Review Notes: Math 311W: Proofs/Number Theory

Spencer Martz

February 12, 2024

This section is concerned with the properties of the integers, $\mathbb{Z} = \ldots, -2, -1, 0, 1, 2, \ldots$

1 The division algorithm, and GCD

1.1 The Well Ordering Principle:

Any non-empty subset A of the positive integers $\mathbb{P}$ has a least element–e.g. there exists some $n \in A\ s.t,\ \forall b \in A,\ n \leq b$ This allows us to define and operate on the least element of the set.

Note: We are not concerned about finite sets. Any finite set with an ordering has a least element, However, the infinite sets, $\mathbb{N} = \mathbb{P} \cup 0$ and $\mathbb{P}$, are special in that they always have a least element.

Observe this is not true for all infinite subsets of $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ – Subsets of $\mathbb{R}, \mathbb{Q}$ generally have no least element since I can make a smaller one, and Z does not have a least negative integer, since they go to -inf.

1.1.1 Theorem 1.1.1: The Division Theorem

Let $a, b, \in P$ with $a > 0$. Then $\exists\ q, r \in P,\ 0 \leq r < a$, s.t:

$$b = aq + r \tag{1}$$

Proof: Consider the set $D = \{b - ak \mid b - ak > 0, k \in N\}$
Now, if $a > b$, we have $b = 0a + b$, where $b = r < a$.
If $a \leq b$, then b = b - 0a is positive, and so is in D. So, D is non empty, and by the well ordering principle, D has a least element, say r = b - aq.
However, this implies that b=aq + r – we show now, that $r < a$.
Suppose r $\geq$ a, then (r - a) $\geq$ 0 and is an element of D. Then $r - a = (b + aq) - a = b - (a(q+1))$, which is certainly less than $b - aq$.
It has been shown that if $r \geq a$, then there exists an element of D less then r, which is a contradition of r being the least element of D.
This implies that $r \leq a$ and the proof is complete.

1.2 Definition of a divides b, $a|b$

For two integers a and b, we say a divides b (denoted $a|b$) if there exists an integer c, st.

$$b = ac \tag{2}$$

(this means, r = 0 from the division theorem)

1.3 Theorem 1.1.2: The GCD theorem

For any $a, b, \in P$, $\exists d \in P$ s.t:

$$d|a \text{ and } d|b \tag{3}$$

and

$$\forall c \in P \ s.t. \ c|a, \text{ and } c|b \implies c|d \tag{4}$$

Proof: Consider the set of all integral linear combonations of a and b greater than 0 – $D = \{as + bt \mid as + bt > 0, s, t \in N\}$. Since a and b are certainly in D (say $a = a + 0b$) D is non empty and therefore has a least element, call it d =as +bt.

We will first show: if $c|a$ and $c|b$ then $c|d$:

If $c|a$ and $c|b$, then $\exists k, q \in Z \ s.t. \ b = qc$ and $a = kc.$
Then, $d = as + bt = kcs + qct = c(ks + qt) \implies c|d$

Now, we show $d|a$, and by symmetry it will show, $d|b$.

By theorem 1.1.1, regardless of if $d|a$, $\exists q, r \in Z \ s.t. \ a = dq + r, 0 \leq r < a,$
and we have $r = a - dq \implies r = a - (as + bt)q$
Now, if $r > 0$, $r \in D$, but observe $r = a - (as + bt)q$ is less than $d = as + bt$ – a contradiction.
This implies that r = 0, so $d|a$.
A similar process may be performed to obtain $d|b$, and the proof is complete.

1.4 Corollary 1.1.3: Characterization of the GCD

Let $a, b \in P$, then the GCD of a and b is the least positive linear integral combonation of and b – as in 1.1.2, $d = as + bt$.

Proof: Theorem 1.1.2 shows this is true–for any c which also divides a and b, we have c divides d, so $d \geq c \ \forall c$ which divides a and b, and so d is the greatest common divisor.

