Lecture 19

Instructor's Comments: Do these proofs if you missed them. Otherwise review the theorems with examples.

Theorem: (Bézout's Lemma (Extended Euclidean Algorithm - EEA)) Let $a, b \in \mathbb{Z}$. Then there exist integers x, y such that $ax + by = d$

Proof: We've seen the outline of the proof via an example. Just make the argument abstract. The proof is left as a reading exercise. ■

Theorem: GCD Characterization Theorem (GCDCT) If $d > 0$, $d \mid a$, $d \mid b$ and there exist integers x and y such that $ax + by = d$, then $d = \gcd(a, b)$.

Proof: Let $e = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, by maximality we have that $d \leq e$. Now $e \mid a$ and $e \mid b$ so by Divisibility of Integer Combinations, $e \mid (ax + by) = d$. Thus, by Bounds by Divisibility, $|e| \leq |d|$ and since $d, e > 0$, we have that $e \leq d$. Hence $d = e$. ■

Example: $6 > 0$, $6 \mid 30$, $6 \mid 42$ and $30(3) + 42(-2) = 6$ and hence by the GCD Characterization Theorem, we have that $\gcd(30, 42) = 6$.

Example: Prove if $a, b, x, y \in \mathbb{Z}$, are such that $\gcd(a, b) \neq 0$ and $ax + by = \gcd(a, b)$, then $\gcd(x, y) = 1$.

Proof: Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, we divide by $\gcd(a, b) \neq 0$ to see that

$$\frac{a}{\gcd(a, b)}x + \frac{b}{\gcd(a, b)}y = 1$$

Since $1 \mid x$ and $1 \mid y$ and $1 > 0$, GCD Characterization Theorem implies that $\gcd(x, y) = 1$. ■

Instructor's Comments: This is the 10 minute mark.

Now, we've reached the point where we can prove Euclid's Lemma.

Theorem: (Euclid's Lemma - [Primes and Divisibility PAD]). If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Suppose p is prime, $p \mid ab$ and $p \nmid a$ (possible by elimination). Since $p \nmid a$, $\gcd(p, a) = 1$. By Bézout's Lemma, there exist $x, y \in \mathbb{Z}$ such that

$$\begin{aligned} px + ay &= 1 \\ pbx + aby &= b \end{aligned}$$

Now, since $p \mid p$ and $p \mid ab$, by Divisibility of Integer Combinations, $p \mid p(bx) + ab(y)$ and hence $p \mid b$.

Instructor's Comments: This is the 20 minute mark

Handout or Document Camera or Class Exercise

Prove or disprove the following:

(i) If $n \in \mathbb{N}$ then $\gcd(n, n+1) = 1$.

(ii) Let $a, b, c \in \mathbb{Z}$. If $\exists\, x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$ then $\gcd(a, b) \mid c$.

(iii) Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, b) \mid c$ then $\exists\, x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$.

Solution:

(i) $n + 1 = n(1) + 1$ and so by the GCD Characterization Theorem, $\gcd(n+1, n) = \gcd(n, 1) = 1$. Hence this is true.

(ii) $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. Thus, by Divisibility of Integer Combinations, $\gcd(a, b) \mid (ax^2 + by^2)$ which implies that $\gcd(a, b) \mid c$. Hence this is true.

(iii) This is false. Suppose that $a = 3$, $b = 0$ and $c = 6$. Then $\gcd(a, b) = 3 \mid 6 = c$ however, $3x^2 + 0y^2 = 6$ implies that $x^2 = 2$, a contradiction.

Instructor's Comments: This is the 30-35 minute mark. At the end of this lecture, I think it would be wise to talk about the midterm a bit. It is coming up so I've left a bit of extra time to review for the midterm.