An Olympiad Notebook

a journey into olympiad mathematics

Adyansh Mishra

March 5, 2024

Contents

Preface
Not a Book, • Acknowledgments, • Notation,

I Number Theory 1

2 1 Divisibility
Basic Properties, 2 • Euclid's Division Lemma, 4 • Primes, 4 • GCD and LCM, 5 • Coprime, 6 • Infinitude of Primes, 7

II Appendices 8

9 Functions
The theory, 9

Preface

§1 Not a Book

This is a collection of notes written by me on all of the four subjects included in mainstream olympiads. Much of the contents is sourced from a various plethora of free and paid books.

This is not meant to be a one-spot go to for all your Olympiad preparation, even though I have tried to include every bit of information I could get my hands on. One important part that is missing from it are problems. The Primary reason for that being my laziness and the fact and these are meant to be my *notes*, which shall capture my Olympiad journey. This is not an olympiad go-to book. Be aware

§2 Acknowledgments

> **Remark 2.1.** Write acknowledgments and attribute licenses. Also change many examples except the free ones. Later edit some theory to ensure no book is being mimicked.

§3 Notation

- $\mathbb{N} = \{1, 2, 3 \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$

Part I

Number Theory

CHAPTER 1

Divisibility

"Give him threepence, since he must gain out of what he learns"
– Euclid of *Alexandaria*

Motivation: The easier it is, the grander its uses are.

§1.1 Basic Properties

Definition 1.1.1 (Division)
The operation division is defined as:

1. An integer y is said to be a multiple of x if
$$y \in \{kx : k \in \mathbb{Z}\}$$
2. If y is a multiple of x then, y is *divisible* by x and x divides y which is written as:
$$x \mid y.$$

Proposition 1.1.2 — Let $x, y, z \in \mathbb{Z}$

1. $\forall x \neq 0$, $x \mid x$ and $x \mid 0$.
2. $1 \mid x$.
3. $x \mid y$ and $y \mid z \implies x \mid z$.
4. $x \mid y \iff \dfrac{y}{x} \in \mathbb{Z}$

Most of the proofs here are trivial, but let us show that using the last proposition we can prove the third one.

Proof. $x \mid y \iff \dfrac{y}{x} \in \mathbb{Z}$ and $y \mid z \iff \dfrac{z}{y} \in \mathbb{Z}$. But $\dfrac{z}{x} = \dfrac{y}{x} \cdot \dfrac{z}{y} \in \mathbb{Z} \iff x \mid z$. □

We may note that because of the definition of division, we get the following theorem:

Theorem 1.1.3

If $x \mid y$, then either $|y| \geq |x|$ or $y = 0$.

The 0 case is extremely important and often hard to see. Remember to look out for this case.

Proof. $|y| = |k \cdot x| = |k| \cdot |x|$. But, $|k| \cdot |x| \geq |x| \iff |y| \geq |x|$. Note here that k is not taken to be 0 since, $y = k \cdot x = 0 \cdot x = 0$. But this case is already mentioned. □

The following is not of a severe importance in the view that it is hard to see or prove. But it allows us to quickly formalise our solutions and is thus useful for proofs.

Lemma 1.1.4

If $x \mid a$, then $x \mid ac + b \iff x \mid b$.

Proof. The proof is trivial as, $x \mid a \iff a = kx : k \in \mathbb{Z}$.

Direction 1 Note, $x \mid ac+b \iff ac+b = nx : n \in \mathbb{Z}$, hence, $b = nx - ac = nx - kcx = (n-kc)x \iff x \mid b$.

Direction 2 And, $x \mid b \iff b = mx : m \in \mathbb{Z}$, hence, $ac + b = kcx + mx = (kc + m)x \iff x \mid ac + b$. □

Finally, we may conclude this section of properties by stating all the previous properties and some more.

Theorem 1.1.5

Let x, y, $z \in \mathbb{Z}$

1. $\forall x \neq 0$, $x \mid x$ and $x \mid 0$.
2. $1 \mid x$.
3. $x \mid y$ and $y \mid z \implies x \mid z$.
4. $x \mid y \iff \dfrac{y}{x} \in \mathbb{Z}$.
5. $\forall z \neq 0$, $x \mid y \iff xz \mid yz$.
6. $x \mid a$, $x \mid b \implies x \mid an + bm$.
7. $x \mid y$, $y \mid x \iff y = \pm x$.
8. $x \mid y \implies x \mid yz$.

