Number Theory

MATH 354, YALE UNIVERSITY, SPRING 2019

These are lecture notes for MATH 354b, "Number Theory," taught by Ross Berkowitz at Yale University during the spring of 2019. These notes are not official, and have not been proofread by the instructor for the course. They live in my lecture notes respository at

https://github.com/jopetty/lecture-notes/tree/master/MATH-354.

If you find any errors, please open a bug report describing the error and label it with the course identifier, or open a pull request so I can correct it.

Contents

1 January 14, 2019

Didn't go to lecture today.

2 January 16, 2019

2.1 Review from last time

Some definitions from last time.

Definition (Divisibility)**.** We say that a divides b if $b = ac$ for some $c \in \mathbb{Z}$. *Divisibility*

Definition (Division Algorithm)**.** Fix a and b. We want to divide a by b. Then there exists some unique q and some $0 \leq r \leq a$ such that $b = aq + r$. *Division Algorithm*

Definition (Prime)**.** A number is prime if its only positive divisors are 1 and itself. *Prime*

These are things we learned in grade school.

Theorem 2.1 (Well-Ordering Principle)**.** *Every nonempty subset of $\mathbb{Z}_{<0}$ has a least element. This is the defining property of $\mathbb{Z}$.*

2.2 Today

Definition (GCD)**.** Let $a, b \in \mathbb{Z}$. The greatest common divisor is the largest common divisor of a and b, so $\gcd(a, b) = \max\{d \mid d \text{ divides } a \text{ and } b\}$. We know this exists because of well-ordering. *GCD*

Definition (GCD)**.** Alternatively, the gcd of a and b is a d such that all other common divisors of a and b divide d as well. Eventually we'll prove that these are equivalent. *GCD*

Definition (GCD)**.** Given a and b in some PID, we say that the GCD is he principal generator d of the ideal (a, b), so $(a, b) = (d)$. Alternatively, the gcd is the smallest positive number in (a, b) if we're working in $\mathbb{Z}$. *GCD*

Notation (GCD)**.** As a nod to the last definition, we often write the GCD of two numbers as (a, b) to emphasize the relation to ideals. *GCD*

Some properties of greatest common divisors:

Lemma 2.1. *Let d be the greatest common divisor of a and b. Then for any $x \in \mathbb{Z}$ we know that $(a, b + ax) = d$ as well. Then the GCD is unchanged under linear combinations.*

Proof. It's clear that d still divides $b + ax$ if it divides a and b, so its clear that $(a, b + ax) \geq (a, b)$. Independently, we know that there can't be a larger divisor since if d' divides $b + ax$ then d' divides b, and we already know that d is the largest divisor of b which also divides ax. Thus $(a, b + ax) \leq (a, b)$ so $(a, b + ax) = d$. ∎

Lemma 2.2. *Let $I = \{ax + by \mid x, y \in \mathbb{Z}\} = (a, b)$. Then $I = \{dx \mid x \in \mathbb{Z}\}$ where d is the greatest common divisor of a and b.*

Proof. We show containment each way. First we note that $I \subseteq d\mathbb{Z}$ since every element of I is divisible by d since if d divides a and b then it divides $ax + by$. Then we show that $d\mathbb{Z} \subseteq I$ (this is sometimes called Bezout's Lemma). By the Well-Ordering property, we know that there exists some $c = \min(I \cap \mathbb{Z}_{>0})$. We know that $c \geq d$ since it must be the case that d divides c. On the other hand, if we can show that c is a common divisor of a and b then we know that $c \leq d$ as well. We know that $a = cq + r$ for $0 \leq r \leq c$. Then we know that $c \in I$ implies that $c = ax + by$ so $r = a - cq = a(1 - xq) + b(-yq)$ so $r \in I$. Since c is the minimum positive element we know that $c = 0$ and so $a = cq$ so it divides a. Repeat for b. Then $c \leq d$ and $c \geq d$ so $c = d$. This also gives us the definition of the GCD which is the divisor of a and b which is divisible by all other common divisors. ■

This part could be proved with the Extended Euclidean Algorithm.

Uniqueness of prime factorization

Lemma 2.3. *Let a and b be relatively prime. If a divides bc then a divides c.*

Proof. Note that $(a, b) = 1$, so there exist some $x, y \in \mathbb{Z}$ such that $1 = ax+by$. Multiplying through by c, we get that

$$c = cax + cby.$$

Since a divides cb it divides cby and it trivially divides cax so a divides c. ■

Corollary 2.1. *If p is prime and p divides ab then p divides a or p divides b.*

Corollary 2.2. *If p divides $\prod a_i$ then for some i we know that p divides a_i (this is the above corollary with induction).*

Theorem 2.2. *All integers have a unique prime factorization. For every $n \in \mathbb{Z}_{\geq 2}$ there exists a unique set of primes $p_1, \cdots, p_k$ and positive integers $a_1, \cdots, a_k$ such that $n = \prod_{i=1}^{k} p_i^{a_i}$.*

Proof. Assume that we have two (more than one) such lists of primes and their powers. Denote them $P = p_1, \cdots, p_k$ (possible with repeats) and $Q = q_1, \cdots, q_\ell$. Assyme by way of contradiciton that the lists are disjoint (otherwise we cancel the like terms). We know that p_1 divides $\prod_{i=1}^{\ell} q_i$, so p_1 must divide q_i for some i. This can happen if and only if $p_1 = q_i$. This contradicts the disjointness of our list and presents a contradiciton. ■

2.3 Before next class

1. Read §1.1 – §1.3 in *Ireland and Rosen*;
2. Read §3, §4.1, and §4.2 in *Rosen*;
3. Think about which textbook is preferred.