Homework 6

Due: March 12, 2025

All homeworks are due at 11:59 PM on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit.

Problems marked with a * are problems which may appear on the midterm or final with some modification.

Problem 1

For each of the statements below, determine if it is *always* true, *sometimes* true, or *never* true. Justify your answers. To justify an "always" or "never" answer, write a proof; to justify a "sometimes" answer, give one witness that makes the statement true and one that makes the statement false, explaining these judgments.*

For example, the statement

> Let $a, b : \mathbb{N}$ and suppose $a \mid b$. Then the greatest prime factor of b divides a.

is *sometimes* true. It is true if $a = 6$ and $b = 12$, since $6 \mid 12$ and the greatest prime factor of 12 is 3, which divides 6. It is false if $a = 2$ and $b = 6$, since $2 \mid 6$ but the greatest prime factor of 6 is 3, which does not divide 2.

a. Let $p, q, r, s : \mathbb{N}$ be prime numbers and suppose that $pq = rs$. Then $p = r$ and $q = s$.

b. Let $p : \mathbb{N}$ be prime. Then p is relatively prime to every positive natural number except for p itself.

c. Let $a, b, c, n : \mathbb{N}$ and suppose that $3ab \equiv 3ac \mod n$. Then $b \equiv c \mod n$.

d. Let $a, b, m, n : \mathbb{N}$ be larger than 1 where $n \mid m$ and $a \equiv b \mod m$. Then $a \equiv b \mod n$.

e. Let $a, b : \mathbb{N}$. Then $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$.

f. Let $a, b, c, d, n : \mathbb{N}$ be integers with c and d positive and $n \geq 2$. If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $a^c \equiv b^d \mod n$.

Solution:

a. Sometimes. True if $p = r = 2$ and $q = s = 3$; false if $p = s = 2$ and $q = r = 3$.

b. Never. p is not relatively prime to $2p$ because $\gcd(p, 2p) = p > 1$ since primes are nonunits by definition.

c. Sometimes. True if $a = b = c = n = 1$ since $3 \equiv 3 \pmod 1$ and $1 \equiv 1 \pmod 1$; false if $b = 1$ and $a = c = n = 3$ since $27 \equiv 9 \pmod 3$ (they're both congruent to 0) but $3 \not\equiv 1 \pmod 3$.

d. Always.

We have that there is integer k_1 such that $a - b = k_1 \cdot m$. Furthermore, since $n \mid m$, we have that there is an integer k_2 such that $m = k_2 n$. Thus, we have $a - b = k_1 \cdot (k_2 n) = (k_1 \cdot k_2)n$ which shows that $a \equiv b \mod n$.

e. Sometimes. True if $a = b = 1$ since $\gcd(1 + 1, 1 + 1) = 2 = 1 + \gcd(1, 1)$; false if $a = 2$ and $b = 1$ since $\gcd(3, 2) = 1$ while $1 + \gcd(2, 1) = 1 + 1 = 2$.

f. Sometimes. If $a = 1$ and $b = 1$ then this is always true. However, if $n = 3$, $a = 2$, $b = 2$ and $c = 3$, $d = 6$ we have $a^c = 8 \equiv 2 \mod 3$ but $b^d = 64 \equiv 1 \mod 3$.

Problem 2

For each of the following, find the multiplicative inverse for the given element by using the extended Euclidean algorithm. If no inverse exists, explain why. *

a. 4 (mod 17)

b. 25 (mod 21)

c. 4 (mod 6)

For each of the following, find the positive integer values for x that satisfy the congruence. If x has finitely many solutions, list all of them. If x has infinitely many solutions, state that there are infinitely many solutions and list three of them. *

d. $x \equiv 3 \pmod 4$

e. $2x \equiv 7 \pmod 2$

f. $2 \equiv 6 \pmod x$

Solution:

a. **Extended Euclidean Algorithm:** $4(mod\ 17)$

a	b	q	s	t	g
4	17	4	-4	1	1
1	4	4	1	0	1
0	1		0	1	1

This is the extended Euclidean algorithm table for $4(mod\ 17)$. After finding that the greatest common divisor between 4 and 17 was 1, which means that they are relatively prime, I went back up on the right side of the table to get $s = -4$ and $t = 1$. We can now use the extended Euclidean algorithm to find the multiplicative inverse for 4 $(mod\ 17)$:

