Intro to Discrete Structures Lecture 13

Pawel M. Wocjan

School of Electrical Engineering and Computer Science

University of Central Florida

wocjan@eecs.ucf.edu

The Euclidean Algorithm

Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then

$$\gcd(a, b) = \gcd(b, r)\,.$$

The Euclidean Algorithm

$$\underline{\underline{f \mid g}} \wedge \underline{\underline{g \mid f}} \Rightarrow f = g$$

$$\gcd(a,b) \mid \gcd(b,r) \wedge$$
$$\gcd(b,r) \mid \gcd(a,b) \Rightarrow \gcd(a,b) = \gcd(b,r)$$

$$\gcd(a,b) \mid a \wedge \gcd(a,b) \mid b \Rightarrow$$
$$\gcd(a,b) \mid ma + nb \text{ for all } m,n \in \mathbb{Z}$$
$$\Rightarrow \gcd(a,b) \mid r$$

$$\underbrace{\gcd(a,b)}_{d} \mid b \wedge \underbrace{\gcd(a,b)}_{d} \mid r$$
$$\Rightarrow \gcd(a,b) \mid \gcd(b,r)$$

The Euclidean Algorithm

Example 12: Find $\gcd(414, 662)$ using the Euclidean Algorithm.

$$\underbrace{662}_{a} = \underbrace{414}_{b} \cdot \underbrace{1}_{q} + \underbrace{248}_{r} \qquad \gcd(662,414) = \gcd(414,248)$$

$$414 = 248 \cdot 1 + 166$$

$$248 = 166 \cdot 1 + 82$$

$$166 = 82 \cdot 2 + 2$$

$$82 = \underline{\underline{2}} \cdot 41 + 0 \implies \gcd(662,414) = 2$$

Some Useful Facts

Theorem 1:

$$\forall a \, \forall b \, \exists s \, \exists t \; \gcd(a, b) = sa + tb \, .$$

The pair (s, t) can be efficiently computed with the extended Euclidean algorithm.

The Extended Euclidean Algorithm

Example 1: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

page 232

$$
\begin{aligned}
252 &= 1 \cdot \boxed{198} + \boxed{54} \\
198 &= 3 \cdot 54 + 36 \\
54 &= 1 \cdot 36 + \boxed{18} \\
36 &= 2 \cdot 18 + 0
\end{aligned}
$$

$36 = 198 - 3 \cdot 54$

$18 = 54 - 36$

$\gcd(252, 198) = 18$

$\gcd(36, 18) = \gcd(18, 0) = 18$

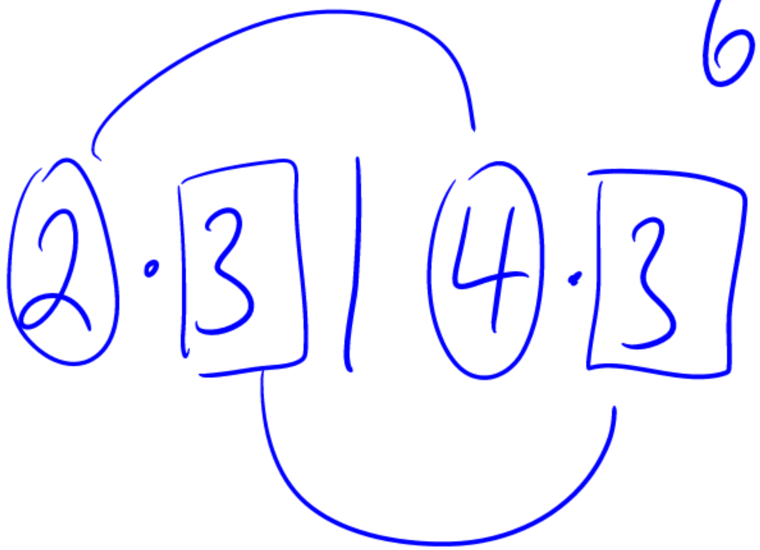
Some Useful Facts

Lemma 2: If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

$6 \mid 12$

$12 = 4 \cdot 3$

$6 = 2 \cdot 3$



Some Useful Facts

Lemma 1:

$$\gcd(a, b) = 1 \wedge a \mid bc \Rightarrow a \mid c$$

Proof of the uniqueness of the prime factorization of a positive integer:

$$\gcd(3,5) = 1 \qquad 3 \mid 5 \cdot 9 = 45$$

Mathematical Induction

Mathematical induction is based on the rule of inference

$$\begin{array}{lll} 1. & & P(1) \\ 2. & & \forall k\,(P(k) \rightarrow P(k+1)) \\ \hline 3. & \therefore & \forall n P(n) \end{array}$$

which is true for the domain of natural numbers $\mathbb{N}$.

Climbing an Infinite Ladder

1. We can reach the first rung of the ladder.
2. If we can reach a particular rung of the ladder, then we can reach the next rung of the ladder.
3. Therefore, we can reach any rung of the ladder.

Principle Mathematical Induction

To prove that $P(n)$ is true for all natural numbers n, where $P(n)$ is a propositional function, we complete two steps:

- Basis step: We verify that $P(1)$ is true.
- We show that the conditional statement

$$P(k) \to P(k+1)$$

is true for all natural numbers k.

Warning

- In a proof of mathematical induction is is **not** assumed that $P(k)$ is true for all k.
- It is only shown that **if it is assumed** that $P(k)$ is true, then $P(k+1)$ is also true.
- Thus, a proof of mathematical induction is not a case of begging the question, or circular reasoning.

Example

Example: Show that

$$P(n): \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \quad \text{is true.}$$

Basis step $P(1)$ $\quad 1 = \sum_{i=1}^{1} i = \frac{1(1+1)}{2} = 1$

Example

Inductive Step $\forall k\, P(k) \rightarrow P(k+1)$

assume that $P(k)$ is true

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

$P(k) \rightarrow P(k+1)$

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

Example

Example 2: Conjecture a formula for the sum of the first n positive integers. Then prove your conjecture using mathematical induction.

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2} \iff P(k+1) \text{ holds}$$

Example

The Number of Subsets of a Finite Set

The Number of Subsets of a Finite Set

DeMorgan for Intersection

Example 10: Prove

$$\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j}$$

whenever $A_1, A_2, \ldots, A_n$ are subset of a universal U and $n \geq 2$.

DeMorgan for Intersection

DeMorgan for Intersection

Creative Uses of Mathematical Induction

Example: Show that every $2^n \times 2^n$ checkerboard with one square removed can be tiled using L-shaped triominoes.

Creative Uses of Mathematical Induction

Strong Induction

Strong induction is based on the rule of inference

$$
\begin{array}{lll}
1. & & P(1) \\
2. & & \forall k \, (\wedge_{j=1}^{k} P(j) \rightarrow P(k+1)) \\
\hline
3. & \therefore & \forall n P(n)
\end{array}
$$

which is true for the domain of natural numbers $\mathbb{N}$.

Strong Induction

To prove that $P(n)$ is true for all natural numbers n, where $P(n)$ is a propositional function, we complete two steps:

- Basis step: We verify that $P(1)$ is true.
- We show that the conditional statement

$$\bigwedge_{j=1}^{k} P(j) \rightarrow P(k+1)$$

is true for all natural numbers k.

Existence of Prime Factorization

Example: Show that if n is an integer greater than 1, then n can be written as the product of primes.

Existence of Prime Factorization

Existence of Prime Factorization

Example 2: Show that if n is an integer greater than 1, then n can be written as the product of primes.

Winning Strategy

Example 3:

Winning Strategy

Winning Strategy

$$d = \gcd(a, b)$$

$$d \mid a \iff \exists k \quad a = k \cdot d$$

$$d \mid b \iff \exists l \quad b = l \cdot d$$

multiples of d

Let $m, n \in \mathbb{Z}$ be arbitrary.

$$ma + nb = mkd + nld$$

$$= (mk + nl) \cdot d$$

$$\iff d \mid (ma + nb)$$

$$d \mid e \wedge d \mid f$$

$$\Rightarrow d \mid \gcd(e, f)$$