LECTURE 4

September 13, 2023

1. The Division Algorithm

Recall in the previous lecture we started to have a look at divisibility and the Euclidean division algorithm.

NOTATION 1.1. For $a, b \in \mathbb{Z}$ with $a \neq 0$, we will say a *divides* b and write $a \mid b$ if b is an integer multiple of a, i.e. there exists some integer $k \in \mathbb{Z}$ such that $b = ka$.

THEOREM 1.2 (Division Algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ such that $a = qb + r$. We call q the quotient and r the remainder of the division a by b. By unique, we mean that there is exactly one q and one r that will make $a = qb + r$.*

REMARK 1.3. $a \equiv r \bmod b$ since $a - r = qb$.

PROOF. Define $S = \{a - kb : k \in \mathbb{Z} \text{ and } a - kb \geq 0\}$. Note that S is bounded below by 0 and S has to be nonempty, which we have to verify! We will take two cases, depending on the value of a.

(1) If $a \geq 0$, then $a = a - 0 \cdot b \in S$.
(2) If $a < 0$, then $(-a)(b - 1) = a - a \cdot b \geq 0$ and so $a - ab \in S$.

Thus, S cannot be empty.

By the Well-Ordering Principle (Theorem 1.4), there exists an $r = \min(S)$, i.e. $r \in S$ and for all $m \in S$, $r \leq m$. Since $r \in S$, we know that $0 \leq r$ and there exists a $k \in \mathbb{Z}$ such that $r = a - kb$. Let us relabel k as q, so that $a = qb + r$.

We now need to show that $0 \leq r < b$. We know $0 \leq r$, so we check $r < b$. Towards contradiction, assume that $r \geq b$. Then this implies that $0 \leq r - b = a - qb - b = a - b(q + 1) \in S$ and $r - b < r = \min(S)$, which is absurd. Therefore, it must be the case that $r < b$.

Finally, we need to show that q and r are unique. Take $q', r' \in \mathbb{Z}$ such that $0 \leq r' < b$ and $a = q'b + r'$, we need to show that $q' = q$ and $r' = r$. Observe that $0 \leq r' = a - q'b \in S$ so $r' \geq \min(S) = r$. Now proceed by contradiction and assume that $r' \neq r$. Since $r' \geq r$ from, and $r' \neq r$, then $r' > r$. So now $0 < r' - r = a - q'b - (a - qb) = (q - q')b$ which implies that $b \mid r' - r$ therefore, by Proposition 2.4, $|b| \leq |r' - r|$ which implies that $b \leq r' - r \leq r'$. This is absurd since $r' < b$. Therefore, $r = r'$ and thus, it follows that $q = q'$ as well. $\square$

2. Greatest Common Divisor

Definition 2.1. Let $a, b \in \mathbb{Z} \setminus \{0\}$. The *greatest common divisor* of a and b is defined as

$$\gcd(a, b) = \max\{k \in \mathbb{N} : k \mid a \text{ and } k \mid b\}$$

Remark 2.2. $\gcd(a, b)$ is well-defined and $1 \leq \gcd(a, b) \leq \min\{|a|, |b|\}$. We justify that We justify that $D = \{k \in \mathbb{N} : k \mid a \text{ and } k \mid b\}$ contains 1 and thus, nonempty. Second, if $k \in D$, then because $k \mid a$, then $|k| \leq |a|$ which implies that $k \leq |a|$. Similarly, since $k \mid b$, then $|k| \leq |b|$ which implies that $k \leq |b|$. Therefore, $\min\{|a|, |b|\}$ is an upper bound for D.

Theorem 2.3 (Bezouts' Theorem). *For $a, b \in \mathbb{Z} \setminus \{0\}$, there exists integers $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$.*

Proof. Define $S = \{xa + yb : x, y \in \mathbb{Z}, xa + yb \geq 1\}$. We need to observe that $S \neq \emptyset$. Indeed, take $1 \leq |a| = \frac{|a|}{a} \cdot a + 0 \cdot b \in S$ which implies that $|a| \in S$ and similarly, $|b| \in S$ as well. By the Well-Ordering Principle (Theorem 1.4), there exists a $d = \min(S)$ and $d \leq \min\{|a|, |b|\}$. Since $d \in S$, there exists $x, y \in \mathbb{Z}$ such that $d = xa + yb$ and $d \geq 1$.

We want to show that $xa + yb = \gcd(a, b)$. The first step is to show that d divides a. By the Division Algorithm (Theorem 1.2), there exists $q, r \in \mathbb{Z}$ such that $0 \leq r < d$ such that $a = qd + r$. We claim that $r = 0$ so that $d \mid a$. Assume otherwise that $r \neq 0$, and so in particular, $1 \leq r < d$, and so writing $1 \leq r = a - qd = a - q(xa + yb) = (1 - qx)a + (-qy)b$, and thus, $r \in S$ and $r < d = \min(S)$ which is absurd. The proof to show that $d \mid b$ is similar.

Finally, we need to show that d is a common divisor of a and b, and we need to show that it is the greatest. If we take $k \in \mathbb{N}$ such that $k \mid a$ and $k \mid b$, then we need to deduce that $k \leq d$. Since $k \mid a$ and $k \mid b$, then $k \mid xa + yb = d$ (by Proposition 2.3), which implies that $|k| \leq |d|$ (by Proposition 2.4) and therefore, $k \leq d$ as desired. □

Remark 2.4. If $a, b \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, b) = 1$, then a and b are called *relatively prime* or *coprime*. In this case, by Bezout's Theorem (Theorem 2.3), there exists integers $x, y \in \mathbb{Z}$ such that $xa + yb = 1$.

3. Prime Numbers

Definition 3.1. A $p \in \mathbb{N}$ is called a prime number if

(1) $p \geq 2$
(2) the number $k \in \mathbb{N}$ such that $k \mid p$ are $k = 1$ and $k = p$.

Remark 3.2. If $n \in \mathbb{N}$ with $n \geq 2$, always $1, n \in \{k \in \mathbb{N} : k \mid n\}$. A number $p \geq 2$ if this set is the smallest possible.