote the number of positive integers $n \leq 2005$ with $S(n)$ even. Find $|a - b|$.

Chapter 3

Modular Arithmetic

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

- 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.
- *(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 $a^n \equiv b^n \pmod{m}$.

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 $641 \mid 2^{2^5}$.)

Example 1. Find the remainder when 6^{2023} is divided by 37.

Example 2. *(AIME I 2010 P2)* Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999\text{ 9's}}$ is divided by 1000.

Example 3. Prove that $7 \mid 3^{2n+1} + 2^{n+2}$ for all natural numbers n.

Example 4. Prove that $7 \mid 2222^{5555} + 5555^{2222}$.

Example 5. Find the units digit of 7^{7^7}.

Example 6. Prove that every year, including any leap year, has at least one Friday 13th.

Example 7. For what values of n, $2^n + 27$ is divisible by 7.

Example 8. Find all positive integer pairs (x, y) such that $x^3 = 2^y + 15$.

Example 9. Suppose k is a non-negative integer. Prove that $2^k - 5$ never leaves remainder 1 when divided by 7.

Example 10. *(AIME 1994 P1)* The increasing sequence $3, 15, 24, 48, \ldots$ consists of those positive multiples of 3 that are one less than a perfect square. What is the remainder when the 1994th term of the sequence is divided by 1000?

Example 11. *(USAMO 1979 P1)*Determine all non-negative integral solutions $(n_1, n_2, \ldots, n_{14})$ if any, apart from permutations, of the Diophantine Equation

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

Example 12. *(AIME II 2016 P11)* For positive integers N and k, define N to be k-nice if there exists a positive integer a such that a^k has exactly N positive divisors. Find the number of positive integers less than 1000 that are neither 7-nice nor 8-nice.

Theorem 3.1 (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

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Corollary 3.1.1 (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

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

Example 1. Find $2^{98} \pmod{33}$.

Example 2. *(AIME 1983 P6)* Let $a_n = 6^n + 8^n$. Determine the remainder on dividing a_{83} by 49.

Example 3. Define $f(x) = x^{x^{x^x}}$. Find the last two digits of $f(2023)$.

Linear Congruence

- *(Inverses)* 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)* $\frac{a}{m} + \frac{b}{n} \equiv a \cdot m^{-1} + b \cdot n^{-1} \equiv ay + bx \cdot (mn)^{-1} \equiv \frac{an+bm}{mn}$.
- *(Inverses multiply like fractions)* $\frac{a}{m} \cdot \frac{b}{n} \equiv (a \cdot m^{-1}) \cdot (b \cdot n^{-1}) \equiv ab \cdot (mn)^{-1} \equiv \frac{ab}{mn}$.

References

1. Aditya Khurmi. (2020) Modern Olympiad Number Theory.
2. Stevens, Justin. (2013). Olympiad Number Theory Through Challenging Problems (3rd Ed).
3. Yu Hong-Bing. (2010). Problems of Number Theory in Mathematical Competitions. World Scientific.
4. Titu Andreescu, Dorin Andrica, Zuming Feng. (2006). 104 Number Theory Problems: From the Training of the USA IMO Team.
5. David A. Santos. (2005). Number Theory for Mathematical Contests.
6. Mathew Crawford. Introduction to Number Theory (2nd edition). Art of Problem Solving.
7. Art of Problem Solving Website. https://artofproblemsolving.com.
8. OmegaLearn.org. Mastering AMC10/12.