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.

3 Lecture 3

Didn't take notes today.

4 Wednesday, January 23

Recall the uniqueness of prime factorization, where for all $n \in \mathbb{N}$ we have a unique list of primes $p_1, \dots, p_k$ and $a_i, \dots, a_k \in \mathbb{Z}_{>0}$ such that $n = \prod_{i=1}^{k} p_i^{a_i}$.

4.1 Infinitude of Primes

Problem 4.1. How many primes are there?

Theorem 4.1. *There are infinitely many primes.*

Euclid's Proof. Assume by way of contradiction we have a finite list of primes $p_1, \dots, p_k$ of all primes. Let $M = \prod p_i$, and consider $M + 1$. By the existence of prime factorization, we know that $M + 1 = \prod_{i=1}^{k} p_i^{a_i}$. Without a loss of generality assume that $a_1 \neq 0$. Then p_1 divide $M + 1$ and since p_1 divides M it must be the case that p_1 divides 1 as well which presents a contradiction. ■

Fact: Let $p_1, p_2, p_3, \dots$ be a list of primes in order. By the uniqueness of prime factorization, there is an injective correspondence between vectors $(a_1, a_2, \dots) \in (\mathbb{Z}_{\geq 0})^{\infty}$ with finitely many nonzero entries and $\mathbb{N}$. The correspondence is $n = \prod p_i^{a_i}$ with a lot of a_i being zero.

NOTE: THE BELOW IS BY CONTRADCTION and (*) ONLY HOLDS FOR $k = \infty$. If we assume that the list of primes is finite, then we would have an injective correspondence between $(a_1, \dots, a_k) \in (\mathbb{Z}_{\geq 0})^k$ and $\mathbb{N}$. Therefore

$$\prod_{i=1}^{k} \left(\sum_{j=0}^{\infty} \frac{1}{p_i} \right) = \sum_{n=1}^{\infty} \frac{1}{n}. \tag{*}$$

Then by uniqueness of prime factorization for each $n \in \mathbb{N}$ we know that $1/n$ appears exactly once when you expand this product. This is Euler's product for the ζ function?

Euler's Proof. Assume by way of contradiction that there are finitely many primes. Then

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{k} \left(1 + \frac{1}{p_1} + \cdots \right) = \prod_{i=1}^{k} \left(\frac{1}{1 - 1/p_i} \right) < \infty.$$

Yet we know that $\sum 1/n$ diverges, which presents a contradiction. ■

Lemma 4.1. *For any $n \in \mathbb{Z}$ there exists a unique $a, b \in \mathbb{Z}$ such that a is square free (meaning that no square number divides it) and $n = ab^2$.*

Erdős' Proof. Assume by way of contradiction that there are finitely many primes. Then any square-free number $n = \prod p_i^{a_i}$ where $a_i \in \{0, 1\}$. Thus there are only 2^k square-free numbers. Now let's look at all numbers at most N for some N. By the above lemma, they

can be specified by (a, b) where a is square-free and b^2 is square. There are 2^k square-free numbers and at most $\sqrt{N}$ square numbers, so $N \leq 2^k\sqrt{N}$ for all N, so $2^k \geq \sqrt{N}$ for all N, which is very very false if $N > 2^{2k}$. ■

4.2 Congruence Equations & Modular Arithmetic

Congruence

Definition (Congruence)**.** We say that $a \equiv b \pmod{m}$ if and only if m divides $b - a$. Alternatively, we say that $a \equiv b \pmod{m}$ if and only if there exists some k such that $a = b + mk$.

Theorem 4.2 (Some quick remarks)**.**

1. *Congruency is an equivalence relation on the integers (transitive, symmetric, and reflexive);*
2. *For some fixed m, we define the congruence class $\bar{a}$ to be the set $\bar{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$;*
3. *Arithmetic on these congruence classes holds; If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. Thus $\bar{a} + \bar{b} = \overline{a + b}$ and $\bar{a}\bar{b} = \overline{ab}$. This forms the commutative ring $\mathbb{Z}/m\mathbb{Z}$.*

Problem 4.2. Let a, b, m be fixed. When is the congruence $ax \equiv b \pmod{m}$ solvable?