$$as + bt = g \rightarrow as = g - bt \rightarrow as - g = -bt$$

$$as - g = -bt \rightarrow b|(as - g) \rightarrow as \equiv g(mod\ b)$$

If we plug in $a = 4$, $s = -4$, $b = 17$, and $g = 1$, we get the following:

$$4 * (-4) \equiv 1(mod\ 17)$$

This means that -4 (mod 17) is the multiplicative inverse of 4 (mod 17), so if we solve for $rem(17, -4) \rightarrow 17 = (-1)(-4) + 13$, we get that the multiplicative inverse of 4 (mod 17) is 13.

b. **Extended Euclidean Algorithm:** 25 (mod 21) To calculate the multiplicative inverse, we know that 25 (mod 21) is equal to 4 (mod 21) if we do $25 - 21 = 4$. Therefore, since we subtracted by a multiple of 21, 4 (mod 21) and 25 (mod 21) will have the same multiplicative inverse:

a	b	q	s	t	g
4	21	5	-5	1	1
1	4	4	1	0	1
0	1		0	1	1

This is the extended Euclidean algorithm table for 4(mod 21). After finding that the greatest common divisor between 4 and 21 was 1, which means that they are relatively prime, I went back up on the right side of the table to get $s = -5$ and $t = 1$. We can now use the extended Euclidean algorithm to find the multiplicative inverse for 4 (mod 21):

$$as + bt = g \rightarrow as = g - bt \rightarrow as - g = -bt$$

$$as - g = -bt \rightarrow b|(as - g) \rightarrow as \equiv g(mod\ b)$$

If we plug in $a = 4$, $s = -5$, $b = 21$, and $g = 1$, we get the following:

$$4 * (-5) \equiv 1(mod\ 21)$$

That means that -5 (mod 21) is the multiplicative inverse of 4 (mod 21) which equals 16.

c. 4 does not have an inverse mod 6. For any x, $4x$ will be even, and thus rem($4x$, 6) will be even. So this remainder cannot be 1.

d. Infinite. -1, 3, 7.

e. No solution.

f. 1, 2, 4.

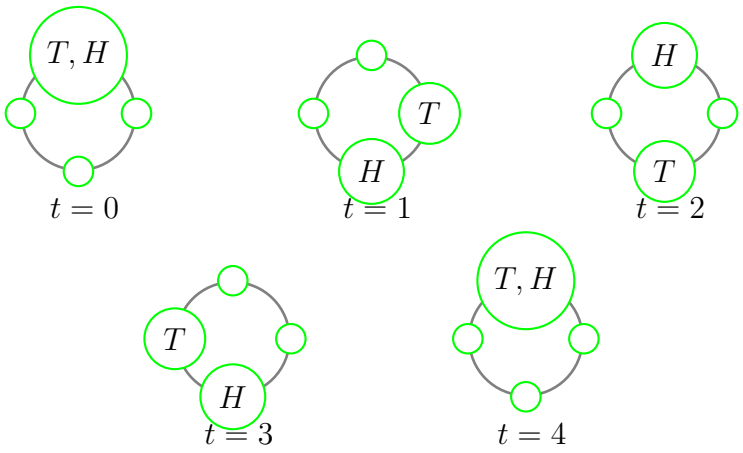
Problem 3

a. In a true mélange of classic animal-based math problems, a tortoise and hare are playing a game that involves hopping around a circular track of lily pads. At the start, they stand on the same lily pad. Then, every second, the slow tortoise jumps one lily pad clockwise, while the swift hare jumps two lily pads clockwise. They keep hopping until they once again end up on the same lily pad as each other (regardless of whether it is the lily pad on which they started).

If there are n lily pads, where n is a positive natural number, determine, with proof, the number of seconds it will take for the tortoise and hare to finish their game.

> **HINT:** Label the lily pads 0 through $n-1$. Can you write down a function $t(k)$ that outputs the number of the lily pad occupied by the tortoise after k seconds? What about $h(k)$ for the hare? When are these functions equal?

