Lecture 2 Notes

David Gieseker

October 14, 2020

1 Euclid's Knowledge

Let's first review the division algorithm.

Theorem. *Let* $a, b \in \mathbb{Z}$ *and* $b > 0$*. Then,* $\exists! q, r \in \mathbb{Z}$ *such that* $a = qb + r$ *where* $0 \le r < b$*.*

This is the same as what we learned from elementary school. We know that q is the quotient and r is the remainder – and both are unique.

Proof. (existence) Let $S = \{n \in \mathbb{Z} \mid \exists x \in \mathbb{Z}, n = a - bx \ge 0\}$. Suppose that $S \ne \emptyset$ (the elements are potential q's). Then, we can consider 3 different cases:

1. If $a \ge 0$, we take $x = 0$ and $a \in S$.
2. If $a < 0$, we take $x = a$. Then, $n = a - ab = a(1 - b)$. But since $b > 0$ and $b \in \mathbb{Z}$, $n = a(1 - b) \ge 0$. Therefore, $a \in S$.

And by the Well-Ordering Property, there is a least element r of S. If we denote its corresponding x to be q, then $r = a - bq \ge 0 \implies a = qb + r$.
Next, we show that $0 \le r < b$. We showed $r \ge 0$ previously. Then assume that $r \ge b$, and thus $0 \le r - b = a - b(q + 1) \in S$. However, r is assumed to be a least element of S, so $r \le r - b$ and $b \le 0$. This is a contradiction, so $r < b$. $\square$

Proof. (uniqueness) Assume that quotients and remainders are not unique. Then $a = qb + r = q'b + r'$, where $0 \le r < b, 0 \le r' < b$. If the remainder is not unique, then we can take $r > r'$ without loss of generality. Thus, we have $0 < r - r' \le r < b$. And since $0 \ne q - q' \in \mathbb{Z}$, $|q - q'| \ge 1$. Then from the original equation, we have $r - r' = (q' - q)b \ge b$. This is a contradiction to the prior inequality. Thus, $r = r'$ must hold, and $q = q'$ follows as $b > 0$. $\square$

Definition. *Let* $d, m \in \mathbb{Z}$ *where* $d \ne 0$*. Then* d *divides* m *if* $\exists e \in \mathbb{Z}, m = ed$*, notated by* $d \mid m$*.*

Definition. *Let* $m, n \in \mathbb{Z}$*. Then,* $d \in \mathbb{Z}$ *is a greatest common divisor, notated by* $d = (m, n)$*, of* m *and* n *if:*

(i) $d > 0$

(ii) $d \mid m, d \mid n$

(iii) *if* $e \in \mathbb{Z}$ *and* $e \mid m, e \mid n$*, then* $e|d$.

In other words, d *is a divisor of* m *and* n *that divides any other common divisors.*

Definition. $f \in \mathbb{Z}$ *is a* $\mathbb{Z}$ *linear combination of* $m, n \in \mathbb{Z}$ *if* $\exists x, y \in \mathbb{Z}$ *such that* $f = xm + yn$.

Theorem. *Let* $m, n \in \mathbb{Z}$*, and at least one of which is nonzero. Then,* $d = (m, n)$ *exists, is unique, and is a* $\mathbb{Z}$ *linear combination of* m *and* n.

Proof. Let's define $S = \{am + bn > 0 \mid a, b \in \mathbb{Z}\}$. Now, we first show that $d \mid m$. S is nonempty, since we can always take $a = sgn(m), b = 0$ and $am + bn \in S$ must hold. Thus, it must have a least element d. Then by the division algorithm, $\exists q, r \in \mathbb{Z}$ such that $m = qd + r$ and $0 \leq r < d$.

$$r = m - qd = m - (am + bn)q = (1 - aq)m - bqn \geq 0$$

Therefore, r is also a $\mathbb{Z}$ linear combination of m and n. However $r < d$ and d is the least element of S, so $r = 0$ is the only possibility. Therefore, $m = qd \implies d \mid m$. Similarly, $d \mid n$ can be proven with a similar method.
Now, suppose that e is another common divisor of m and n. Thus $m = xe$ and $n = ye$, so $d = (ax + by)e$ and it follows that $e|d$. Therefore $d = (m, n)$ by definition, and it is a $\mathbb{Z}$ linear combination of m and n as it is in S. □

Proof. (uniqueness) Let d, d' be two GCD's of m and n. Then, $d|d'$ and $d'|d$ must both hold. This is true only when $d = \pm d'$, and since $d, d' > 0$ they must be equal. □