# Introduction to Decision Sciences

## Lecture 8

Andrew Nobel

October 4, 2017

# Divisibility

# Factors and Multiples

**Definition:** Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say $a$ *divides* $b$, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$.

- $a$ is a *factor* of $b$
- $b$ is a *multiple* of $a$

**Fact 1:** Let $a, b, c \in \mathbb{Z}$

(a) If $a|b$ and $a|c$ then $a|(b+c)$

(b) If $a|b$ and $b|c$ then $a|c$

(c) If $a|b$ then $a|bc$ for all $c \in \mathbb{Z}$

**Corollary 2:** If $a|b$ and $a|c$ then $a|mb + nc$ for all $m, n \in \mathbb{Z}$

# Division Algorithm

**Fact:** Let $d \geq 1$ be a *divisor*. If $a \in \mathbb{Z}$ then there exists a unique *quotient* $q \in \mathbb{Z}$ and *remainder* $0 \leq r < d$ such that

$$a = q\,d + r \tag{0.1}$$

In this case we say "$r$ equals $a$ modulo $d$", written $r = a \bmod d$, meaning that $r$ is the remainder when $a$ is divided by $d$.

**Proof:** For each $k \in \mathbb{Z}$ let $A_k$ be the interval $\{kd + r : 0 \leq r < d\}$. Then

- $\mathbb{Z} = \bigcup_{k \in \mathbb{Z}} A_k$ (the intervals cover the integers)
- $A_i \cap A_j = \emptyset$ if $i \neq j$ (the intervals don't overlap)

Thus every $a \in \mathbb{Z}$ is in a unique interval $A_q$, which implies (0.1) for some $0 \leq r < d$.

# Modular Arithmetic

**Definition:** Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}_+$.

- $a$ is *congruent* to $b$ mod $m$, written $a \equiv b \pmod{m}$, if $m \mid (a - b)$

*Idea:* We can walk from $a$ to $b$ (or from $b$ to $a$) by taking steps of size $m$.

**Example:** The set of integers equivalent to $3$ mod $5$ is

$$\{k : k \equiv 3 \pmod{5}\} \;=\; \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$

**Fact:** $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$, that is, $a$ and $b$ have same remainder when divided by $m$.

# Basic Properties of Modular Arithmetic

**Fact 1:** $a \equiv b \pmod{m}$ iff $a = b + k\,m$ for some $k \in \mathbb{Z}$

**Fact 2:** If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

(a) $a + c \equiv (b + d) \pmod{m}$

(b) $ac \equiv (b\,d) \pmod{m}$

**Corollary 3**

- $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $(a\,b) \bmod m = ((a \bmod m)\,(b \bmod m)) \bmod m$

# Prime Numbers

# Prime Numbers

**Definition:** An integer $n \geq 2$ is *prime* if it is divisible only be $1$ and itself. Otherwise, it is *composite*.

**Examples**

- The number $2$ is prime, the only even prime.
- The numbers $3, 5, 7, 11, 13, 17, 19, 23, \ldots$ are prime
- The numbers $4, 6, 8, 9, 10, 12, \ldots$ are composite

# Prime Factorization

**Fundamental Theorem of Arithmetic:** Every integer $n \geq 2$ is prime or can be expressed uniquely as a product of primes, called the *prime factors* of $n$.

In other words, for every integer $n \geq 2$ there exist $r \geq 1$, primes $p_1, \ldots, p_r$, and integers $b_1, \ldots, b_r \geq 1$ such that

$$n = p_1^{b_1} \cdots p_r^{b_r}$$

and this representation of $n$ as a product of primes is unique.

**Corollary:** There are infinitely many primes.

# More on Primes

**Fact:** If $n$ is composite then it has a prime factor less than or equal to $\sqrt{n}$

**Example:** Show that $127$ is prime

# Prime Number Theorem

**Qu:** How frequently to primes occur among integers $1, 2, \ldots, n$?

**Definition:** For $n \geq 1$ let $\pi(n) =$ number of primes among $1, 2, \ldots, n$

**Prime Number Theorem:** As $n$ tends to infinity,

$$\frac{\pi(n)}{(n/\ln n)} \to 1 \quad \text{or equivalently} \quad \pi(n) \sim \frac{n}{\ln n}$$

Examples: $\pi(100) \approx 22$, $\pi(1000) \approx 145$, $\pi(10,000) \approx 1086$

By contrast, number of perfect squares among $1, 2, \ldots, n$ is roughly $\sqrt{n}$.

# Conjectures Concerning Primes

**Unsolved**

- Every even integer $n \geq 4$ is the sum of two primes.
- There are infinitely many primes of the form $p = n^2 + 1$, some $n \in \mathbb{N}$.
- There are infinitely many primes $p$ such that $p + 2$ is also prime.

**Solved**

- The primes contain arbitrarily long arithmetic sequences, i.e., sequences of the form $a, a + d, \ldots, a + kd$ (Green and Tau, 2006).

# Greatest Common Divisor

# Greatest Common Divisor

**Definition:** The greatest common divisor of $a, b \in \mathbb{Z}$, written $\gcd(a, b)$, is the largest integer $d$ such that $d \mid a$ and $d \mid b$.

