Lecture 17

Greatest Common Divisors

Instructor's Comments: Arguably, this is the toughest portion of the course. These arguments for gcds are often tricky and counter intuitive and take a bit of practice before mastering.

As an exercise, let's list the divisors of 84:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 12, \pm 14, \pm 21, \pm 28, \pm 42, \pm 81$$

Divisors of 120:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 10, \pm 12, \pm 15, \pm 20, \pm 24, \pm 30, \pm 40, \pm 60, \pm 120$$

Hence the greatest common divisors of 84 and 120 is 12.

Definition: The *greatest common divisors* of integers a and b with $a \neq 0$ or $b \neq 0$ is an integer $d > 0$ such that

(i) $d \mid a$ and $d \mid b$

(ii) If $c \mid a$ and $c \mid b$, then $c \leq d$

We write $d = \gcd(a, b)$.

Note:

(i) $\gcd(a, a) = |a| = \gcd(a, 0)$

(ii) Define $\gcd(0, 0) = 0$. Note that $\gcd(a, b) = 0 \Leftrightarrow a = b = 0$

(iii) **Exercise:** $\gcd(a, b) = \gcd(b, a)$

Instructor's Comments: This is the 10 minute mark

Claim: $\gcd(a, b)$ exists.

Proof: Suppose that $a \neq 0$ or $b \neq 0$. Clearly $1 \mid a$ and $1 \mid b$ so a divisor exists.

To show there is a greatest common divisor, it suffices to show that there is an upper bound on common divisors of a and b. If d is a positive integer such that $d \mid a$ and $d \mid b$, then Bounds by Divisibility states that $d \leq |a|$ and $d \leq |b|$. Hence,

$$1 \leq d \leq \min\{|a|, |b|\}$$

Since the range on divisors is bounded, there must be a maximum. ∎

Instructor's Comments: This is more of a pedantic proof but it sets up the idea for all future GCD proofs without tools so is worth talking about.

Claim: $\gcd(a, b)$ is unique.

Proof: Suppose d and e are both the greatest common divisors of a and b. Then $d \mid a$ and $d \mid b$. Thus, since e is maximal, $d \leq e$. Similarly, $e \leq d$. Hence $d = e$.

Instructor's Comments: This is the 10 minute mark

Handout or Document Camera or Class Exercise

Example: Prove that $\gcd(3a+b, a) = \gcd(a, b)$ using the definition directly.

Proof: . Let $d = \gcd(3a+b, a)$ and $e = \gcd(a, b)$. Then by definition, $d \mid (3a+b)$ and $d \mid a$. By Divisibility of Integer Combinations,

$$d \mid (3a+b) - 3a = b$$

Since e is the maximal divisor of a and b, we have that $d \leq e$.

Now, since $e \mid a$ and $e \mid b$, Divisibility of Integer Combinations gives us that $e \mid (3a+b)$. Since d is maximal, $e \leq d$. Hence $d = e$. ■

Instructor's Comments: This is the 20 minute mark

Instructor's Comments: This is the 30 minute mark. From this point on in the course, the theorem cheat sheets on the Math 135 Resources page will be quite useful for students. There will be many named theorems that students will be expected to know.. Don't rush the next example. Maybe do it in this lecture and review it a bit in the next lecture. GCDWR works very well if the two parameters in the greatest common divisor depend on each other in some way.

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

Example: $\gcd(72, 40) = 8$. Now, $72 = 40(2) - 8$ and so GCD With Remainder says that

$$\gcd(72, 40) = \gcd(40, -8) = 8$$

Note that this looks similar to the division algorithm, but the 'remainder' here can be negative. You can apply this multiple times to help reduce the gcd computation a lot (this we will see later).

Instructor's Comments: Delay the proof until next class. Talk about the previous example more - maybe even It's included here only if my timings above are incorrect.

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: Compare and contrast to the quickness of using the theorem with the 'by hand' method earlier in this lecture

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 probably a theorem you could omit/rush if needed. It has few applications for us and many could intuit fairly quickly. It IS however a good example of using elimination which they will likely need on their midterm.

Suppose we wanted to find a divisors of two numbers a and b. Can we do so? How far do we have to look? Here is a theorem explaining this.

Proposition: (Finding a Prime Factor) (FPF) Let $a, b \in \mathbb{N}$. If $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof: Suppose $n = ab$ and $a > \sqrt{n}$. Then

$$\begin{aligned} ab &> b\sqrt{n} \\ n &> b\sqrt{n} \\ \sqrt{n} &> b \end{aligned}$$

Hence $b \leq \sqrt{n}$. ∎