Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 6

Extended Euclidean Algorithm

- Gives a fast way to compute $\gcd(a, b)$ and integers x and y such that
$$\gcd(a, b) = ax + by$$

Extended Euclidean Algorithm Example

Find $x, y \in \mathbb{Z}$ such that $506x + 391y = \gcd(506, 391)$.

Extended Euclidean Algorithm Example

Find $x, y \in \mathbb{Z}$ such that $506x + 391y = \gcd(506, 391)$.

x	y	r	q
1	0	506	0
0	1	391	0
1	-1	115	$\left\lfloor \frac{506}{391} \right\rfloor = 1$
-3	4	46	$\left\lfloor \frac{391}{115} \right\rfloor = 3$
7	-9	23	$\left\lfloor \frac{115}{46} \right\rfloor = 2$
-17	22	0	$\left\lfloor \frac{46}{23} \right\rfloor = 2$

Therefore, $506(7) + 391(-9) = 23 = \gcd(506, 391)$.

Notes on EEA

1. Bézout's Lemma is the Extended Euclidean Algorithm in the textbook.
2. With $\gcd(a, b)$, what if
    1. $b > a$? Then swap a and b. This works since $\gcd(a, b) = \gcd(b, a)$.
    2. $a < 0$ or $b < 0$? Solution is to make all the terms positive. This works since
    $$\gcd(a, b) = \gcd(|a|, |b|).$$
3. In practice, one can accomplish these goals by changing the headings then accounting for this in the final steps. (Examples can be found on the lecture notes on EEA)

Fundamental Theorem of Arithmetic (UFT)

Suppose that $n > 1$ is an integer. Then n can be factored uniquely as a product of prime numbers up to reordering of prime numbers.

Divisors From Prime Factorization (DFPF)

Theorem: Divisors From Prime Factorization (DFPF). Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where each $\alpha_i \geq 1$ is an integer. Then d is a positive divisor of n if and only if a prime factorization of d can be given by

$$d = \prod_{i=1}^{k} p_i^{\delta_i} \qquad \text{where } \delta_i \in \mathbb{Z}, 0 \leq \delta_i \leq \alpha_i \text{ for } 1 \leq i \leq k$$

Example: Positive divisors of $63 = 3^2 \cdot 7$ are given by

$$3^0 \cdot 7^0, 3^0 \cdot 7^1, 3^1 \cdot 7^0, 3^1 \cdot 7^1, 3^2 \cdot 7^0, 3^2 \cdot 7^1$$

or

$$1, 7, 3, 21, 9, 63$$

GCD From Prime Factors (GCDPF)

Theorem: GCD From Prime Factors (GCDPF). If

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{k} p_i^{\beta_i}.$$

where $0 \le \alpha_i$ and $0 \le \beta_i$ are integers and the p_i are distinct primes, then

$$\gcd(a, b) = \prod_{i=1}^{k} p_i^{m_i}$$

where $m_i = \min\{\alpha_i, \beta_i\}$ for $1 \le i \le k$.

Example:

$$\begin{aligned}
\gcd(20000, 30000) &= \gcd(2^5 \cdot 3^0 \cdot 5^4, 2^4 \cdot 3^1 \cdot 5^4) \\
&= 2^{\min\{4,5\}} \cdot 3^{\min\{0,1\}} \cdot 5^{\min\{4,4\}} \\
&= 2^4 \cdot 5^4 \\
&= 10000
\end{aligned}$$

Tips for GCD Problems

When tackling a GCD type problem, try the following tips in order

- (HWY 401) Use key theorems especially the following:
  - Bézout's Theorem (EEA) [Good when gcd is in hypothesis].
  - GCDWR [Good when terms in gcd depend on each other; good for computations].
  - GCDCT [Good when gcd is in conclusion].
- (HWY 7) Use the definition of gcd.
- (Flying) Use prime factorizations.

