Lecture 20

Handout or Document Camera or Class Exercise

Instructor's Comments: This is where things might start to differ. The idea at this point is to make the Monday lecture the Extended Euclidean Algorithm because this is a computational topic and it would help ease the lecture before the midterm. Thus, this lecture and lecture 21 can be swapped without harm. I'm going to give the gcd theorem lecture here and delay the EEA lecture until Lecture 21.

Instructor's Comments: This may or may not be a Friday lecture. Friday lectures I reserve time to do a clicker question. Modify accordingly.

Which of the following statements is false?

A) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \leq b \;\wedge\; \gcd(a,b) \leq a)$

B) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \neq 0 \implies (a \neq 0) \;\vee\; (b \neq 0))$

C) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \mid a \;\wedge\; \gcd(a,b) \mid b)$

D) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (((c \mid a) \;\wedge\; (c \mid b)) \;\wedge\; \gcd(a,b) \neq 0 \implies c \leq \gcd(a,b))$

E) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \gcd(a,b) \geq 0$

Solution: The first is false. Consider $a = b = -1$. The second is true (use the contrapositive). The third is true by definition (mention the $a = b = 0$ case). The fourth is also true by definition. The fifth is true again by definition.

In this lecture, we'll go over some key gcd theorems that you will need to prove some problems on your assignment.

Instructor's Comments: IMPORTANT TIP: If the gcd condition appears in the hypothesis, then Bézout's Lemma (EEA) might be useful. If the gcd condition appears in the conclusion, then GCDCT might be useful. It might be good to rewrite GCDCT on the board: if d is a positive integer and a common divisor of a and b and gcd(a,b) is an integer linear combination of a,b. Then gcd(a,b) = d.

Handout or Document Camera or Class Exercise

Example: Let $a, b, c \in \mathbb{Z}$. Prove if $\gcd(ab, c) = 1$ then $\gcd(a, c) = \gcd(b, c) = 1$.

Example: State the converse of the previous statement and prove or disprove.

Proof: By Bézout's Lemma, there exists $x, y \in \mathbb{Z}$ such that $ab(x) + c(y) = 1$. Since $1 \mid a$ and $1 \mid c$ and $a(bx) + c(y) = 1$, by the GCD Characterization Theorem, $\gcd(a, c) = 1$. Similarly, $\gcd(b, c) = 1$. ■

Proof: If $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$. Since $\gcd(a, c) = 1$, Bézout's Lemma, there exists integers x and y such that $ax+cy = 1$. Similarly, there exists integers k and m such that $bk + cm = 1$. Multiplying gives

$$\begin{aligned} 1 &= (ax + cy)(bx + cm) \\ &= abx^2 + acxm + bcyx + c^2ym \\ &= abx^2 + c(axm + byx + xym) \end{aligned}$$

Since $1 \mid ab$, $1 \mid c$ and $1 > 0$, by GCD Characterization theorem, $\gcd(ab, c) = 1$. ■

Instructor's Comments: This is the 10-15 minute mark

Note: IMPORTANT TIP: If the gcd condition appears in the hypothesis, then EEA or Bézout's theorem is useful. If the gcd condition appears in the conclusion, then GCDCT is useful.

Proposition: (GCD of One) (GCDOO). Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if there exists integers x and y such that $ax + by = 1$.

Proof: Suppose $\gcd(a, b) = 1$. Then by Bézout's Lemma, there exists integers x and y such that $ax + by = 1$.

Now, suppose that there exist integers x and y such that $ax + by = 1$. Then since $1 \mid a$ and $1 \mid b$, then by the GCD Characterization Theorem, $\gcd(a, b) = 1$. ■

Instructor's Comments: This is the 25 minute mark

Proposition: Division by the GCD (DBGCD). Let $a, b \in \mathbb{Z}$. If $\gcd(a, b) = d$ and $d \neq 0$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof: Suppose that $\gcd(a, b) = d \neq 0$. Then by Bézout's Lemma, there exist integers x and y such that $ax + by = d$. Dividing by the nonzero d gives $\frac{a}{d}x + \frac{b}{d}y = 1$. Thus, by GCDOO, we see that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. ■

Example: Let $a = 91$ and $b = 70$. Then $\gcd(a, b) = 7$ and by DBGCD, we have that

$$1 = \gcd(\tfrac{a}{d}, \tfrac{b}{d}) = \gcd(\tfrac{91}{7}, \tfrac{70}{7}) = \gcd(13, 10).$$

Instructor's Comments: This is the 35-37 minute mark

Definition: We say that two integers a and b are coprime if $\gcd(a, b) = 1$.

Proposition: Coprimeness and Divisibility (CAD). If $a, b, c \in \mathbb{Z}$ and $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

Proof: Suppose that $\gcd(a, c) = 1$ and $c \mid ab$. Since $\gcd(a, c) = 1$, by Bézout's Lemma, there exists integers x and y such that $ax + cy = 1$. Multiplying by b gives $abx + cby = b$. Since $c \mid ab$ and $c \mid c$, by Divisibility of Integer Combinations, we have that $c \mid (ab(x) + c(by))$ and hence $c \mid b$. ■

Example: Let $a = 14$, $b = 30$ and $c = 15$. Then $c \mid ab$ since $15 \mid (14)(30) = 420$ and $\gcd(a, c) = \gcd(14, 15) = 1$. Thus, by CAD, $c \mid b$ or $15 \mid 30$.

Instructor's Comments: This is the 50 minute mark. Remind students of the theorem cheat sheets on the website.