Common Core 5th Grade Curriculum

Albert Ye

September 11, 2023

1 Lecture 1

Definition 1

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

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

$\square$

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 $\{b_1 a_1 + \cdots + b_n a_n | b_i \in \mathbb{Z}\}$.

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 ± 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 $(a_1, a_2, \dots, a_n)$.

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 $c = qd$ implie $c \in (d)$. $\square$

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

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 $\operatorname{ord}_p ab = n + m$. □

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. □

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 $\operatorname{ord}_p q$ be defined as the greatest integer $n \geq 0$ such that $p^n(x)|g(x)$ but $p^{n+1}(x) \not| g(x)$.

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 $c \in k^x = k \setminus \{0\}$ and the product is over all irreducible, nonconstant, monic polynomials.

Then, $a_p = \operatorname{ord}_p g$, 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 $m9x) = \frac{a}{b}x^{d-n}g(x)$. Then $m(x)$ is a polynomial such that $\deg(r(x) - m(x)) < \deg r(x)$.

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

Definition 19

If $f_1(x), \ldots, f_n(x)$ are polynomials, let $(f_1, f_2, \ldots, f_n)$ 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 $x \in k^x$ then αd is also a gcd o f and g; $(\alpha d) = (d)$.

Now, recall that a nonconstant polynomial $f(x)$ is **irreducible** if its only divisors are of the form αf or α ($\alpha \in k^*$); 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 $\operatorname{ord}_p f$ 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 $\operatorname{ord}_p(ab) = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$.

Finally, we can prove 18.

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

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

6 Lecture 6

Proposition 23

If $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (any field) then $k[x]$ contains infinitely many irreducible polynomials.

Proof. Suppose not, and $p_1(x), \dots, p_n(x)$ exhaust the irreducible polynomials. Thus $q(x) = 1 + p_1(x)p_2(x)\cdots p_n(x)$ is a polynomial not divisible by the $p_i(x)$, but it must factor into a product of the $p_i(x)$, a contradiction. □

Lemma 6.0.1

Every integer $n \neq 0$ can be written as $n = ab^2$ where a is squarefree.

Definition 24

An integer $n \neq 0$ is squarefree if it isn't divisible by the square of any prime.

Proof. If $|n| = 1$ then it's squarefree. If $|n| > 1$ then $n = (-1)^{\epsilon(n)} p_1^{2a_1+b_1} \cdots p_m^{2a_m+b_m}$, where b_i is either 0 or 1 for all i. Then, in turn,

$$n = [p_1^{2a_1} \cdots p_m^{2a_m}][(-1)^{\epsilon(n)} p_1^{b_1} \cdots p_m^{b_m}].$$

We see that the first term is b^2 and the second term is a squarefree a. □

Definition 25

$\nu(n)$ =number of positive divisors

$\sigma(n)$ =sum of positive divisors

Proposition 26

Let $n \in \mathbb{Z}_{>1}$ have a prime factorization $n = p_1^{a_1} \cdots p_m^{a_m}$. Then,

- $\nu(n) = (a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$
- $\sigma(n) = \left(\sum_{i=0}^{a_1} p_1^i\right) \cdots \left(\sum_{i=0}^{a_n} p_n^i\right)$.

Recall that $\sum_{n=a}^{b} x^n = \frac{x^{b+1} - x^a}{x-1}$, so $\sigma(n) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_n^{a_n+1} - 1}{p_n - 1}\right)$.

Definition 27

An integer > 0 is **perfect** if $\sigma(n) = 2n$.

Euler claimed that every even perfect number can be written as $2^m(2^{m+1} - 1)$, where $2^{m+1} - 1$ is a Mersenne prime.

Definition 28 (Mobius Mu Function)

The Mobius $\mu : Z_{>0} \to \{0, \pm 1\}$ returns $\mu(n) = 0$ if n is not squarefree, $\mu(1) = 1$, and if $n > 1$, $n = p_1, \dots, p_m$, then $\mu(n) = (-1)^m$.

Proposition 29

If $n > 1$ then $\sum_{d|n} \mu(d) = 0$.