Linear Diophantine Equation (LDE)

We want to solve $ax + by = c$ where $a, b, c \in \mathbb{Z}$ under the condition that $x, y \in \mathbb{Z}$

Linear Diophantine Equation (LDE)

We want to solve $ax + by = c$ where $a, b, c \in \mathbb{Z}$ under the condition that $x, y \in \mathbb{Z}$

Relate to the equation of a line

$y = \frac{-ax}{b} + \frac{c}{b}$

LDET1

Theorem: (LDET1) Let $d = \gcd(a, b)$. The LDE

$$ax + by = c$$

has a solution if and only if $d \mid c$.

LDET1

Theorem: (LDET1) Let $d = \gcd(a, b)$. The LDE

$$ax + by = c$$

has a solution if and only if $d \mid c$.

Proof: ($\Rightarrow$) Assume that $ax + by = c$ has an integer solution, say $x_0, y_0 \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, by Divisibility of Integer Combinations, we have that $d \mid (ax_0 + by_0) = c$.

($\Leftarrow$) Assume that $d \mid c$. Then, there exists an integer k such that $dk = c$. By Bézout's Lemma, there exist integers u and v such that $au + bv = \gcd(a, b) = d$. Multiplying by k gives

$$a(uk) + b(vk) = dk = c$$

Therefore, a solution is given by $x = uk$ and $y = vk$. $\blacksquare$

LDET2

(LDET2) Let $d = \gcd(a, b)$ where $a \neq 0$ and $b \neq 0$. If $(x, y) = (x_0, y_0)$ is a solution to the LDE $ax + by = c$ then all solutions are given by $\{(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n) : n \in \mathbb{Z}\}$

Proof: Note that the above are actually solutions to the LDE. It suffices to show that these are all the solutions. Let (x, y) be a different solution to the LDE (other than (x_0, y_0)). Then,

$$ax + by = c \qquad \text{and} \qquad ax_0 + by_0 = c$$

Subtracting gives

$$a(x - x_0) = -b(y - y_0) \quad \implies \quad \frac{a}{d}(x - x_0) = \frac{-b}{d}(y - y_0)$$

Now, since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ (by DBGCD) and since

$$\frac{b}{d} \mid \frac{-b}{d}(y - y_0) = \frac{a}{d}(x - x_0).$$

By CAD $\frac{b}{d} \mid (x - x_0)$. Thus, $\exists n \in \mathbb{Z}$ such that $x = x_0 + \frac{b}{d}n$. Hence

$$\frac{a}{d}(x - x_0) = \frac{-b}{d}(y - y_0) \quad \implies \quad \frac{a}{d} \cdot \frac{b}{d}n = \frac{-b}{d}(y - y_0)$$

Hence, $y = y_0 - \frac{a}{d}n$ completing the proof. ∎

LDE Example

Solve the LDE $20x + 35y = 15$.

LDE Example

Solve the LDE $20x + 35y = 15$.

Solution: Since $\gcd(20, 35) = 5$ and $5 \mid 15$, we see by LDET1 that we have a solution. Notice here that we can simplify the LDE by dividing by 5 first to give

$$4x + 7y = 3$$

An easy solution is given by $x = -1$ and $y = 1$. To find all solutions, we invoke LDET2 to see that all solutions are given by

$$x = -1 + \frac{7}{\gcd(4,7)}n \qquad y = 1 - \frac{4}{\gcd(4,7)}n$$

for all integers n. Note this is equivalent to the solution set

$$x = -1 - \frac{7}{\gcd(4,7)}n \qquad y = 1 + \frac{4}{\gcd(4,7)}n$$

The most important definition in this course

Definition: Let $m \in \mathbb{N}$. We say that two integers a and b are congruent modulo m if and only if $m \mid (a - b)$ and we write

$$a \equiv b \pmod{m}.$$

If $m \nmid (a - b)$, we write $a \not\equiv b \pmod{m}$.
Commit the previous definition to memory!!!

The most important definition in this course

Definition: Let $m \in \mathbb{N}$. We say that two integers a and b are congruent modulo m if and only if $m \mid (a-b)$ and we write

$$a \equiv b \pmod{m}.$$

If $m \nmid (a-b)$, we write $a \not\equiv b \pmod{m}$.

Commit the previous definition to memory!!!

Examples: $3 \equiv 7 \pmod{4}$, $10 \equiv -8 \pmod{9}$, $4 \equiv 4 \pmod{6}$