Example 1.1.6

Show that if $n \in \mathbb{Z}, n > 1$, then $n \nmid 2n^2 + 3n + 1$.

Proof. Here we can see the use of Lemma 1.1.4. Suppose $n \mid 2n^2 + 3n + 2$, then $n \mid 2n^2 + 3n$, and $n \mid 2n^2 + 3n + 1 \iff n \mid 1$. But, $n \mid 1 \implies |1| \geq |n| \iff 1 \geq n$ which contradicts our earlier statement that $n > 1$. Hence, $n \nmid 2n^2 + 3n + 1$. □

Remark 1.1.7. $|1| \geq |n| \iff 1 \geq n$ because $n > 1 > 0$.

Example 1.1.8

Show that for any two natural numbers, a, $b : a > b$, $a \nmid 2a + b$.

Proof. Again, we can use Lemma 1.1.4. Suppose $a \mid 2a + b$, then $a \mid 2a$ and $a \mid 2a + b \iff a \mid b$. But, $a \mid b \implies |b| \geq |a|$ and $a, b \in \mathbb{N} \implies b \geq a$. This contradicts our the fact $a > b$. Hence $a \nmid 2a + b$. □

§1.2 Euclid's Division Lemma

Euclid's division lemma is something we will make much use of, especially later. For now the unproven statement shall suffice.

Theorem 1.2.1

For any integers a, b, we can find *unique* integers q, r, such that:

$$b = aq + r, \quad 0 \leq r < a.$$

Here, r is called the remainder, and q is called the quotient.

§1.3 Primes

Definition 1.3.1 (Primes)

Any $x \in \mathbb{N}$ is called a prime, if and only if it has exactly 2 *divisors*.

Primes are a very interesting subset of naturals. There properties will be explored later. For now, we use primes to define one of the most important theorem in all of number theory.

§1.3.1 Fundamental Theorem of Arithmetic

Theorem 1.3.2 (Fundamental Theorem of Arithmetic)

Any natural number can be *uniquely* expressed as a product of primes upto order.

By uniquely, we mean there is *at most* and *at least* one way to express any natural as a product of primes. The order in which the product is expressed is irrelevant because of the commutativity of multiplication.

We can further extend this theorem to include all integers by using some claims.

§1.3.2 Integers as Multisets

Claim 1.3.3 — Any non-zero $x \in \mathbb{Z}$ can be expressed a multiset of primes(and -1). If the number is positive, then we can simply use Theorem 1.3.2 and included all the prime factors in its multiset. If the number is negative, then we express it as the multiset of its absolute value and include -1 in the multiset.

Remark 1.3.4. A *multiset* is a set where repeating elements are counted seperately. Each element has a *mulitplicity* which indicates the number of times that element appears in the multiset.

We could, for example, express 20 as $\{2, 2, 5\}$, and -20 as $\{-1, 2, 2, 5\}$.
This allows us to restate Theorem 1.3.2.

Theorem 1.3.5 (Fundamental theorem of Arithmetic in multisets)
Any natural number can expressed as a multiset of primes.

Remark 1.3.6. This multiset, is, by definition *unique*.

It also allows us to restate divisibility for positive integers.

Theorem 1.3.7 (Divisibility in multisets)
$\forall a, b \in \mathbb{N}$,

$$a \mid b \iff A \subseteq B$$

Remark 1.3.8. Henceforth, all variables are integers unless explicitly mentioned.

§1.4 GCD and LCM

§1.4.1 GCD

Definition 1.4.1
$\gcd(a, b)$ is the multiset of all *common* prime factors of a and b.

This gives us the following properties of gcd.

Proposition 1.4.2 —

- $\gcd(a, b)$ is the greatest integer which divides both a and b. In particular, $\gcd(a, b) \leq a, b$.
- $c \mid a$, $c \mid b \iff c \mid \gcd(a, b)$.

We can, in fact, show that the two definition of gcd are equivalent.

Proof. Let $\mathcal{C} = \{p : p \mid a, b \text{ and } p \text{ is a prime}\}$. Suppose that $\gcd(a, b) \neq \mathcal{C}$. Then $\gcd(a, b) > \mathcal{C}$.