Further notes on the GCD and bezout's identity It's pretty weird, huh?

1.5 Lemma 1.1.4 (needed for 1.1.5)

Let a, b be natural numbers, $a \neq 0$, and suppose $b = aq + r$ for $q, r > 0$, then the gcd of a and b is equal to the gcd of a and r.

Proof Let d = gcd(a,b). Since d divides a and d divides b, we have that $d|(b - aq) = r$, and so $d|r$.
Now, since $d|a$ and $d|r$, we have $d|gcd(a, r)$. Also note, (a,r) is a common divisor of a and r, and so divides b=aq+r. So (a,r) divides a, and b, and by 1.1.2 it must also divide d.
It has been shown that $d|(a, r)$ and $(a, r)|d$. Since d and (a,r) are both positive, it must be that d = (a,b) = (a,r)

1.6 Theorem 1.1.5: The euclidean algorithim

Let a, b be positive integers. If a divides b, then a is the gcd(a,b). Otherwise, repeatedly apply theorem 1.1.1 to define a sequence of positive integers, $r_1, r_2 \dots r_n$:

$$\begin{aligned}
b &= aq_1 + r_1 \quad 0 \leq r_1 < a \\
a &= r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4 \quad 0 \leq r_4 < r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

Then r_n is the gcd of a and b.

Proof: Since $r_{1\dots n}$ is a decreasing sequence of positive integers, it must have a final element r_n for which no (non-zero) remainder r_{n+1} exists, so $r_n|r_{n-1}$. Then, by lemma 1.1.4, we have $gcd(r_n, r_{n-1}) = r_n$, as well as
$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-3}, r_{n-2}) = \cdots = (r_1, a) = (a, b)$.

This provides a simple way to find the GCD of two integers, and also may be arranged in a matrix format (although the details will not be discussed here).

We may also speak of the GCD m of a set of integers, $a_{1\dots n}$, where $m|a_i \ \forall i \leq n,$ and $\forall c|a_i,\ c|m$.

1.7 Defintion: Coprime or Relatively prime

Two positve integers a and b are said to be coprime if their gcd is 1.

1.8 Theorem 1.1.6: Properties of coprime integers (A fairly important one!)

Let $a, b, c \in P, (a, b) = 1$, (so a and b are coprime). Then:

$$I. \text{ if } a|bc, \text{ then } a|c$$
$$II. \text{ if } a|c \text{ and } b|c, \text{ then } ab|c$$

Proof: I. By the definition of coprime, and corollary 1.1.3, if $(a, b) = 1$, $\exists s, t \in Z\ s.t.\ sa+tb = 1$.
Multiply both sides by c to obtain: $c = csa + ctb \quad (eq.1)$.
Observe $a|csa$. Now, if $a|bc$, $a|ctb$, so $a|(csa + ctb)$, and so $a|c$.

II. Consider eq. 1. Since $a|c$, we have $ab|ctb$, and since $b|c$ we have $ab|csa$,
so $ab|(csa + ctb)$ and $ab|c$.

2 1.2: Mathmatical Induction

2.1 Defintion: The Principle of Mathematical Induction

Let P(n) be an assertion involving the natural number n. Then, if

$$P(1) \text{ is true, and}$$
$$P(k) \implies P(k+1),$$

then P(n) is true for all n.

2.2 Theorem 1.2.1: The Principle of Induction follows from the Well-Ordering Principle.

Proof: Suppose the induction hypothesis is satified, that is, P(1) is true, and $P(k) \implies P(k+1)$.
Let S be the set of all n for which P(n) is not true, and assume S is non empty, then by the well ordering princple it has a least element, call it t. Since P(1) is true, $t \neq 1$, and $t-1 > 0$. Now, since t is the least element of s, t-1 is not in is, and so P(t-1) is true. However, $P(k) \implies P(k+1)$, so P((t-1)+1) = P(t) is true, which contradicts $t \in S$, implying S is empty, and so P(n) is true for all n.

