CS250: Discrete Math for Computer Science

L16: $\sqrt{2} \notin \mathbf{Q}$ & $|\text{Primes}| = \aleph_0$

Common Divisors

For postive integers, a, b, CD$(a, b) \stackrel{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a,b) \stackrel{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\mathrm{CD}(6, 45) = \{1, 3\}$$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a, b) \stackrel{\text{def}}{=} \left\{ d \geq 1 \;\middle|\; d|a \,\wedge\, d|b \right\}$

$$\begin{aligned} \mathrm{CD}(6, 45) &= \{1, 3\} \\ \mathrm{CD}(12, 100) &= \{1, 2, 4\} \end{aligned}$$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a,b) \stackrel{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\begin{aligned}
\mathrm{CD}(6,45) &= \{1,3\} \\
\mathrm{CD}(12,100) &= \{1,2,4\} \\
\mathrm{CD}(12,49) &= \{1\}
\end{aligned}$$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a,b) \overset{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\begin{aligned}
\mathrm{CD}(6,45) &= \{1,3\} \\
\mathrm{CD}(12,100) &= \{1,2,4\} \\
\mathrm{CD}(12,49) &= \{1\}
\end{aligned}$$

Def. greatest common divisor, $\mathrm{gcd}(a,b) \overset{\text{def}}{=} \max(\mathrm{CD}(a,b))$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a,b) \overset{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\begin{array}{rcl} \mathrm{CD}(6,45) & = & \{1,3\} \\ \mathrm{CD}(12,100) & = & \{1,2,4\} \\ \mathrm{CD}(12,49) & = & \{1\} \end{array} \qquad \begin{array}{rcl} \gcd(6,45) & = & 3 \\ \gcd(12,100) & = & 4 \\ \gcd(12,49) & = & 1 \end{array}$$

Def. greatest common divisor, $\gcd(a,b) \overset{\text{def}}{=} \max(\mathrm{CD}(a,b))$

Common Divisors

For postive integers, a, b, $\text{CD}(a, b) \overset{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\begin{array}{rclcrcl} \text{CD}(6,45) & = & \{1,3\} & & \text{gcd}(6,45) & = & 3 \\ \text{CD}(12,100) & = & \{1,2,4\} & & \text{gcd}(12,100) & = & 4 \\ \text{CD}(12,49) & = & \{1\} & & \text{gcd}(12,49) & = & 1 \end{array}$$

Def. greatest common divisor, $\text{gcd}(a, b) \overset{\text{def}}{=} \max(\text{CD}(a, b))$

Def. Integers a, b are **relatively prime** iff $\text{gcd}(a, b) = 1$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a, b) \overset{\mathrm{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\begin{array}{rclrcl}
\mathrm{CD}(6,45) & = & \{1,3\} & \gcd(6,45) & = & 3 \\
\mathrm{CD}(12,100) & = & \{1,2,4\} & \gcd(12,100) & = & 4 \\
\mathrm{CD}(12,49) & = & \{1\} & \gcd(12,49) & = & 1
\end{array}$$

Def. greatest common divisor, $\gcd(a, b) \overset{\mathrm{def}}{=} \max(\mathrm{CD}(a, b))$

Def. Integers a, b are **relatively prime** iff $\gcd(a, b) = 1$

Prop. If $a = p_1^{i_1} \cdots p_k^{i_k}$ and $b = p_1^{j_1} \cdots p_k^{j_k}$ are already factored into products of powers of distinct primes, then

$$\gcd(a, b) = p_1^{\min(i_1, j_1)} \cdots p_k^{\min(i_k, j_k)}$$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a,b) \overset{\text{def}}{=} \{d \geq 1 \mid d|a \ \wedge \ d|b\}$

$$\begin{array}{rclcrcl} \mathrm{CD}(6,45) & = & \{1,3\} & & \gcd(6,45) & = & 3 \\ \mathrm{CD}(12,100) & = & \{1,2,4\} & & \gcd(12,100) & = & 4 \\ \mathrm{CD}(12,49) & = & \{1\} & & \gcd(12,49) & = & 1 \end{array}$$

Def. greatest common divisor, $\gcd(a,b) \overset{\text{def}}{=} \max(\mathrm{CD}(a,b))$

