

# Common Core 5th Grade Curriculum

ALBERT YE

September 1, 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  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ ,  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ .

### 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.

Vinogradar 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  $p_1, \dots, p_n$  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  $\pi(x) : \mathbb{N} \rightarrow \mathbb{N}$  return the number of primes  $p$  such that  $0 < p \leq x$ .

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

### Theorem 5 (Prime Number Theorem)

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x} = 1.$$

In other words,  $\pi(x) \sim \frac{x}{\log x}$ .

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

## 1.2 Prime Factorization

### Theorem 6 (Uniqueness of Prime Factorization)

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

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

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  $S = \{1, \frac{1}{2}, \frac{1}{4}, \dots\}$ .

□

The rest of the proof will follow later.

#### Definition 8

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

## 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  $\text{ord}_p a$  denote the largest integer  $n$  such that  $p^n | a$ , i.e.  $a = p^n b$ .

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

#### 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  $(a_1, a_2, \dots, a_n)$ .

*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  $c = qd$  implies  $c \in (d)$ . □

**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. □

**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  $a$ . □

**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  $p|b$ . □

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  $\text{ord}_p ab = \text{ord}_p a + \text{ord}_p b$ .

*Proof.* Let  $\text{ord}_p a = n, \text{ord}_p b = m$ . 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  $\text{ord}_p ab = n + m$ . □

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

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

This is because  $\text{ord}_q p = \begin{cases} 1 & q = p \\ 0 & q \neq p \end{cases}$ . This implies that the only factors that will contribute to  $\text{ord}_q n$  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.  $\square$

### 3 Lecture 3

#### Lemma 3.0.1

Every nonconstant irreducible polynomial has a factorization into nonconstant irreducible polynomials.

### 4 Lecture 4

#### 4.1 Factorization of Polynomials

Recall 3.0.1 from last lecture.

Again let  $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ .

#### Definition 16

A nonzero polynomial is called **monic** if the coefficient of its leading term is 1.

#### Definition 17

If  $p(x) \in k[x]$  is nonconstant irreducible, and  $0 \neq q(x) \in k[x]$  is any other polynomial. Let  $\text{ord}_p q$  be defined as the greatest integer  $n \geq 0$  such that  $p^n(x) | q(x)$  but  $p^{n+1}(x) \nmid q(x)$ .

#### Theorem 18

Every nonconstant polynomial  $g(x)$  admits a unique factorization of the form  $g(x) = c \prod_{p(x)} p(x)^{a_p}$ , where  $c \in k^\times = k \setminus \{0\}$  and the product is over all irreducible, nonconstant, monic polynomials.

Then,  $a_p = \text{ord}_p g$ , and  $c$  is the leading term of  $g$ .

We start with the following lemma:

#### Lemma 4.1.1

If  $f(x), g(x) \in k[x]$  are polynomials with  $0 \neq g(x)$  then we can find polynomials  $q(x)$  and  $r(x)$  with either  $r(x) = 0$  or  $0 \leq \deg r(x) < \deg g(x)$  s.t.  $f(x) = q(x)g(x) + r(x)$ .

*Proof.* If  $g|f$ , then  $g(x)q(x) = f(x)$  for some  $q(x)$ , and let  $r(x) = 0$ . Suppose otherwise, and  $f \neq 0$ . Consider the set  $f(x) \in \{f(x) - h(x)g(x), h(x) \in k[x]\}$ , and let  $q(x)$  be such that  $r(x) = f(x) - q(x)g(x)$  is of least degree in this set.

It remains to show  $r = 0$  or  $\deg r < \deg g$ . Suppose otherwise, and that  $r(x)$  has leading term  $ax^d$  and  $g(x)$  has leading term  $bx^n$  with  $d \geq n$ . Let  $m(x) = \frac{a}{b}x^{d-n}g(x)$ . Then  $m(x)$  is a polynomial such that  $\deg(r(x) - m(x)) < \deg r(x)$ .

