# Common Core 5th Grade Curriculum

Albert Ye

August 25, 2023

## 1 Lecture 1

**Definition 1**

An integer $p \neq 0, 1, -1$ is **prime** if the only integers which divide $p$ are $\pm 1$ and $\pm p$.

Recall that the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

**Theorem 2** (Twin Prime Conjecture)

There are infinitely many $p \in \mathbb{N}$ such that $p$ is prime and $p + 2$ is prime.

Yitang Zhang proved bounded gaps between primes, so there are infinitely many prime $p, p + N$.

**Theorem 3** (Goldbach Conjecture)

Every even number can be written as the sum of two primes.

Vinagradar proved that every odd number can be written as the sum of 3 primes. The proof should use something called sieves.

**Proposition 4**

There are infinitely many primes.

*Proof.* Suppose not and $p_1, \ldots, p_n$ are all the primes. Then, let $p_1 \cdots p_n + 1 = N$.

As we will see, every integer admits a unique decomposition into a product of primes. □

### 1.1 Counting Primes

Let $\pi(x) : N \to \mathbb{N}$ return the number of primes $p$ such that $0 < p < x$.

Then, $\pi(x)$ is unbounded: $\lim_{x\to\infty} \pi(x) = \infty$.

**Theorem 5** (Prime Number Theorem)

$$\lim \frac{\pi(x)}{x/\log x} = 1.$$

In other words, $\pi(x) \to \frac{x}{\log x}$¿

A better approximation is $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. The error for $\mathrm{Li}(x)$ is $|\pi(x) - \mathrm{Li}(x)| = O(\log x\sqrt{x})$.

### 1.2 Prime Factorization

**Theorem 6** (Uniqueness of Prime Factorization)

Every integer $0 \neq n \in \mathbb{Z}$ can be written as

$$n = (-1)^{Z(n)} \prod_{p \text{ prime}} p^{a_p} \qquad a_p \in \mathbb{N},$$

where all but finitely many $a_p$ are zero, $\epsilon(n) = \begin{cases} 0 & n > 0 \\ 1 & n < 0 \end{cases}$.

To prove this, we first look at a lemma:

**Lemma 1.2.1**

If $a, b \in \mathbb{Z}$ and $b > 0$, there exist integers $q, r$ such that $a = qb + r$ and $0 \leq r < b$.

*Proof.* Consider the set of integers of the form $\{a - xb | x \in \mathbb{Z}\} = S$. The set $S$ contains infinitely many positive integers, so contains a least positive integer $r = a - qb$.

**Remark 7**

This property does not hold for $S \subset \mathbb{Q}$. Consider $S = \{1, \frac{1}{2}, \frac{1}{4}, \ldots\}$.

□

The rest of the proof will follow later.

**Definition 8**

Let $a_1, \ldots, a_n$ be integers. Denote $(a_1, \ldots, a_n)$ to be the set $\{b_1 a_1 + \cdots + b_n a_n | b_i \in \mathbb{Z}\}$.

# 2 Lecture 2

## 2.1 Prime Factorization, cont.

Recall the theorem of uniqueness of prime factorizations. Also recall that a prime number $p$ is an integer $\neq 0$, so that the only divisors of $p$ are $\pm 1$ and $\pm p$.

**Definition 9**

If $0 \neq a \in \mathbb{Z}$ and $p \in \mathbb{Z}$ is prime, let $\operatorname{ord}_p a$ denote the largest integer $n$ such that $p^n | a$, i.e. $a = p^n b$.

We define $\operatorname{ord}_p 0 = \infty$.

**Lemma 2.1.1**

If $a, b \in \mathbb{Z}$, then there exists $d \in \mathbb{Z}$ such that $(d) = (a, b)$. Recall Definition 8 for $(a_1, a_2, \ldots, a_n)$.

*Proof.* Let $d$ be the smallest integer $> 0$ in $(a, b)$. We claim that $(d) = (a, b)$. As $d \in (a, b)$, we see that $(d) \subseteq (a, b)$. We have to show that $(a, b) \subseteq (d)$.

Take $c \in (a, b)$, then we see from 1.2.1 that $c = qd + r$ with $0 \leq r < d$. THen $r = c - qd \in (a, b)$. By minimality of $d$, we see that $r = 0$, so $c = qd$ implie $c \in (d)$. □

**Definition 10**

If $a, b \in \mathbb{Z}$, then a greatest common divisor $d$ of $a, b$ is an integer which divides $a, b$ such that any other integer $c$ with that property satisfies $c|d$.

**Remark 11**

If we insist $d \geq 0$, then it is unique. Because if $c, d \geq 0$ are both $\gcd(a, b)$, then $c|d$ and $d|c$, which implies $c = \pm d$, but because of positivity we must have $c = d$.

**Proposition 12**

If $a, b \in \mathbb{Z}$, then the $d$ appearing in 2.1.1 s.t. $d = (a, b)$ is a greatest common divisor of $a, b$.

*Proof.* If $(d) = (a, b)$, then $a \in (d) = d\mathbb{Z} \implies d|a$. If $c \in \mathbb{Z}$ is any common divisor of $a$ and $b$, then $c$ divides $an + bm$ for all $m, n \in \mathbb{Z}$. As $d \in (a, b)$, $d$ has this form, so $c|d$.

Thus, by definition, $d$ must be the greatest common divisor. $\square$

**Definition 13**

We say that $a, b \in \mathbb{Z}$ are **relatively prime** if $(a, b) = 1$.

In other words, the only nonzero integers that divide $a$ and $b$ are $\pm 1$.

**Lemma 2.1.2**

Suppose $a|bc$, and $(a, b) = 1$. Then, $a|c$.

*Proof.* $(a, b) = 1$ implies $1 = an + bm$ for some $n, m$. So $c = acn + bcm$. Notice that the right term contains $bc$ and the left term contains $a$, so $c$ must be divisible by $a$. $\square$

**Corollary 14**

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

*Proof.* If $(p, a) = p$, then we're done as $p|a$.

Suppose instead that $(p, a) = 1$. From 2.1.2, we have $p|b$. $\square$

We take the contrapositive to see that if a prime $p$ doesn't divide $a$ or $b$, then it doesn't divide $ab$.

**Proposition 15**

Fix a prime $p$. If $a, b \in \mathbb{Z}$, then $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$.

*Proof.* Let $\operatorname{ord}_p a = n, \operatorname{ord}_p b = m$. Then, we see that $a = p^n c, b = p^m d$ where $p \nmid c, p \nmid d$. So $ab = p^n c \cdot p^m d = p^{n+m}(cd)$. We know that $p$ cannot divide $cd$ from 14, so $\operatorname{ord}_p ab = n + m$. $\square$

Now, we can finally prove Theorem 6.

*Proof of 6.* Fix $n \in \mathbb{Z}$ and suppose that $n = (-1)^{\epsilon(n)} \prod_p p^{a_p}$.

Then, fix a prime $q$. We see that

$$\operatorname{ord}_q n = 0 + \sum_p a_p \operatorname{ord}_q p = a_q.$$

This is because $\operatorname{ord}_q p = \begin{cases} 1 & q = p \\ 0 & q \neq p \end{cases}$. This implies that the only factors that will contribute to $\operatorname{ord}_q n$ are the terms of $q$, of which there are $a_q$.

Hence, $a_p$ for each prime $p$ is determined solely by $n$, so the prime factorization is unique. $\square$