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 @15211 on Piazza
- There is one homework drop.
- If you are confused about graph induction, please see

  @127_f16

  @127_f17

Primes and Greatest Common Divisors

Rec For $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a divides b, written $a \mid b$ if
$(\exists k \in \mathbb{Z})(b = ak)$

Def Let $a, b \in \mathbb{Z}$. The greatest common divisor of a and b, denoted $\gcd(a,b)$, is the greatest $d \in \mathbb{Z}$ such that $d \mid a$ and $d \mid b$. We define $\gcd(0,0) = 0$.

Ex $\gcd(4, 18) = 2$

We check:

$1 \mid 4$, $1 \mid 18$

$2 \mid 4$, $2 \mid 18$

$3 \nmid 4$, $3 \mid 18$

$4 \mid 4$, $4 \nmid 18$

$\gcd(n, 0) = n$

We check:

$n \mid n$, $n \mid 0$

Thm (Fundamental Theorem of Arithmetic) Every integer ≥ 2 can be uniquely expressed as a product of primes.

Cor If $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$ are prime factorizations, then

$$\gcd(a,b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$$

However, no efficient algorithm is known for factorization.

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

$$a = qb + r$$

We say r is the remainder and write $r = a \bmod b$.

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

(i) $\gcd(a,b) = \gcd(a-b, b)$

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

Pf In discussion

Note The lemma and the Division Algorithm provide an algorithm for finding the gcd.

GCD Algorithms

Ex Let's use the lemma (and the Division Algorithm) to find gcds.

① $\gcd(8,12) = \gcd(8,4)$
$= \gcd(4,4)$
$= \gcd(0,4)$
$= 4$

② $\gcd(287,91) = \gcd(14,91)$
$= \gcd(7,14)$
$= \gcd(0,7)$
$= 7$

$287 = 3 \times 91 + 14$
$91 = 6 \times 14 + 7$
$14 = 2 \times 7 + 0$

Alg (Euclidean) Recursively apply the gcd.

gcd(a,b):
  if $b=0$, return a
  else, return $\gcd(b, \underbrace{a \bmod b}_{r})$

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

$$ax + by = \gcd(a,b)$$

Alg (Extended Euclidean): Run the Euclidean algorithm in reverse.

Ex $\gcd(287,91) = 7$
$= 91 - 6 \times 14$
$= 91 - 6 \times (287 - 3 \times 91)$
$= 19 \times 91 + 6 \times 287$

$287 = 3 \times 91 + 14$
$91 = 6 \times 14 + 7$
$14 = 2 \times 7 + 0$

Modular Equivalences

Def Let $a,b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $m \mid (a-b)$, we say that a is congruent to b modulo m, denoted $a \equiv b \pmod{m}$

Ex $53 - 9 = 44 = 4 \times 11$. So $53 \equiv 9 \pmod 4$
$53 \equiv 9 \pmod{11}$

$-11 - 1 = -12 = (-4) \times 3$. So $-11 \equiv 1 \pmod 3$
$-11 \equiv 1 \pmod 4$

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

$a \equiv b \pmod m$ iff $a \bmod m = b \bmod m$

The theorem tells us that two numbers are congruent if they have the same remainders when divided by m.

Ex $53 = 4 \times 11 + 9$ $\quad$ $-11 = (-4) \times 3 + 1$
$9 = 0 \times 11 + 9$ $\quad$ $1 = (0) \times 3 + 1$

Pf By the division algorithm,
$a = q_a m + r_a$ for some $q_a, r_a \in \mathbb{Z}$ $\quad 0 \le r_a < m$
$b = q_b m + r_b$ for some $q_b, r_b \in \mathbb{Z}$ $\quad 0 \le r_b < m$
$\left(\begin{array}{l} r_a = a \bmod m \\ r_b = b \bmod m \end{array} \right)$

So $a - b = m(q_a - q_b) + (r_a - r_b)$

$\Leftarrow$) Suppose $a \bmod m = b \bmod m$
Then $a - b = m(q_a - q_b) + 0$.
So $m \mid (a-b)$.
Therefore $a \equiv b \pmod m$

$\Rightarrow$) Suppose $a \equiv b \pmod m$.
Then $m \mid (a-b)$
$m \mid m(q_a - q_b) + (r_a - r_b)$
So $mk = m(q_a - q_b) + (r_a - r_b)$ for $k \in \mathbb{Z}$. So $(r_a - r_b) = m(k - q_a + q_b)$.
$m \mid (r_a - r_b)$
Since $0 \le r_a, r_b < m$, $-m < r_a - r_b < m$. So
$m = l(r_a - r_b) \Rightarrow r_a - r_b = 0$
Therefore $r_a = r_b$ $\square$

Modular Addition and Multiplication

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

$a \equiv b \pmod m$ iff $a = km + b$ for some $k \in \mathbb{Z}$.