Note that $\gcd(a, b)$ must contain an element $x \notin \mathcal{C}$ where x is prime.(Since it is an element in the multiset of $\gcd(a, b)$).
But, $x \in \gcd(a, b) \iff x \mid \gcd(a, b)$, and $x \mid \gcd(a, b)$, $\gcd(a, b) \mid a, b \implies x \mid a, b$. x is prime, and $x \mid a, b \implies x \in \mathcal{C}$. This contradicts our earlier deduction that $x \notin \mathcal{C}$. By *reductio ad absurdum*, we have $\gcd(a, b) = \mathcal{C}$. □

Claim 1.4.3 — Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$. Then,

$$\gcd(a, b) = p_1^{\min(\beta_1, \alpha_1)} p_2^{\min(\beta_2, \alpha_2)} \dots p_n^{\min(\beta_n, \alpha_n)}$$

Where, $\alpha_i, \beta_i \in \mathbb{N}_0$.

This is simply a consequence of the definition of gcd.

Definition 1.4.4 (GCD)
We may now state that the following are equivalent.

- $\gcd(a,b) = A \cap B$
- $\gcd(a,b)$ is the greatest integer which divides both a and b. In particular, $\gcd(a,b) \leq a, b$.
- Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$. Then,

$$\gcd(a,b) = p_1^{\min(\beta_1,\alpha_1)} p_2^{\min(\beta_2,\alpha_2)} \dots p_n^{\min(\beta_n,\alpha_n)}$$

  Where, $\alpha_i, \beta_i \in \mathbb{N}_0$.

§1.4.2 LCM

Definition 1.4.5 (LCM)
The following three definitions are equivalent.

- $\operatorname{lcm}(a,b) = A \cup B$
- $\operatorname{lcm}(a,b)$ is the least number divisible by both a and b. Particularly, $\operatorname{lcm}(a,b) \geq a, b$.
- Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$. Then,

$$\operatorname{lcm}(a,b) = p_1^{\max(\beta_1,\alpha_1)} p_2^{\max(\beta_2,\alpha_2)} \dots p_n^{\max(\beta_n,\alpha_n)}$$

From the definitions of gcd and lcm we obtain the following very important theorem.

Theorem 1.4.6

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

Proof.

$$\begin{aligned}\gcd(a,b) \cdot \operatorname{lcm}(a,b) &= p_1^{\min(\alpha_1,\beta_1)+max(\alpha_1,\beta_1)} \dots p_n^{(\max(\alpha_n,\beta_n)+\min(\alpha_n,\beta_n))} \\ &= p_1^{\alpha_1+\beta_1} \dots p_2^{\alpha_n+\beta_n} \\ &= a \cdot b\end{aligned}$$

□

§1.5 Co-prime

Definition 1.5.1
Two numbers, a, b are called co-prime if $\gcd(a,b) = 1$.

Definition 1.5.2
A number x is pairwise co-prime to n other numbers $p_1, p_2 \dots p_n$, if $\gcd(x,p_1) = \gcd(x,p_2) \dots = \gcd(x,p_n) = 1$.

§1.6 Infinitude of Primes

Theorem 1.6.1 (Euclid)
There are infinitely many primes.

Proof. Let there be finitely many primes, $\{p_1, p_2 \dots, p_n\}$. Define N as $p_1 p_2 \dots p_n + 1$.
Note that N is pairwise co-prime to all, $p_1 p_2 \dots p_n$ because if $p_i \in \{p_1, p_2 \dots, p_n\} \mid N$ and $p_i \mid p_1 p_2 \dots p_n \iff p_i \mid 1$. But, $p_i \in \mathbb{N} \implies p_i = 1$ which is absurd.

Since $N \in \mathbb{N}$, N must have a prime factor, p because of Theorem 1.3.2. And $p \notin \{p_1, p_2 \dots, p_n\}$ because N is pairwise co-prime to all primes in $\{p_1, p_2 \dots, p_n\}$. This contradicts our assumption that $\{p_1, p_2 \dots, p_n\}$ was the set of all primes, proving that there are infintely many primes.

□

Add motivation fo stuff

Part II

Appendices

APPENDIX A

Functions

§A.1 The theory

Yeah so?