Obs. 1. If $(a, m) = 1$ then we can use Bezout's theorem. This tells us that tehre exist some X, Y such that $1 = aX + mY$. Then we multiply through by b to get that $b = a(Xb) + m(Yb)$. Then $aXb \equiv b \pmod{m}$.

Lemma 4.2. *The congruence $ax \equiv b \pmod{m}$ has solutions if and only if the GCD of a and m divides b.*

Proof. Let d be the GCD of a and m. By Bezout, there exists some $X_0, Y_0 \in \mathbb{Z}$ such that $d = aX_0 + bY_0$. Since d divides b there exists some k such that $b = dk$. Then $b = aX_0k + mY_0k$ so $b \cong aX \pmod{m}$ for $X = X_0k$. In the other direction, just write it out. If there is a solution then $b \cong aX \pmod{m}$ so $b = aX + mY$. Since the GCD divides the right hand side it must divide the left as well, so d divides b. ■

Problem 4.3. Can there be lots of different solutions? What do solutions look like?

5 Monday, January 28

5.1 *Solving* $ax \equiv b \pmod{m}$

Recall from last lecture that $ax \equiv b \pmod{m}$ is solvable if and only if the GCD divides m. If we let $m' = m/d$ then the solutions are unique modulo m'.

Proof. Let x_1, x_2 be solutions to $ax_1 \equiv b \pmod{m}$ and $ax_2 \equiv b \pmod{m}$. Consider then that $a(x_1 - x_2) \equiv 0 \pmod{m}$. Let $a' = a/d$. Then $da'(x_1 - x_2) = dm'k$. We know that m' divides $a'(x_1 - x_2)$, and since $(m', a') = 1$ we know that m' divides $x_1 - x_2$. ■

Corollary 5.1. *If $(a, m) = 1$ then there is a unique solution to $ax \equiv b \pmod{m}$.*

Corollary 5.2. *If $a \not\equiv 0 \pmod{p}$ for prime p then there is a unique solution to $ax \equiv b \pmod{p}$ in $\mathbb{Z}/p\mathbb{Z}$.*

Chinese Remainder Theorem

Theorem 5.1 (Chinese Remainder Theorem)**.** *If we have $m_1, \ldots, m_r$ all relatively prime and the system of equations*

$$x \equiv a_1 \pmod{m_1}, \ldots, a \equiv a_r \pmod{m_r},$$

then there is a unique solution modulo $M = m_1 \cdots m_r$. Alternatively, the rings

$$\mathbb{Z}/M\mathbb{Z} \cong \bigoplus_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$$

are isomorphic.

Lemma 5.1. *If $a_1, \ldots, a_r$ are pairwise relatively prime to m then the product $a_1 \cdots a_r$ is also relatively prime to m as well.*

Lemma 5.2. *If $a_1, \ldots, a_r$ all divide m and are all pairwise relatively prime to m then the product $a_1 \cdots a_r$ divides m.*

Proof of CRT. Let $\hat{M}_i = M/m_i = \prod_{j \neq i} m_i$. We find a helper y_i such that $y_i \equiv 0 \pmod{\hat{M}_i}$ and $y_i \equiv 1 \pmod{m_i}$. Then we'll have that $x = \sum a_i y_i$. Note that $(\hat{M}_i, m_i) = 1$ so we know that $1 = x_i \hat{M}_i + y_i m_i$ has a solution. Let $y_i = x_i \hat{M}_i$. THis shows existence. To show uniqueness, just apply Lemma 5.2 above. ■

5.2 *Algorithmic Speed for the Chinese Remainder Theorem*

The Euclidean Algorithm runs in logarithmic time in the inputs a, b. The worst case is when we plug in two consecutive Fibonacci numbers since they are recursively defined in almost the exact opposite way that Euclid's algorithm reduces numbers.