Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 5

Euclid's Theorem [INF P]

- There exist infinitely many primes
- Idea: Argue by contradiction that there are finitely many primes and consider the number

$$N = 1 + \prod_{i=1}^{n} p_i$$

- Then note by Divisibility of Integer Combinations that

$$p \left| \left(N - \prod_{i=1}^{n} p_i \right) = 1 \right.$$

Greatest Common Divisor

- **Definition:** The *greatest common divisor* of integers a and b with $a \neq 0$ or $b \neq 0$ is an integer $d > 0$ such that
  1. $d \mid a$ and $d \mid b$
  2. If $c \mid a$ and $c \mid b$, then $c \leq d$

  We write $d = \gcd(a, b)$.
- $\gcd(120, 84) = 12$, $\gcd(0, 0) = 0$, $\gcd(a, b) = \gcd(b, a)$, $\gcd(a, a) = |a| = \gcd(a, 0)$
- $\gcd(a, b)$ exists and is unique.

GCD With Remainder [GCDWR]

- **Theorem:** GCD With Remainder (GCDWR) If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.
- Watch the $a = b = 0$ case
- **Proof:** 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, $d \mid a + b(-q)$ and hence $d \mid r$. 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, $e \mid b(q) + r(1)$ and hence $e \mid a$. Since d is the largest divisor of a and b, we see that $e \leq d$.

  Hence $d = e$. ■

Euclidean Algorithm

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

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

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

Back Substitution

Find $x, y \in \mathbb{Z}$ such that $1239x + 735y = \gcd(1239, 735)$.

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

$$
\begin{aligned}
21 &= 231(1) + 42(-5) && \text{By Eqn 4} \\
&= 231(1) \\
&\quad + (504(1) + 231(-2))(-5) && \text{By Eqn 3} \\
&= 231(1) + 504(-5) + 231(10) \\
&= 231(11) + 504(-5) \\
&= (735(1) + 504(-1))(11) \\
&\quad + 504(-5) && \text{By Eqn 2} \\
&= 735(11) + 504(-16) \\
&= 735(11) \\
&\quad + (1239 + 735(-1))(-16) && \text{By Eqn 1} \\
&= 735(27) + 1239(-16)
\end{aligned}
$$

Bézout's Lemma [EEA]

Theorem: Let $a, b \in \mathbb{Z}$. Then there exist integers x, y such that $ax + by = \gcd(a, b)$.

GCD Characterization Theorem [GCDCT]

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

GCD Characterization Theorem [GCDCT]

Theorem: 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 $d = e$. ■

Mixed Examples

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

Mixed Examples

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

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

Mixed Examples

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

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

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

Mixed Examples

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 $\gcd(x, y) = 1$. ■

Good 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.

Euclid's Lemma or 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 $p \mid b$.

GCD of One [GCDOO]

Proposition: 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, $\gcd(a, b) = 1$. ■

Division by the GCD [DBGCD]

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

Division by the GCD [DBGCD]

Proposition: 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 $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. ■

Coprimeness and Divisibility [CAD]

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

Coprimeness and Divisibility [CAD]

Proposition: 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 $c \mid ab$, there exists an integer k such that $ab = ck$. Substituting gives $ckx + cby = b$. Thus $c(kx + by) = b$ and so $c \mid b$ since $kx + by \in \mathbb{Z}$. ■

Summary

- Lots of theorems this week (INF P, FPF, GCDWR, EEA, PAD, GCDCT, GCDOO, DBGCD, CAD, etc.)
- Theorem Cheat Sheets are available on the Math 135 Resources Page.
- Practice recalling theorems with **and without** the cheat sheets.
- Practice mixing the use of theorems.
- Toolbox analogy.