Lecture 18

Proposition: GCD With Remainder (GCDWR) If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

Proof: (of GCDWR) If $a = b = 0$, then $r = a - bq = 0$. Hence $\gcd(a, b) = 0 = \gcd(b, r)$. Now assume that $a \neq 0$ or $b \neq 0$. Let $d = \gcd(a, b)$ and $e = \gcd(b, r)$. Since $a = bq + r$ and $d \mid a$ and $d \mid b$, by Divisibility of Integer Combinations, $d \mid (a - bq) = r$. Thus, since e is the maximal common divisor of b and r, we see that $d \leq e$.

Now, $e \mid b$ and $e \mid r$ so by Divisibility of Integer Combinations, $e \mid (bq + r) = a$. Since d is the largest divisor of a and b, we see that $e \leq d$.

Hence $d = e$. ■

Instructor's Comments: This is the 7-10 minute mark

Handout or Document Camera or Class Exercise

Prove that $\gcd(3s+t, s) = \gcd(s, t)$ using GCDWR.

Solution: $3s + t = (3)s + t$. Thus, GCD With Remainders states that $\gcd(3s+t, s) = \gcd(s, t)$ by setting $a = 3s + t$, $b = s$, $q = 3$ and $r = t$. ■

Instructor's Comments: This is the 15 minute mark

Euclidean Algorithm How can we compute the greatest common divisor of two numbers quickly? This is where we can combine GCD With Remainders and the Division Algorithm in a clever way to come up with an efficient algorithm discovered over 2000 years ago that is still used today.

Example: Compute $\gcd(1239, 735)$.

Solution:

$$\begin{aligned} 1239 &= 735(1) + 504 && \text{Eqn 1} \\ 725 &= 504(1) + 231 && \text{Eqn 2} \\ 504 &= 231(2) + 42 && \text{Eqn 3} \\ 231 &= 42(5) + 21 && \text{Eqn 4} \\ 42 &= 21(1) + 0 \end{aligned}$$

Thus, by GCDWR, we have

$$\begin{aligned} \gcd(1239, 735) &= \gcd(735, 504) \\ &= \gcd(504, 231) \\ &= \gcd(231, 42) \\ &= \gcd(42, 21) \\ &= \gcd(21, 0) \\ &= 21 \end{aligned}$$

Note: This process stops since remainders form a sequence of non-negative decreasing integers. In this process, the greatest common divisor is the last nonzero remainder.

Instructor's Comments: This is the 25 minute mark

Question: Food for thought: What is the runtime of the Euclidean Algorithm?

Back Substitution Remember our goal for GCDs is to prove Euclid's Lemma. It turns out that this question is deeply connected to the following question:

Question: Do there exist integers x and y such that $ax + by = \gcd(a, b)$?

It turns out that the answer to this question is yes! This result is known as Bézout's Lemma (or EEA in this course). We first show this is true in an example by using the method of Back Substitution and then later using the Extended Euclidean Algorithm. Using the $\gcd(1239, 735) = 21$ example from before, we start with the last line and work our way backwards to see:

$$\begin{aligned} 21 &= 231(1) + 42(-5) && \text{By Eqn 4} \\ &= 231(1) + (504(1) + 231(-2))(-5) && \text{By Eqn 3} \\ &= 231(11) + 504(-5) \\ &= (735(1) + 504(-1))(11) + 504(-5) && \text{By Eqn 2} \\ &= 735(11) + 504(-16) \\ &= 735(11) + (1239 + 735(-1))(-16) && \text{By Eqn 1} \\ &= 735(27) + 1239(-16) \end{aligned}$$

Instructor's Comments: This is the 35 minute mark

Handout or Document Camera or Class Exercise

Use the Euclidean Algorithm to compute $\gcd(120, 84)$ and then use back substitution to find integers x and y such that $\gcd(120, 84) = 120x + 84y$.

Instructor's Comments: If a student finishes quickly, challenge them to find two such linear combinations.

Solution:

$$\begin{aligned} 120 &= 84(1) + 36 \\ 84 &= 36(2) + 12 \\ 36 &= 12(3) + 0 \end{aligned}$$

Thus, by the Euclidean Algorithm (or by GCDWR), we have that $\gcd(120, 84) = 12$. Next,

$$\begin{aligned} 12 &= 84 + 36(-2) \\ &= 84 + (120 + 84(-1))(-2) \\ &= 84(3) + 120(-2) \end{aligned}$$

Note: Food for thought: Note also that $84(3 + 120) + 120(-2 - 84)$ will also work and so on.

Instructor's Comments: This is the 45 minute mark

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

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 definition and the maximality of e we have that $d \leq e$. Again by definition, $e \mid a$ and $e \mid b$ so by Divisibility of Integer Combinations, $e \mid (ax + by)$ implying that $e \mid d$. Thus, by Bounds by Divisibility, $|e| \leq |d|$ and since $d, e > 0$, we have that $e \leq d$. Hence $d = e$. ■

Instructor's Comments: This is the 50 minute mark