Pf If $a \equiv b \pmod m$, then $a = jm + r$ and $b = \ell m + r$ by the previous theorem. Then $r = b - \ell m$, so $a = m(j-\ell) + b$.
If $a = km + b$ for some $k \in \mathbb{Z}$, then $km = a - b$, so $m \mid (a-b)$. So $a \equiv b \pmod m$.

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

$a + c \equiv b + d \pmod m$ $\quad$ $ac \equiv bd \pmod m$

Pf Suppose $a \equiv b \pmod m$ and $c \equiv d \pmod m$.
Then $a = km + b$, $c = jm + d$.
$a + c = m(k+j) + b + d$
By the lemma, $a + c \equiv b + d \pmod m$
Showing $ac \equiv bd$ is left as an exercise. □

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

Pf Since $0 \le r < 4$, there are only 4 options.
1. $n \equiv 0 \pmod 4$. Then $n^2 \equiv 0^2 \equiv 0 \pmod 4$
2. $n \equiv 1 \pmod 4$. Then $n^2 \equiv 1^2 \equiv 1 \pmod 4$
3. $n \equiv 2 \pmod 4$. Then $n^2 \equiv 2^2 \equiv 0 \pmod 4$
4. $n \equiv 3 \pmod 4$. Then $n^2 \equiv 3^2 \equiv 1 \pmod 4$

Clm 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 $a,b \in \mathbb{Z}$.
From the above claim, $a^2 \equiv 0 \pmod 4$ or $a^2 \equiv 1 \pmod 4$
$m \equiv 0 + 0 \pmod 4$ or $m \equiv 0 + 1 \pmod 4$ or $m \equiv 1 + 1 \pmod 4$
By assumption, $m = 4k + 3$, so $m \equiv 3 \pmod 4$. This is a contradiction. □

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

$ax \equiv 1 \pmod{m}$,

we say x is an inverse of a mod m, denoted a^{-1} mod m.

Thm Let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $\gcd(a, m) = 1$ iff a has a unique multiplicative inverse.

Pf $\Rightarrow$) In the notes

$\Leftarrow$) Suppose for contradiction that a has a unique multiplicative inverse x and $\gcd(a, m) > 1$.

Then $xa \equiv 1 \pmod{m}$, so

$xa = km + 1$ for some $k \in \mathbb{Z}$

$1 = km - xa$

Let $d = \gcd(a, m) > 1$. By definition, $d \mid m$ and $d \mid a$.

So $d \mid km$ and $d \mid xa$.

Therefore $d \mid (km - xa)$, so $d \mid 1$. This is a contradiction. $\square$

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

$ax + by = \gcd(a, b)$

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

$ax \equiv 1 \pmod{m} \iff ax = km + 1$ for some $k \in \mathbb{Z}$

$ax - km = 1 = \gcd(a, m)$

So the extended Euclidean algorithm on a and m will recover x!

Ex Suppose $3x \equiv 4 \pmod{11}$. Solve for x, if a solution exists.

To cancel out the 3, multiply both sides by 3^{-1}

$3^{-1} \cdot 3x \equiv 3^{-1} \cdot 4 \pmod{11}$

$1x \equiv 3^{-1} \cdot 4 \pmod{11}$

We use the egcd algorithm.

$$\begin{aligned} \gcd(11, 3) &= \gcd(3, 2) \\ &= \gcd(2, 1) \\ &= \gcd(1, 0) \\ &= 1 \checkmark \end{aligned} \qquad \begin{aligned} 11 &= 3 \times \underline{3} + \underline{2} \\ 3 &= 1 \times \underline{2} + \underline{1} \\ 2 &= 2 \times \underset{b}{\underline{1}} + \underset{r}{\underline{0}} \end{aligned} \qquad \Rightarrow \qquad \begin{aligned} 1 &= 3 - 2 \\ &= 3 - (11 - 3 \times 3) \\ &= 4 \times 3 - 1 \times 11 \end{aligned}$$

So 3^{-1} mod $11 = 4$, and $x \equiv 4 \cdot 4 \equiv 16 \equiv 5 \pmod{11}$.