However,  $r(x) - m(x) = f(x) - (q(x) + \frac{a}{b}x^{d-n}g(x))g(x)$ , so  $r(x) - m(x) \in S$ . This contradicts the definitions of  $r(x)$ .  $\square$

#### Definition 19

If  $f_1(x), \dots, f_n(x)$  are polynomials, let  $(f_1, f_2, \dots, f_n)$  be defined similarly to integers.

**Lemma 4.1.2**

Given  $f(x), g(x) \in k[x]$ , there is a  $d(x) \in k[x]$  s.t.  $(f, g) = (d)$ .

*Proof.* Let  $d(x)$  be a polynomial of least degree in  $(f, g)$ . We have  $(d) \subset (f, g)$ . Let  $c(x) \in (f, g)$ . Then, if  $d|c$ , we're done. If not, then there exists  $q(x), r(x)$  s.t.  $c(x) = q(x)d(x) + r(x)$ , with  $\deg r(x) < \deg d(x)$ . Then  $r(x) = c(x) - q(x)d(x) \in (f, g)$ , which is a contradiction as  $\deg r < \deg d$ .  $\square$

## 5 Lecture 5

Continue proving 18.

**Definition 20**

We say  $f(x), g(x) \in k[x]$  are **relatively prime** if  $(f, g) = 1$ .

**Definition 21**

A greatest common divisor, or gcd of  $f$  and  $g \in k[x]$  is a polynomial  $d(x)$  which divides  $f$  and  $g$  and has the property that if  $c(x) \in k[x]$  divides  $f$  and  $g$  then  $c|d$ . (Ambiguous up to a scalar.)

**Lemma 5.0.1**

If  $f$  and  $g$  are relatively prime and  $f|gh$ , then  $f|h$ .

*Proof.* If  $(f, g) = 1$  then  $1 = a(x)f(x) + b(x)g(x)$ . So  $h(x) = a(x)f(x)h(x) + b(x)g(x)h(x) = f(x)(a(x)h(x) + b(x)j(x))$  for some other polynomial  $j(x)$ . Then,  $f(x)|h(x)$ .  $\square$

If  $d(x) = (f(x), g(x))$  and  $x \in k^*$  then  $\alpha d$  is also a gcd of  $f$  and  $g$ ;  $(\alpha d) = (d)$ .

Now, recall that a nonconstant polynomial  $f(x)$  is **irreducible** if its only divisors are of the form  $\alpha f$  or  $\alpha$  ( $\alpha \in k^*$ ); i.e. if any polynomial divides  $f$ , it's either a scalar or a scalar multiple of  $f$ .

**Lemma 5.0.2**

If  $p(x)$  is irreducible and  $p|fg$ , then  $p|f$  or  $p|g$ .

*Proof.*  $(p, f) = (1)$  or  $(p) = (\alpha p)$  for all  $x \in k^*$ . If  $(p, f) = (p)$ , then  $p|f$ . Otherwise,  $(p, f) = (1)$ , so from Lemma 5.0.1 we have  $p|g$ .  $\square$

**Definition 22 (Order in Polynomial Terms)**

If  $p$  is a nonconstant polynomial and  $g \neq f \in k[x]$  then  $\text{ord}_p f$  is the largest  $a \in \mathbb{Z}_{\geq 0}$  such that  $p^a|f$ .

**Lemma 5.0.3**

If  $p(x) \in k[x]$  is irreducible and  $a, b \in k[x]$ , then  $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$ .

Finally, we can prove 18.

*Proof.* Write  $0 \neq f(x) = c \prod_p p(x)^{a_p}$ . For every monic irreducible polynomial  $q$ ,  $\text{ord}_q f = \sum_p a_p \text{ord}_q p$ , and we see that  $\text{ord}_q p = \begin{cases} 1 & q = p \\ 0 & q \neq p. \end{cases}$  This must be  $a_q$ .

The scalar  $c$  is the leading coefficient of  $f$ , so every polynomial factorization uniquely determines one polynomial.  $\square$