Lecture 25, Oct. 26

25.1 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 $as + bt = d$.

Proof. If $b \mid a$, then $gcd(a, b) = |b|$ and we can take $s = 0$ and $t = \pm 1$ to get $as + bt = d$.

Suppose $b \nmid a$.

Then apply the Division Algorithm repeatedly to get

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\cdots$$

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n + 0$$

$$gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_n, 0) = r_n$$

Thus $d = gcd(a, b) = r_n$, the last non-zero remainder.

We have

$$\begin{aligned} d = r_n =& r_{n-2} - q_n r_{n-1} \\ =& S_0 r_{n-2} + S_1 (r_{n-3} - q_{n-1} r_{n-2}) \text{ where } S_0 = 1 \text{ and } S_1 = -q_n \\ =& S_1 r_{n-3} + (S_0 - q_{n-1} S_1) r_{n-2} \\ =& S_1 r_{n-3} + S_2 r_{n-2} \text{ where } S_2 = S_0 - q_{n-1} S_1 \end{aligned}$$

We have a sequence $(S_l)_{l \geq 0}$ by $S_0 = 1$, $S_1 = -q_n$ and

$$S_{l+1} = S_{l-1} - q_{n-l} S_l$$

We claim that

$$d = r_k = S_{l-1} r_{n-l-1} + S_l r_{n-l}.$$

Proof by induction: $\cdots$. $\square$

25.2 Example. Let $a = 5151$ and $b = 1632$. Find $d = gcd(a, b)$ and find $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Solution.

$$5151 = 1632 \cdot 3(q_1) + 255$$
$$1632 = 255 \cdot 6(q_2) + 102$$
$$255 = 102 \cdot 2(q_3) + 51$$
$$102 = 51 \cdot 2 + 0$$

Thus $d = gcd(a, b) = 51$

$$S_0 = 1$$
$$S_1 = -q_3 = -2$$
$$S_2 = S_0 - S_1 q_2 = 13$$
$$S_3 = S_1 - S_2 q_1 = -41$$

So we can take $s = 13$ and $t = -41$ to get $as + bt = d$

25.3 Example. Let $a = 754$ and $b = -3973$. Find $d = gcd(a, b)$ and find $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Solution.

$$3973 = 754 \cdot 5(q_1) + 203$$
$$754 = 203 \cdot 3(q_2) + 145$$
$$203 = 145 \cdot 1(q_3) + 58$$
$$145 = 58 \cdot 2(q_4) + 29$$
$$58 = 29 \cdot 2 + 0$$

Thus $d = gcd(a, b) = 29$

$$S_0 = 1$$
$$S_1 = -q_4 = -2$$
$$S_2 = S_0 - S_1 q_3 = 3$$
$$S_3 = S_1 - S_2 q_2 = -11$$
$$S_4 = S_2 - S_3 q_1 = 58$$

Thus $(3973)(-11) + (754)(58) = 29$

Thus we can take $s = 58$ and $t = 11$ to get $as + bt = d$

25.4 Theorem (More Properties of GCD)**.** *Let $a, b, c \in \mathbb{Z}$*

1. *if $c \mid a$ and $c \mid b$ then $c \mid gcd(a, b)$*
2. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ iff $gcd(a, b) \mid c$*

3. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$ iff $gcd(a, b) = 1$*

4. *if $d = gcd(a, b) \neq 0$ (which is the case unless $a = b = 0$) then $gcd(a/d, b/d) = 1$*

5. *if $a \mid bc$ and $gcd(a, b) = 1$ then $a \mid c$*

Proof. 5. Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid bc$ and $gcd(a, b) = 1$. Since $a \mid bc$, choose $k \in \mathbb{Z}$ such that $bc = ak$. Since $gcd(a, b) = 1$, we can choose $s, t \in \mathbb{Z}$ such that $as + bt = 1$. Then $c = c \cdot 1 = c \cdot (as + bt) = acs + bct = acs + akt = a(cs + kt)$. So $a \mid c$

$\square$