2.3 Theorem 1.2.2: The Binomial Theorem

Let $x, y \in Z, n \in P$. Then, $(x+y)^n$ is given:

$$(x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + \binom{n}{n-1}x^1 y^{n-1} + \binom{n}{n}x^0 y^n$$

where $\binom{n}{k}$ is given as $\frac{n!}{k!(n-k)!}$ Note,

$$1 = \binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n!} = \frac{n!}{0!(n-0)!} = \binom{n}{0} = 1 \tag{5}$$

Proof: By induction on n Base case n=1: We have $(x+y)^1 = x+y$. Oberserve our coefficents are $\binom{1}{0} = \binom{1}{1} = 1$, so the base case holds. Now, suppose inductively it is true for n=k, we have:

$$(x+y)^k = \binom{k}{0}x^k + \cdots + \binom{k}{i}x^{k-i}y^i + \cdots + \binom{k}{k-1}x^1 y^{k-1} + \binom{k}{k}y^k \tag{6}$$

Now, observe that $(x+y)^{k+1} = (x+y)(x+y)^k$. Then, we may expand the product to get:

$$(\binom{k}{0}x^{k+1} + \binom{k}{0}x^k y) + (\binom{k}{1}x^k y + \binom{k}{1}x^{k-1}y^2) + \cdots + (\binom{k}{k}xy^k + \binom{k}{k}y^{k+1}) \tag{7}$$

and regrouping like terms, we get:

$$\binom{k}{0}x^{k+1} + (\binom{k}{0} + \binom{k}{1})x^k y + (\binom{k}{1} + \binom{k}{2})x^{k-1}y^2 + \cdots + (\binom{k}{i} + \binom{k}{i+1})x^{k-i+1}y^i + \cdots + \binom{k}{k}y^{k+1} \tag{8}$$

Now, by eq. 5 we have that $\binom{k}{k} = \binom{k}{0} = \binom{k+1}{k+1} = \binom{k+1}{0} = 1$, so we may write the first and last terms as
$\binom{k+1}{0}x^{k+1}$ and $\binom{k+1}{k+1}y^{k+1}$. All that is left to show is $\binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i}$

While there is a algebraic solution, recalling Pascal's triangle, this combinatoric identity should be familiar. Infact, it is called pascal's identity, and is precisely the definition of pascals triangle:
the ith entry in the (k+1)th row is the sum of the i and i + 1 terms in the previous row-the "k" row.
In conjuntion with the knowlege that the entries of pascals triangle give the values of $\binom{n}{k}$, this will suffice as proof for the identity: $\binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i}$, and so we have:

$$(x+y)(x+y)^k = (x+y)^{k+1} = \binom{k+1}{0}x^{k+1} + \binom{k+1}{1}x^k y + \cdots + \binom{k+1}{k}xy^k + \binom{k+1}{k+1}y^{k+1} \quad (9)$$

So, $P(k) \implies P(k+1)$, and by the principle of induction, P(n) is true for all n.

3 1.3: Primes and the Unique Factorization Theorem

3.1 Definition of prime

A positive integer p is prime if it has exactly two unqiue divisors, namely 1 and p.

3.2 Lemma 1.3.1 AKA Euclid's Lemma

For p prime, if p divides ab, then p divides a or p divides b.

Proof: Since the only divisors of p are p and 1, it must be that (a,p) is p or 1. If it is p, then $p|a$. So, if p does not divide a, then (a,p) is one.
Now, by theorem 1.1.6, we have for $(a, b) = 1$, if $a|bc$, then $a|c$. Let $p \to a, a \to b, b \to c$ then for $(p, a) = 1$ we have if $p|ab$, then $p|b$.
This theorem can be considered as a special case of 1.1.6 – 1.1.6 is a generalization of euclid's lemma (to a,b) coprime, not just p prime.

3.3 Lemma 1.3.2: The REAL euclid's lemma (or the one he needed)

Let p be prime, and suppose p divides some product $a_1a_2a_3 \dots a_n$. Then $p|a_i$ f.s. $1 \leq i \leq n$.