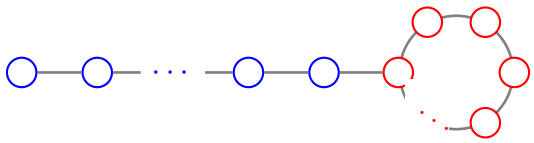
As an example, here's how the game would go on a track of four lily pads (where t is the number of seconds elapsed, and T represents the tortoise and H the hare):



b. After completing their game, the tortoise and hare decide to play again on a different track of lily pads. To get to that track, they'll need to hop down a short road, which is conveniently made of an even number of lily pads.

The tortoise and hare both start at the first lily pad on the road. They both hop down the road, then begin hopping clockwise around the new track once they reach it. Once either animal is on the track, it continues hopping circularly around the track and never returns to the road. As before, the tortoise and hare

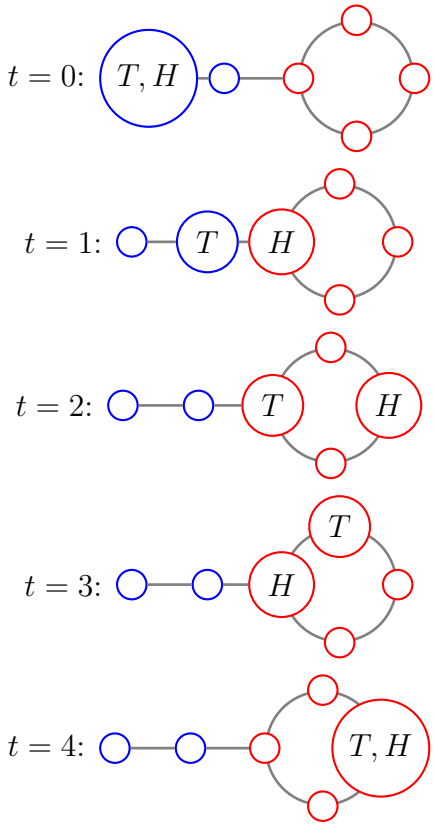
keep hopping until they end up one the same lily pad. The setup is depicted below with the road in blue and the track in red:



As before, the tortoise hops one lily pad each second, while the hare hops two lily pads per second.

Let $r \in \mathbb{N}^+$ be the number of lily pads on the road, and let $c \in \mathbb{N}^+$ be the number of lily pads on the circular track. Show that, if $c \geq r$, the tortoise and hare will meet when exactly c seconds have elapsed and not before.

As an example, letting T denote the tortoise and H the hare, here's how this would play out with $r = 2$ and $c = 4$:



Solution:

a. Label the lily pads with the numbers 0 through $n-1$ starting at the lily pad on which the tortoise and hare stand at time $t = 0$. Since the tortoise moves clockwise one lily pad each second, it will be on lily pad $t \bmod n$ after t seconds, while the hare, moving clockwise by two lily pads per second, will be on lily pad $2t \bmod n$ after t seconds.

When the tortoise and hare are on the same lily pad, then, we will have $t \equiv 2t \pmod{n}$. The goal is to find the least nonzero value of $t \in \mathbb{N}$ that satisfies this congruence.

By subtracting t from both sides, we are equivalently looking to satisfy $0 \equiv t \pmod{n}$, which by the definition of congruence says that $n \mid t$, i.e., $t = cn$ for some $c \in \mathbb{N}$. Thus, since the least nonzero value t of this form is obtained when $c = 1$, we find that the reunion of the tortoise and hare occurs at time $t = n$.

b. First, observe that the tortoise and hare will not meet on the road. At any time $t \in \mathbb{N}^+$ at which both animals are on the road, the tortoise is at the tth lilypad and the hare is at the $(2t)$th one, and we know $2t \neq t$ for any positive natural t. So it must be that they meet on the circular track.

Label the lilypads on the track with the numbers $0, 1, \ldots c-1$ proceeding clockwise and beginning with the first lilypad after the road. The tortoise reaches the circular track at time r, so since the two animals meet on the track, they must meet at a time greater than or equal to r. Moreover, at $t \in \mathbb{N}$ seconds after time r, the tortoise is at position $t \bmod c$.

