Logistics
- Because of Juneteenth, there are only 25 vitamins. The 8 vitamin drops remain, so you only need to complete 17 vitamins for full credit.
- The EECS Department has adjusted the Summer 2021 P/NP decision for CS 70. See @16211 on Piazza.
- There is one homework drop.
- If you are confused about graph induction, please see:
  - @127_P16
  - @127_P17
Primes and Greatest Common Divisors

Rec For $a, b \in \mathbb{Z}$ with $a \neq 0$, we say

Def Let $a, b \in \mathbb{Z}$. The greatest common divisor of $a$ and $b$.

Ex $\gcd(4, 18) = \gcd(n, 0) =$

Thm (Fundamental Theorem of Arithmetic) Every integer $\geq 2$ can be
Cor If $a = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ and $b = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$ are prime factorizations, then

Thm (Division Algorithm) Let $a, d \in \mathbb{Z}$ and $b > 0$. Then there are unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that

Pf Via well-ordering. Let $S = \{s \in \mathbb{N} : s = a - bk, k \in \mathbb{Z}\}$ and apply well-ordering.

Lem Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. Then

(c) \hspace{1cm} (c)

Pf In discussion

Note
GCD Algorithms

Ex. Let's use the lemma (and the Division Algorithm) to find gcds.
1. \( \text{gcd}(8, 12) = \)
2. \( \text{gcd}(287, 91) = \)

Alg. (Euclidean) Recursively apply the gcd.
\[
\text{gcd}(a, b):
\]
  if \( b = 0 \), return
  else, return

Thm. (Bezout's Theorem) If \( a, b \in \mathbb{Z} \), there exist coefficients \( x, y \in \mathbb{Z} \) such that

Alg. (Extended Euclidean): Run the Euclidean algorithm in reverse.
Ex. \( \text{gcd}(287, 91) = 7 \)

\[
287 = 8 \times 91 + 14
\]
\[
91 = 6 \times 14 + 7
\]
\[
14 = 2 \times 7 + 0
\]
Modular Equivalences

Def Let \( a, b \in \mathbb{Z} \) and \( m \in \mathbb{Z}^+ \).

Ex \( 53 - 9 = 44 = 4 \times 11 \).
\[-11 - 1 = -12 = (-4) \times 3.\]

Then Let \( a, b \in \mathbb{Z} \) and \( m \in \mathbb{Z}^+ \). Then
\( a \equiv b \pmod{m} \) if
\[ a \equiv b \pmod{m} \]

Ex \( 53 = \quad -11 = \quad \)
\[ q = \quad 1 = \quad \]
pf for some \( q_a, r_a \in \mathbb{Z} \) \( 0 \leq r_a < m \)
for some \( q_b, r_b \in \mathbb{Z} \) \( 0 \leq r_b < m \)

\( \Leftarrow \) Suppose \( a \equiv b \pmod{m} \).

\( \Rightarrow \) Suppose \( a \equiv b \pmod{m} \).
Modular Addition and Multiplication

Cor Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then

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

$ab \equiv bd \pmod{m}$

Then Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$ab \equiv bd \pmod{m}$

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Showing $ac \equiv bd$ is left as an exercise. □

Clem For $n \in \mathbb{Z}$, $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

Pf

Clem Suppose $m = 4k + 3$ for some $k \in \mathbb{Z}$. Then $m$ is not the sum of two squares of integers.

Pf Suppose for contradiction that $m = a^2 + b^2$ for $a, b \in \mathbb{Z}$.

Note Multiplying and adding numbers preserve congruences.
Subtracting $a \in \mathbb{Z}$ is the same as adding $-a \in \mathbb{Z}$, so subtracting preserves congruences.
Inverses (Modular Division)

**Def:** Let \( a \in \mathbb{Z} \) and \( m \in \mathbb{Z}^+ \). If \( x \in \mathbb{Z} \) is such that

we say \( x \) is an inverse of \( a \mod m \), denoted

\[ \text{Def} \quad a \equiv x \pmod{m} \]

Then let \( a \in \mathbb{Z} \) and \( m \in \mathbb{Z}^+ \). Then \( \gcd(a, m) = 1 \iff \) In the notes

\[ \implies \text{Suppose for contradiction that } a \text{ has a unique multiplicative inverse } x \text{ and } \gcd(a, m) > 1. \]

**Rec:** For \( a, b \in \mathbb{Z} \), the extended Euclidean algorithm provides \( x, y \in \mathbb{Z} \) such that

For \( a \in \mathbb{Z}, m \in \mathbb{Z}^+, \) suppose \( \gcd(a, m) = 1 \). Then the multiplicative inverse exists and satisfies

**Ex:** Suppose \( 3x \equiv 4 \pmod{11} \). Solve for \( x \), if a solution exists.