Proof: By induction on n, the number of factors of p: The base case n=1 is trivial, if $p|a_1$, $p|a_1$.
Now suppose P(r-1) true, P divides some a_i for $p|a_1a_2 \dots a_{r-2}a_{r-1}$.
Now, for P(r), consider $p|b_1b_2b_2 \dots b_r$. We must write $b_1b_2b_2 \dots b_r$ as a product of r-1 integers.
Observe that product $b_{r-1}b_r$ yields an integer as well, so we may take $b_i = a_i$ for $i \leq r - 2$, and $b_{r-1}b_r = a_{r-1}$

$$b_1b_2b_3 \dots b_{r-2}(b_{r-1}b_r) = a_1a_2a_3 \dots a_{r-2}a_{r-1} \tag{10}$$

So, by our inductive hypothesis we have p divides some $a_{1\dots(r-1)} = b_{1\dots(r-1)}$,
or p divides $a_{r-1} = b_{r-1}b_r$ in which case by Lemma 1.3.1 p divides b_{r-1} or, b_r. So, $P(r-1) \implies P(r)$, and by the principle of induction P(n) is true for all $n \geq 1$.

3.4 Theorem 1.3.3: The Unique Factorization Theorem for Integers

I. Let $n \in P, n > 2$. Then

$$\exists p_{1\dots r} \text{ prime, s.t. } p_1p_2 \dots p_r = n \tag{11}$$

II. This prime factorization is also unqiue in the sense that for some $n = q_1q_2 \dots q_t$, q_i prime, then t equals r, and we may relabel the q_i so each $q_i = p_i$.

Proof: I. We show each integer greater than 2 has a unqiue prime factorization by strong induction. The base case $P(n = 2)$ is trivial, as 2 is prime and so we have a prime factorization for n. Now suppose $P(2 \leq m < n)$ true, so all integers less then n have a unique factorization. Now, n is either prime or composite. In the former case, we have a prime factorization, n. In the latter case, by definition n is a product of two integers $a, b < n$. By our induction hypothesis, a, and b, each have a prime factorization, and this implies n does aswell-simply the concatenation of a's and b's prime factors. So, in either case n has a prime factorization, and we have shown $P(2 \leq m < n) \implies P(n)$, and by the principle of strong induction, P(n) is true for all $n > 2$.

II. We show this factorization is unqiue by induction on r, the number of prime factors of n. For the base case, r=1, n is prime. Then suppose we have a factorization

$$n = q_1 q_2 \ldots q_s \text{ for } q_i \text{ prime,} \tag{12}$$

If $s \geq 2$, we have s+1 unqiue factorizations for n: $1, q_1$, and $q_1 q_2 \ldots$, – so n is not prime, a contradiction. This implies s = 1 and the base case is complete.

Now,inductively suppose P(r-1), that $n = p_1 p_2 ... p_{r-1}$ is a unique factorization as described above, and suppose

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s \tag{13}$$

Now, since $p_1 | q_1 q_2 \ldots q_r$, by lemma 1.3.2 we have that p_1 divides some q_i. Let it be q_1 for clarity. Now, since q_1 is prime, it must be that $p_1 = q_1$, and we may cancel as follows:

$$\cancel{p_1} p_2 \ldots p_r = \cancel{q_1} q_2 \ldots q_s \implies p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s \tag{14}$$

Since the LHS is a product of r-1 primes our induction hypthesis implies s-1 = r -1, so s = r, and we may relabel the q_i so each $q_i = p_i$ for $i \geq 2$ We already have $p_1 = q_1$, and so we have $p_i = q_i$ for $i \geq 1$, and the proof is complete.