Proof. $n = p_1^{a_1} \cdots p_m^{a_m}$. Notice that for any $a_i > 1$, we can ignore and take mod 2 because non-squarefree implies a Mobius of 0.

Therefore, $\sum_{d|n} \mu(d) = \sum \mu(p_1^{\epsilon_1} \cdots p_m^{\epsilon_m}) = (1-1)^m = 0$. □

Definition 30

If f, g are two functions $\mathbb{Z}_{>0} \to \mathbb{C}$, then the Dirichlet convolution of f and g is defined to be $(f \cdot g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

Remark 31

Dirichlet convolution is associative; given $f, g, h : \mathbb{Z}_{>0} \to \mathbb{C}$, then $((f \cdot g) \cdot h)(n) = (f \cdot (g \cdot h))(n) = \sum f(d_1)g(d_2)h(d_3)$,

Definition 32

Let $1(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$. Then, $(f * 1)(N) = \sum_{d|n} f(d)$.

Theorem 33 (Mobius Inversion)

If $f : \mathbb{Z}_{>0} \to \mathbb{C}$ and $F(n) = \sum_{d|n)f(d)}$, then $\sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) = f(n)$, or as we simplify it, $\mu \times F = f$.

7 Lecture 7

Definition 34 (Euler Totient)

We define $\phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$. $\phi(n)$ is the number of integers in $[1, n]$ relatively prime to n.

$\phi(1) = 1$, $\phi(p) = p - 1$ for prime p.

Proposition 35

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

Proof. Consider the set $\left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\}$. Write these fractions in lowest terms.

For each $d|n$, we wish to count the functions above with d in lowest terms. These fractions will be a subset of the fractions $\frac{a}{n}$ where $\frac{n}{d}|a$, i.e. a subset of the fractions $\left\{\frac{1}{d}, \frac{2}{d}, \ldots, \frac{d}{d}\right\}$. There are $\phi(d)$ many fractions on this list with d in the domain, when written in lowest terms.

So if $J_d \subset \left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\}$ corresponds to the fractions of denominator d in lowest terms, then $S = \bigcup_{d|n} J_d$, and $n = |S| = \sum_{d|n} |J_d| = \sum_{d|n} \phi(d)$. □

From Mobius inversion, we have $\phi = (\phi \cdot 1) \cdot \mu$. We know that $(\phi \cdot 1) = id$ where $id(n) = n$, so we have $\mu \cdot id = \sum_{d|n} \mu(d)\frac{n}{d}$. Now, let $n = p_1^{a_1} \cdots p_m^{a_m}$. Then,

$$\begin{aligned} \mu \cdot id &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} \cdots \text{ (by definition of Mobius inversion)} \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right) = \phi(n). \end{aligned}$$

Theorem 36

$\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

Also consider $\pi(x) = \frac{x}{\log x}(1 + \left(\frac{1}{\log x}\right)$.

Proof. Of $n \in \mathbb{Z}_{>0}$, let $p_1, \dots, p_{\pi(n)}$ be the primes $\leq n$ and let

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(1 - \frac{1}{p_i}\right)^{-1}.$$

Notice that each inner value for the product term is $\sum_{a=0}^{\infty} \left(\frac{1}{p_i}\right)^a$.

Then, $\lambda(n) = \sum \frac{1}{p_1^{a_1} \cdots p_{\pi(n)}^{a}}$, where the sum is over all $\pi(n)$-tuples $(a_1, \dots, a_{\pi(n)}) \in \mathbb{Z}_{\geq 0}^{\pi(n)}$. Then, we have

$$\log \lambda(n) = -\sum_{i=1}^{\pi(n)} \log(1 - p_i)^{-1} = \sum_{i=1}^{\pi(n)} \sum_{m=1}^{\infty} (mp_i^m)^{-1}.$$

If we can prove that $\log \lambda(n)$ converges, then we see that $\lambda(n)$ is divergent and we are done.

I'll pick this up later.

Somehow we're done. Easy. $\square$

8 Lecture 8

We go back to 36.