Math 3510 Handout 2
02/16/16
Facts from Number Theory

Division Algorithm for $\mathbb{Z}$
If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \quad \text{and} \quad 0 \leq r < m.$$

Greatest common divisor
The greatest common divisor of two positive integers m and n is usually defined as the greatest integer d with $1 \leq d \leq \min\{m, n\}$ such that d is a divisor of both m and n.

Theorem If m and n are positive integers, then the greatest common divisor of m and n is the the least positive integer d such that $d = km + ln$ for some **integers** k and l.

Lemma 1 Let m and n be positive integers. If $d = km + ln$ for some integers $k, l \in \mathbb{Z}$ and d is the least positive integer of this form, then d is a common divisor of m and n.

Proof Consider the set
$$H = \{km + ln \mid k, l \in \mathbb{Z}\}.$$
One can show that H is a group. By Theorem 6.6, H is cyclic, and thus there is a positive integer d such that $H = \langle d \rangle$. Now $n = 0 \cdot m + 1 \cdot n$ and $m = 1 \cdot m + 0 \cdot n$ are both in H. Thus d is a common divisor of m and n. $\square$

Lemma 2 Let m and n be positive integers, and let $d = km + ln$ for some $k, l \in \mathbb{Z}$. If d' is any common divisor of m and n, then d' is a divisor of d.

Proof If d' is a common divisor of m and n, then d' is a divisor of $km + ln = d$.

$\square$

Lemma 3 Let m and n be positive integers and d be the greatest common divisor of m and n. Then there exist $k, l \in \mathbb{Z}$ such that $d = km + ln$.

Proof Perform Euclid's division algorithm repeatedly: let $n = a_0$ and $m = a_1$, then there exist q_1 and a_2 such that
$$a_0 = a_1 q_1 + a_2 \quad \text{and} \quad 0 \leq a_2 < a_1.$$
Repeating this, we get q_2 and a_3 such that

$$a_1 = a_2 q_2 + a_3.$$

Etc. The remainders $a_1 > a_2 > a_3 > \ldots \geq 0$. Thus there is integer t such that $a_{t+1} = 0$. We would have

$$a_{t-2} = a_{t-1} q_{t-1} + a_t$$

and
$$a_{t-1} = a_t q_t + a_{t+1} = a_t q_t.$$
Then we can argue that $d = a_t$: on the one hand, any common divisor of m and n would be a divisor of each of $a_2, a_3, \ldots, a_t$; on the other hand, any divisor of a_t is also a divisor of $a_{t-1}, \ldots, a_2, a_1, a_0$. Finally, every number in the sequence $a_2, a_3, \ldots, a_t$ can be written as $km + ln$ for some $k, l \in \mathbb{Z}$. In particular $a_t = d$ is of the form $km + ln$ for $k, l \in \mathbb{Z}$. $\square$

Relatively prime
Two positive integers are relatively prime if there greatest common divisor is 1.

Theorem If m and n are relatively prime and n divides km, then n divides k.

Proof Let $a, b \in \mathbb{Z}$ be such that $1 = am + bn$. Then $k = akm + bkn$. Now n is a divisor of both km (therefore akm) and bkn, so it is a divisor of k. $\square$