3.5 Theorem 1.3.4: There are infinite prime numbers

Proof: Suppose there are finitely many, n, prime numbers, then we may list them, $p_1, p_2, \ldots p_n$. Let N be the product of all primes plus one:

$$N = p_1 p_2 \ldots p_n + 1 \tag{15}$$

Observe that no p_i divides N, since it has a remainder of 1. Now, by the UFT (Theorem 1.3.3), we have n as a unqiue factorization of integers, and so it has atleast 1 prime divisor, q. Since no p_i divides N, $q \neq p_i$ for any i, and we have contradicted that $p_{1 \ldots n}$ is the complete list of primes, so there are infinite primes.

3.6 Theorem 1.3.5: Characterization of the GCD and LCM from prime factorization

Let $a, b \in p$, and let

$$a = p_1^{n_1} p_2^{n_2} p_3^{n_3} \ldots p_r^{n_r}$$
$$b = p_1^{m_1} p_2^{m_2} p_3^{m_3} \ldots p_r^{m_r}$$

be prime factorizations of a and b, with some n_i or m_i perhaps 0 to allow a common list of primes. Then the gcd d, and lcm f, are given by:

$$d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$$
$$f = p_1^{j_1} p_2^{j_2} \ldots p_r^{j_r}$$

where each k_i is the least of n_i and m_i, and each j_i is the greatest of each n_i and m_i.

4 1.4: Modular Arithmetic and Congruence Classes

4.1 Defintion of a modulo b and congruence

For integers a and b, $n > 1$, a is congruent to b modulo n, if a and b have the same remainder when divided by n. This is denoted:

$$a \equiv b \mod n \tag{16}$$

Consider that if and b have the same remainder when divided by n, we may write
$a = kn + r, \quad b = qn + r$, and so $a - b = kn - qn$, which is divible by n. It follows that

$$a \equiv b \mod n \iff n|(a - b) \tag{17}$$

We also have for $a \equiv b \mod n$ (not proven here)

$$a + c \equiv b + c \mod n$$
$$a - c \equiv b - c \mod n$$
$$ca \equiv cb \mod n$$

However, division is not so simple.

4.2 Congruence Classes

Fix $n > 1$ and let a be any integer. Then, the congrunce class of $a \mod n$ is the set of all integers which are congruent to $a \mod n$

$$[a]_n = \{s \in \mathbb{P} \mid s \equiv a \mod n\}, \qquad [a]_n = [b]_n \iff a \equiv b \mod b \tag{18}$$

The set of all congruence classes mod n is denoted $\mathbb{Z}_n$, and has n elements (see 1.1.1).
$[0]_n$ is called the zero-congruence class, and is all the multiples of n. Since there are infinite ways to represent a congruence class:

$$\cdots = [a - n]_n = [a]_n = [a + n]_n = [a + kn]_n = \dots \tag{19}$$

As such it is useful to pick a set of n "standard representatives" – nearly always the integers up to n-1. For example:

$$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$$
$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$$
$$\mathbb{Z}_4 = \{[0]_4, [1]_4 l, [2]_4, [3]_4, \}$$
$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, [2]_{10}, [3]_{10}, [4]_{10}, [5]_{10}, [6]_{10}, [7]_{10}, [8]_{10}, [9]_{10}\}$$

4.3 Congruence Class Operations

Operations (paticularly multiplication and addition) on congruence class are defined as follows:

$$[a]_n + [b]_n = [a + b]_n$$
$$[a]_n [b]_n = [ab]_n$$

This may seem trivial, however considering $[a]_n$ is not a number, but a infinte set of numbers, it requires proving. The following theorems show these defintions are reasonable.

4.4 Theorem 1.4.1: Congruence Class Operations are Well-Defined

If $[a]_n \equiv [c]_n$, then:

$$[a+b]_n \equiv [b+c]_n$$
$$[ab]_n \equiv [bc]_n$$

Proof: If $[a]_n \equiv [c]_n$, we have that $n|a-c$ (and c-a), and so $a-c = nk \implies a = c+nk$. So we have (by the definition of congruence class):

$$[a+b]_n \equiv [c+nk+b]_n \equiv [b+c]_n \tag{20}$$

Similarly, we have:

$$[ab]_n \equiv [(c+nk)b]_n \equiv [cb+nkb]_n \equiv [bc]_n \tag{21}$$

4.5 Corollary 1.4.2; Congruence Class Operations are Really Well Defined

If $[a]_n \equiv [c]_n$, $[b]_n \equiv [d]_n$, then:

$$[a+b]_n \equiv [c+d]_n \tag{22}$$
$$[ab]_b \equiv [cd]_n \tag{23}$$

Proof: Follows directly from 1.4.1.

