Lecture 18

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. ■

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

$$px + ay = 1$$
$$pbx + aby = b$$

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

Corollary: (Generalized Euclid's Lemma) Suppose $a_1, a_2, ..., a_n \in \mathbb{Z}$ and p is a prime number. Show that if $p \mid a_1 a_2 ... a_n$ then $p \mid a_i$ for some integer $1 \leq i \leq n$.

Proof: Exercise using induction.

Instructor's Comments: This is the 50 minute mark