We must now determine the hare's position at time $r + t$. Since r is even, the hare reaches lily pad 0 on the track at time $\frac{r}{2}$. Since the hare hops 2 lily pads each second, the hare's position at time $r + t$ is given (modulo c) by $2\left(r + t - \frac{r}{2}\right) = 2\left(t + \frac{r}{2}\right)$.

Thus, to find the first time when the tortoise and hare are at the same lily pad on the track, we must find the minimal $t \in \mathbb{N}$ such that

$$t \equiv 2\left(t + \frac{r}{2}\right) \pmod{c}.$$

Expanding and separating variables, we must equivalently solve

$$0 \equiv t + r \pmod{c}.$$

Since $c \geq r$, the smallest value of $t \geq 0$ for which this is true is $t = c - r$. So the tortoise and hare must meet at time $r + t = r + (c - r) = c$.

Problem 4 (Mind Bender — *Extra Credit*)

You are playing a game with a hare in which you and the hare alternate turns. The hare starts at 0 and each time it is the hare's turn, it jumps some non-zero distance $b : \mathbb{N}$ forward.

Each time it is your turn you can do one of two things: you can either (1) do nothing or (2) use your length $a : \mathbb{N}$ lasso to pull the hare distance a backwards. This is a very useful lasso which satisfies the property that $a > b$ and $\gcd(a, b) = 1$. You are also allowed to pull the hare to negative positions.

Show that for any $n : \mathbb{N}$, there is a series of actions (waits or pulls) you can always choose so that the hare is at n at some point.

For example, if $a = 9$, $b = 4$ and $n = 2$ and the game proceeds as follows, the hare is at 2 at some point: **Hare:** jumps to 4; **You:** pull the hare to -5; **Hare:** jumps to -1; **You:** pull the hare to -10; **Hare:** jumps to -6; **You:** do nothing; **Hare:** jumps to -2; **You:** do nothing; **Hare:** jumps to 2.

Solution:

Recall from class that there exist integers k_1 and k_2 such that

$$1 = k_1 \cdot a + k_2 \cdot b. \tag{1}$$

In particular, let $r_1 = a$ and $r_2 = b$ and consider the equations corresponding to running Euclid's gcd algorithm

$$\begin{aligned} r_1 &= q_1 r_2 + r_3 \\ r_2 &= q_2 r_3 + r_4 \\ r_3 &= q_3 r_4 + r_5 \\ &\dots \\ r_{k-2} &= q_{k-2} r_{k-1} + r_k \end{aligned}$$

where $r_k = \gcd(a, b) = 1$. Rearranging, we have

$$\begin{aligned} r_3 &= r_1 - q_1 r_2 \\ r_4 &= r_2 - q_2 r_3 \\ r_5 &= r_3 - q_3 r_4 \\ &\dots \\ r_k &= r_{k-2} - q_{k-2} r_{k-1}. \end{aligned}$$

In other words, we can express r_i for $i \geq 3$ as an integer linear combination of r_{i-1} and r_{i-2}. Repeatedly applying this, we have that we can express $r_k = \gcd(a, b) = 1$ as an integer linear combination of $r_1 = a$ and $r_2 = b$, showing Equation 1.

We next show that it is always possible to get the hare to either -1 or 1. Apply Equation 1 and observe that, critically, since $a > b$ we know $|k_1| < |k_2|$. We case on whether k_1 is negative.

- If k_1 is negative then k_2 must be positive. In this case, we let the hare jump for k_2 turns and for any $-k_1$ of these turns we pull and for the remaining turns we do nothing. Note that we only have enough turns to pull the hare since $|k_1| < |k_2|$. By Equation 1 the hare will end at 1 after this.
- If k_1 is positive then k_2 must be negative. In this case, we let the hare jump for $-k_2$ turns and we pull for any k_1 of these turns and do nothing for the remainder. Again, note that we only have enough turns to pull the hare since $|k_1| < |k_2|$. By Equation 1 times -1, we have that the hare will end at -1 after this.

Next, we show that it is always possible to get the hare to 1. In particular, either we have a strategy to get the hare to 1 or we have a strategy to get the hare to -1. In the former case we are done. In the latter case, if we repeat our strategy $b - 1$ times then the hare ends at $-b + 1$ and after one more jump ends at 1.

Lastly, to get our hare to n, we can simply repeat our strategy to get the hare to 1 n-many times.