Def. Integers a, b are **relatively prime** iff $\gcd(a,b) = 1$

Prop. If $a = p_1^{i_1} \cdots p_k^{i_k}$ and $b = p_1^{j_1} \cdots p_k^{j_k}$ are already factored into products of powers of distinct primes, then

$$\gcd(a,b) = p_1^{\min(i_1,j_1)} \cdots p_k^{\min(i_k,j_k)}$$

$$\gcd(2^1 \cdot 3^1 \cdot 5^0, 2^0 \cdot 3^2 \cdot 5^1) \;=\; 2^0 \cdot 3^1 \cdot 5^0 \;=\; 3$$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a, b) \overset{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\begin{array}{rclcrcl}
\mathrm{CD}(6,45) & = & \{1,3\} & & \gcd(6,45) & = & 3 \\
\mathrm{CD}(12,100) & = & \{1,2,4\} & & \gcd(12,100) & = & 4 \\
\mathrm{CD}(12,49) & = & \{1\} & & \gcd(12,49) & = & 1
\end{array}$$

Def. greatest common divisor, $\gcd(a, b) \overset{\text{def}}{=} \max(\mathrm{CD}(a, b))$

Def. Integers a, b are **relatively prime** iff $\gcd(a, b) = 1$

Prop. If $a = p_1^{i_1} \cdots p_k^{i_k}$ and $b = p_1^{j_1} \cdots p_k^{j_k}$ are already factored into products of powers of distinct primes, then

$$\gcd(a, b) = p_1^{\min(i_1, j_1)} \cdots p_k^{\min(i_k, j_k)}$$

$$\begin{array}{rclcl}
\gcd(2^1 \cdot 3^1 \cdot 5^0, 2^0 \cdot 3^2 \cdot 5^1) & = & 2^0 \cdot 3^1 \cdot 5^0 & = & 3 \\
\gcd(2^2 \cdot 3^1 \cdot 5^0, 2^2 \cdot 3^0 \cdot 5^2) & = & 2^2 \cdot 3^0 \cdot 5^0 & = & 4
\end{array}$$

Common Divisors

For postive integers, a, b, $\mathrm{CD}(a, b) \stackrel{\text{def}}{=} \{d \geq 1 \mid d|a \wedge d|b\}$

$$\begin{array}{rclrcl} \mathrm{CD}(6,45) & = & \{1,3\} & \gcd(6,45) & = & 3 \\ \mathrm{CD}(12,100) & = & \{1,2,4\} & \gcd(12,100) & = & 4 \\ \mathrm{CD}(12,49) & = & \{1\} & \gcd(12,49) & = & 1 \end{array}$$

Def. greatest common divisor, $\gcd(a, b) \stackrel{\text{def}}{=} \max(\mathrm{CD}(a, b))$

Def. Integers a, b are **relatively prime** iff $\gcd(a, b) = 1$

Prop. If $a = p_1^{i_1} \cdots p_k^{i_k}$ and $b = p_1^{j_1} \cdots p_k^{j_k}$ are already factored into products of powers of distinct primes, then

$$\gcd(a, b) = p_1^{\min(i_1, j_1)} \cdots p_k^{\min(i_k, j_k)}$$

$$\begin{array}{rclcl} \gcd(2^1 \cdot 3^1 \cdot 5^0, 2^0 \cdot 3^2 \cdot 5^1) & = & 2^0 \cdot 3^1 \cdot 5^0 & = & 3 \\ \gcd(2^2 \cdot 3^1 \cdot 5^0, 2^2 \cdot 3^0 \cdot 5^2) & = & 2^2 \cdot 3^0 \cdot 5^0 & = & 4 \\ \gcd(2^2 \cdot 3^1 \cdot 7^0, 2^0 \cdot 3^0 \cdot 7^2) & = & 2^0 \cdot 3^0 \cdot 7^0 & = & 1 \end{array}$$

Rationals in Lowest Terms

Def. We say the rational, $\frac{a}{b}$, is in **lowest terms** iff $\gcd(a, b) = 1$.

Rationals in Lowest Terms

Def. We say the rational, $\frac{a}{b}$, is in **lowest terms** iff $\gcd(a, b) = 1$.

$\frac{6}{8}$ is not in lowest terms, but $\frac{3}{4}$ is.

Rationals in Lowest Terms

Def. We say the rational, $\frac{a}{b}$, is in **lowest terms** iff $\gcd(a, b) = 1$.

$\frac{6}{8}$ is not in lowest terms, but $\frac{3}{4}$ is.

Prop. Every rational number, $\frac{a}{b}$, with $b \neq 0$ may be written in lowest terms.

Rationals in Lowest Terms

Def. We say the rational, $\frac{a}{b}$, is in **lowest terms** iff $\gcd(a,b) = 1$.

$\frac{6}{8}$ is not in lowest terms, but $\frac{3}{4}$ is.

Prop. Every rational number, $\frac{a}{b}$, with $b \neq 0$ may be written in lowest terms.

Proof.

$$\frac{a}{b} = \frac{(a/\gcd(a,b))}{(b/\gcd(a,b))} \quad \text{and the latter is in lowest terms.} \qquad \square$$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \dfrac{a}{b}$.

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \frac{a}{b}$.