This implies the definitions of congruence class operations obey the same properties we expect integer operations to obey, and so the operations are "well defined."

4.6 Defintions: Invertible Class and Zero-Divisor Class

Let $n > 1, a \in \mathbb{Z}$.

- An invertible class is an element of $\mathbb{Z}_n$, for which $\exists b \in Z$ s.t. $[a]_n[b]_n = [1]_n$.
  Then $[b]_n$ is the inverse of a, which may be denoted $[a]_n^-1$
- A zero-divsor class is a non-zero element of $\mathbb{Z}_n$, for which $\exists b \neq 0 \in Z$ s.t. $[a]_n[b]_n = [0]_n$.
  Then $[b]_n$ is also a zero-divisor.

4.7 Theorem 1.4.3: Invertibility of a Congruence Class

An element of $\mathbb{Z}_n, [a]_n$ is invertible if a is coprime to n.

Proof: If a is coprime to n, that is (a,n) = 1, we have by theorem 1.1.3 that $\exists s, t$ s.t. $as+nt = 1$. So by the defintion of congruncence, we have that [as] $\equiv 1 \mod n$, so $[as] \equiv [1]_n$, and by theorem 1.4.2, we have

$$[a]_n[s]_n = [1]_n \tag{24}$$

so [a] is invertible (mod n), and in fact has an inverse [s], satifsting as+nt = 1.

4.8 Theorem 1.4.4: Divisbility in Congrunce Classes

Let $n > 1$, a, b, c be integers and (c,n) = 1. Then, if:

$$ac \equiv bc \mod n$$
$$a \equiv b \mod n$$

Proof: If c and n are coprime, by 1.4.3 we have that c is invertible mod n, so $[c]_n^{-1}$ exists, and:

$$[a]_n[c]_n \stackrel{?}{=} [b]_n[c]_n$$
$$[a]_n[c]_n[c]_n^{-1} \stackrel{?}{=} [b]_n[c]_n[c]_n^{-1}$$
$$[a]_n[1]_n \stackrel{?}{=} [b]_n[1]_n$$
$$[a]_n = [b]_n$$

4.9 Theorem 1.4.5: Every element of $\mathbb{Z}_n$ is invertible or a zero divisor, but not both.

Proof: Subcripts of n are omitted for clariy. Suppose an element $[a]$ is invertible (so $[a]^{-1}$ exists). Then, for some $[a][b] = [0]$, we have:

$$[a][b] = [0] \implies [a]^{-1}[a][b] = [a]^{-1}[0] \implies [b] = [0] \tag{25}$$

so by defintion, a is not a zero divisor.

Now, suppose an element c is not invertible, that is, (c,n) ¿ 1. Let d=(c,n), and note $d|c, d|n$, so we have n=dt, c=ds. Observe that:

$$ct = s(dt) = sn \tag{26}$$

so ct is mutliple of n, and thus $[ct] \equiv [c][t] \equiv [0]$, so c is a zero divisor (t is clearly non-zero).

4.10 1.4.6: Invertiblility of congruence classes mod p (prime)

Any non-zero element in $\mathbb{Z}_p$ is invertible.

Proof: If [a] is non-zero, then p does not divide a, and a does not divide p since p is prime. (unless a = p, in which case it is [0], or a=1, in which case it invertible) Now, GCD(a,p) can only be p or 1, and p does not divide a so it is 1. Then, by theorem 1.4.3, we have that a is invertible.