**Claim 1:** $\gcd(a, b)$ is the largest element of the set $S = \{d : d \mid a\} \cap \{d : d \mid b\}$

**Claim 2:** $\gcd(a, b)$ is the unique integer $d \geq 1$ such that

- $d \mid a$ and $d \mid b$
- if $c \mid a$ and $c \mid b$ then $c \mid d$

# GCD and Factorization

Let $a, b \in \mathbb{N}_+$. By the fundamental theorem of arithmetic there exist primes $p_1, \ldots, p_m$ and integers $a_1, \ldots, a_m$ and $b_1, \ldots, b_m \geq 0$ such that

$$a = p_1^{a_1} \cdots p_m^{a_m} \quad \text{and} \quad b = p_1^{b_1} \cdots p_m^{b_m}$$

**Claim:** $\text{gcd}(a, b) = p_1^{\min(a_1,b_1)} \cdots p_m^{\min(a_m,b_m)}$

**Definition**

- $a, b$ are *relatively prime* if $\text{gcd}(a, b) = 1$
- $a_1, \ldots, a_n$ are *pairwise relatively prime* if $\text{gcd}(a_i, a_j) = 1$ for $i \neq j$

# Least Common Multiple

**Definition:** The least common multiple of $a, b \in \mathbb{N}_+$, written $\text{lcm}(a, b)$, is the smallest integer $r$ such that $a \mid r$ and $b \mid r$.

**Fact:** Let $a, b \in \mathbb{N}_+$ with prime factorizations

$$a = p_1^{a_1} \cdots p_m^{a_m} \text{ and } b = p_1^{b_1} \cdots p_m^{b_m}$$

(1) $1 \leq \text{lcm}(a, b) \leq a\, b$ is always well defined

(2) $\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_m^{\max(a_m, b_m)}$

(3) $a\, b = \text{lcm}(a, b)\, \text{gcd}(a, b)$

# The Euclidean Algorithm

**Goal:** Find gcd$(a, b)$ without using prime factorization of $a, b$

**Fact:** If $a = bq + r$ then gcd$(a, b) =$ gcd$(b, r)$.

**Algorithm:** To find gcd$(r_0, r_1)$ with $r_0 \geq r_1 \geq 1$ proceed as follows

- By division algorithm $r_0 = r_1 q_1 + r_2$ with $0 \leq r_2 < r_1$
- By division algorithm $r_1 = r_2 q_2 + r_3$ with $0 \leq r_3 < r_2$
- Continue until $r_{m-1} = q_m r_m$ (remainder is zero)
- By Fact, gcd$(r_0, r_1) =$ gcd$(r_1, r_2) = \cdots =$ gcd$(r_{m-1}, r_m) = r_m$

# Bezout's Theorem

**Theorem:** If $a, b \in \mathbb{N}_+$ then gcd$(a, b) = as_0 + bt_0$ for some $s_0, t_0 \in \mathbb{Z}$.

**Proof:** Define the set $S = \{as + bt : s, t \in \mathbb{Z}\}$.

- Note that $a, b \in S$.
- Let $c = as_0 + bt_0$ be the smallest positive element of $S$.

**Claim:** $c =$ gcd$(a, b)$. It suffices to show that

(a) $c$ is a common divisor of $a, b$, that is, $c \mid a$ and $c \mid b$

(b) If $d \mid a$ and $d \mid b$ then $d \mid c$. (Clear from definition of $c$.)

# Consequences of Bezout's Theorem

**Corollary:** Suppose $a, b, c \in \mathbb{N}_+$. If $a \mid bc$ and gcd$(a, b) = 1$ then $a \mid c$

**Proposition:** If $p$ is prime and $p \mid a_1 \cdots a_n$ then $p$ divides some $a_i$.

**Fact:** If $p$ is prime and $0 < k < p$ then $p \mid \binom{p}{k}$

**FTA (Uniqueness):** Suppose that $n \geq 1$ and $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are primes such that

$$n \;=\; p_1 \cdots p_r \;=\; q_1 \cdots q_s.$$

Then $r = s$ and $q_1, \ldots, q_r$ is just a rearrangement of $p_1, \ldots, p_r$.

# Mathematical Induction

# Overview of Mathematical Induction

**Given:** Propositional function $P(n)$ with domain $\mathbb{N}_+ = \{1, 2, \ldots\}$

**Induction:** Proof strategy to establish that $P(n)$ is true for every $n$

Mathematical basis of induction is the *well ordering property*, an axiom of the natural numbers $\mathbb{N}_+$ that states

- Every non-empty set $S \subseteq \mathbb{N}_+$ has a smallest element

# Mathematical Induction

**Given:** Propositional function $P(n)$ with domain $\mathbb{N}_+$

**Basis step:** Show that $P(1)$ is true

**Inductive step:** Show that $P(k) \rightarrow P(k+1)$ is true for every $k \geq 1$

- assume that $P(k)$ is true "inductive hypothesis"
- establish that $P(k+1)$ is true

**Conclusion:** $P(n)$ is true for every $n \in \mathbb{N}_+$

We can view induction as a (new) rule of inference, namely,

$$[P(1) \wedge \forall k \, (P(k) \rightarrow P(k+1))] \rightarrow \forall n \, P(n)$$

# Validity of Induction

**Informal:** Ladder/Dominos

- $P(1)$ is true by Basis step
- $P(1) \to P(2)$ is true by Inductive step, so $P(2)$ is true
- $P(2) \to P(3)$ is true by Inductive step, so $P(3)$ is true
- $P(3) \to P(4)$ is true by Inductive step, so $P(4)$ is true
- and so on...

**Conclude:** $P(n)$ is true for every $n$

# Validity of Induction

**Formal:** Suppose that basis and inductive steps hold but $\forall n\, P(n)$ is F

- Then $S = \{n : P(n) \text{ is F}\}$ is non-empty
- By well-ordering, $S$ has smallest element $m$
- By Basis step, $P(1)$ is true so $m \geq 2$
- Definition of $S$ implies $P(m-1)$ is T and we know $m - 1 \geq 1$
- Inductive step then implies $P(m)$ is T, a contradiction
- Conclude that $\forall n\, P(n)$ is T