By previous Prop. we may assume that $\frac{a}{b}$ is in lowest terms

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \dfrac{a}{b}$.

By previous Prop. we may assume that $\dfrac{a}{b}$ is in lowest terms

$$\sqrt{2} \cdot b = a$$

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \dfrac{a}{b}$.

By previous Prop. we may assume that $\dfrac{a}{b}$ is in lowest terms

$$\sqrt{2} \cdot b = a$$

$$2 \cdot b^2 = a^2$$

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \dfrac{a}{b}$.

By previous Prop. we may assume that $\dfrac{a}{b}$ is in lowest terms

$$\sqrt{2} \cdot b = a$$

$$2 \cdot b^2 = a^2$$

Thus, a^2 is even. Thus a is even. Let $a = 2d$

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \dfrac{a}{b}$.

By previous Prop. we may assume that $\dfrac{a}{b}$ is in lowest terms

$$\sqrt{2} \cdot b = a$$

$$2 \cdot b^2 = a^2$$

Thus, a^2 is even. Thus a is even. Let $a = 2d$

Thus, $2b^2 = a^2 = 4d^2$. Thus $b^2 = 2d^2$. Thus b is even.

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \dfrac{a}{b}$.

By previous Prop. we may assume that $\dfrac{a}{b}$ is in lowest terms

$$\sqrt{2} \cdot b = a$$

$$2 \cdot b^2 = a^2$$

Thus, a^2 is even. Thus a is even. Let $a = 2d$

Thus, $2b^2 = a^2 = 4d^2$. Thus $b^2 = 2d^2$. Thus b is even.

Thus, $\dfrac{a}{b}$ is not in lowest terms.

$\square$

$\sqrt{2}$ is irrational

Prop. $\sqrt{2}$ is irrational.

Proof.

Suppose for the sake of a contradiction that $\sqrt{2} = \dfrac{a}{b}$.

By previous Prop. we may assume that $\dfrac{a}{b}$ is in lowest terms

$$\sqrt{2} \cdot b = a$$

$$2 \cdot b^2 = a^2$$

Thus, a^2 is even. Thus a is even. Let $a = 2d$

Thus, $2b^2 = a^2 = 4d^2$. Thus $b^2 = 2d^2$. Thus b is even.

Thus, $\dfrac{a}{b}$ is not in lowest terms.

This is a contradiction! Thus our assumption is false. $\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

Let $n = 1 + p_1 \cdot p_2 \cdots p_k$

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

Let $n = 1 + p_1 \cdot p_2 \cdots p_k$

Let d be the smallest divisor of n that is greater than 1.

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

Let $n = 1 + p_1 \cdot p_2 \cdots p_k$

Let d be the smallest divisor of n that is greater than 1.

Thus, $d|n$ and d is prime.

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

Let $n = 1 + p_1 \cdot p_2 \cdots p_k$

Let d be the smallest divisor of n that is greater than 1.

Thus, $d|n$ and d is prime.

Thus, $d = p_i$ for some $1 \leq i \leq k$.

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

Let $n = 1 + p_1 \cdot p_2 \cdots p_k$

Let d be the smallest divisor of n that is greater than 1.

Thus, $d | n$ and d is prime.

Thus, $d = p_i$ for some $1 \leq i \leq k$.

$p_i | (1 + p_1 \cdot p_2 \cdots p_k)$ and $p_i | (-p_1 \cdot p_2 \cdots p_k)$.

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

Let $n = 1 + p_1 \cdot p_2 \cdots p_k$

Let d be the smallest divisor of n that is greater than 1.

Thus, $d|n$ and d is prime.

Thus, $d = p_i$ for some $1 \leq i \leq k$.

$p_i|(1 + p_1 \cdot p_2 \cdots p_k)$ and $p_i|(-p_1 \cdot p_2 \cdots p_k)$.

By Prop. 13.1, $p_i|1$. Thus, $p_i \leq 1$. Thus, p_i is not prime.

$\square$

$|\text{Primes}| = \aleph_0$

Prop. There are infinitely many primes.

Proof.

Suppose for the sake of a contradiction that there are only finitely many primes: $p_1, p_2, \ldots, p_k$.

Let $n = 1 + p_1 \cdot p_2 \cdots p_k$

Let d be the smallest divisor of n that is greater than 1.

Thus, $d|n$ and d is prime.

Thus, $d = p_i$ for some $1 \leq i \leq k$.

$p_i|(1 + p_1 \cdot p_2 \cdots p_k)$ and $p_i|(-p_1 \cdot p_2 \cdots p_k)$.

By Prop. 13.1, $p_i|1$. Thus, $p_i \leq 1$. Thus, p_i is not prime.

This is a contradiction! **Thus our assumption is false.** $\square$