Year 3 — Number Theory

Based on lectures by Dr Henri Johnston
Notes taken by James Arthur

Autumn Term 2021

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Contents

1 Week I - Introduction **2**
1.1 Division Algorithm 2
1.2 Greatest Common Divisor 2

2 Week 2 - stuff **4**

1 Week I - Introduction

1.1 Division Algorithm

Definition 1.1 (Well Ordering Principle)**.** Every non-empty subset of $\mathbb{N}_0$ contains a least element

Theorem 1.2 (Division Algorithm)**.** Given a $a \in \mathbb{Z}$ and a $b \in \mathbb{N}_1$ there exists unique integers q and r satisfying $a = bq + r$ and $0 \leq r < b$.

The proof splits into uniqueness and existence.

Proof. We shall first prove existence, define $S := \{a - xb : x \in \mathbb{Z} \quad \text{and } a - xb \geq 0\}$. We know $S \neq 0$ since,

- if $a \geq 0$, then choose $m = 0$, them $a - mb = a \geq 0$
- if $a < 0$, then let $a = m$, so $a - mb = a - ab = (-a)(b-1) \geq 0$ since $-a > 0$ and $b > 0$[1]

Hence S is non-empty subset of $\mathbb{N}_0$ and so by the well ordering principle S must contain a least element $r \geq 0$. Since $r \in S$, then we have there exists a $q \in \mathbb{Z}$ such that $a - qb = r$ and so $a = qb + r$. Now it remains to check that $r < b$, so assume for a contradiction that $r \geq b$, then let there be a $r_1 = r - b \geq 0$. Then,

$$a = qb + r = qb + (r_1 + b) = (q+1)b + r_1$$

and so $a - (q+1)b = r_1 \in S$ and is smaller than r, a contradiction.

Now let us show uniqueness, assume that there exist another pair q', r' such that $a = q'b + r'$ where $0 \leq r' < b$. Then form $a = a + qb + r = q'b + r'$ we have that, $(q - q')b = r' - r$. If $q = q'$, then we must have $r = r'$, suppose for a contradiction that this isn't true, then,

$$b \leq |q - q'||b| = |r - r'|$$

However, since $0 \leq r, r' < b$ and so $|r - r'| < b$ which gives a contradiction. □

1.2 Greatest Common Divisor

Let us start with a theorem.

Theorem 1.3. Let $a, b \in \mathbb{Z}$, $\exists\, d \in \mathbb{N}_0$ and non-unique $x, y \in \mathbb{Z}$ such that,

(i) $d \mid a$ and $d \mid b$

(ii) and if $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$, then $e \mid d$

(iii) $d = ax + by$

Proof. If $a = b = 0$, then $d = 0$
Suppose that $a \neq b \neq 0$, then let

$$S := \{am + bn : m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$$

Now $a^2 + b^2 > 0$ so S is non-empty and a subset of $\mathbb{N}_1$. Hence, by the Well ordering principle then there must be some minimum element d. Then we can write $d = ax + by$ by definition of S.

By the division Algorithm, $a = qs + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq q < d$. Suppose for a contradiction that $r \neq 0$. Then,

$$0 < r = a - qd = a - q(ax + by) = (1 - qx)a - qby$$

[1] I think this is wrong, I don't see this as true.

Hence, $r \in S$. But $r < d$, contradiciting the minimality of d in S. So we must have $r = 0$, i.e $d \mid a$. The same works for $d \mid b$.

Suppose that $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$. Then e divides any linear combination of a and b, so $e \mid d$. Suppose that $e \in \mathbb{N}_1$ also satisfies (i) and (ii). Then, $e \mid d$ and $d \mid e$ and so $d = \pm e$, but $d, e \geq 0$ and so $d = e$. Thus d is unique. □

Note that this is a standard trick to prove that integers divide, by just proving that $r = 0$ by contradiction.

Corollary 1.4. If $a, b \in \mathbb{Z}$ then there exists a unique $d \in \mathbb{N}_1$ such that.

(i) $d \mid a$ and $d \mid b$

(ii) if $e \in \mathbb{Z}$, then $e \mid a$ and $e \mid b$ then $e \mid d$

Proof. The existence of a d is given by the theorem. In the proof of uniqueness we only use (i) and (ii). □

Definition 1.5 (Greatest Common Divisor)**.** Let $a, b \in \mathbb{Z}$. Them d of the previous corollary is just the greatest common divisor of a and b, written $\gcd(a, b)$. Also sometimes seen as $\text{hcf}(a, b)$.

If $\gcd(a, b) = 1$, then a and b are coprime.

Identity (Bezouts Identity)**.** Given $a, b \in \mathbb{Z}$ there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

2 Week 2 - stuff

test2