Lecture 24, Oct. 25

24.1 Theorem (The Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$*

Since $b \neq 0$, either $b > 0$ or $b < 0$.

Case 1: Suppose $b > 0$. Let $q = \lfloor a/b \rfloor$ ($q \leq a/b$ and $q + 1 > a/b$). Let $r = a - qb$.

Proof. Since $q \leq a/b$ we have

$$\begin{aligned} qb &\leq a \\ 0 &\leq a - qb \\ 0 &\leq r \end{aligned}$$

Since $q + t > a/b$

$$\begin{aligned} (q+1)b &> a \\ qb + b &> a \\ b &> a - qb \\ b &> r \end{aligned}$$

Thus $r < b = |b|$ ☐

Another proof. Suppose $b > 0$ and $a \geq 0$. Consider the sequence

$$0b, 11b, 2b, 3b, \cdots$$

Eventually, the terms kb exceed a. Choose $q \geq 0$ so that $qb \leq a$ and $(q+1)b > a$. (In fact, we choose $q = max(S)$ where $S = \{t \geq - \mid tb \leq a\}$ and we have $S \neq \emptyset$ since $0 \in S$ and S is bounded above by $a + 1$)

Then we have

$$\begin{aligned} qb &\leq a \\ 0 \leq a &- qb \\ 0 &\leq r \end{aligned}$$

and

$$\begin{aligned} (q+1)b &> a \\ qb + b &> a \\ b &> a - qb \\ b &> r \end{aligned}$$

So $r < b = |b|$. ☐

Case 2: Suppose $b < 0$. Let $c = -b$ so $c > 0$. Using the result of Case 1 we can choose $p, r \in \mathbb{Z}$ so that $a = pc + r$ and $0 \leq r < c$. Then $a = -pb + r$. So we can choose $q = -p$ to get $a = qb + r$ and $0 \leq r < |b|$.

Proof of Uniqueness. Suppose that

$$a = qb + r \text{ with } 0 \leq r < |b|$$

and Suppose that

$$a = pb + s \text{ with } 0 \leq r < |b|$$

Suppose, for a contradiction, that $r \neq s$. Then $0 \leq r < s < |b|$. Since $r < s$ we have $s - r > 0$ Since $r \geq 0$ and $s < |b|$ we have $s - r \leq s < |b|$. Thus $0 < s - r < |b|$. Since $a = qb + r$ and $a = pb + s$,

$$\begin{aligned} qb + r &= pb + s \\ qb - pb &= s - r \\ (q - p)b &= s - r \end{aligned}$$

Thus $b \mid (s - r)$

...

Leads to contradiction.

Thus $r = s$.

...

Then $p = q$ □

24.2 Theorem (The Euclidean Algorithm with Back-substitution)**.** *Let $a, b \in \mathbb{Z}$, and let $d = gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$.*

The proof of the theorem provides an **Algorithm** (that is a systematic procedure) called the **The Euclidean Algorithm** for computing $d = gcd(a, b)$ and an algorithm, called **Back-Substitution**, for finding $s, t \in \mathbb{Z}$ such that $as + bt = d$.