Homework 7

Due: Friday, April 5, 2024

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.

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

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

f. Let $n : \mathbb{N}$ and suppose n is not divisible by 3. Then $n^2 \equiv 1 \mod 3$.

Solution:

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.

Observe that, by definition, $\gcd(a, \gcd(a, b)) \mid \gcd(a, b)$. Since $\gcd(a, b) \mid b$, it follows by the transitivity of divisibility that $\gcd(a, \gcd(a, b)) \mid b$. Moreover, definitionally, $\gcd(a, \gcd(a, b)) \mid a$. So $\gcd(a, \gcd(a, b))$ is a common divisor of a and b. But since $\gcd(a, b)$ is the *greatest* common divisor of a and b, we must have $\gcd(a, b) \geq \gcd(a, \gcd(a, b))$.

Furthermore, $\gcd(a, b) \mid a$ by definition and $\gcd(a, b) \mid \gcd(a, b)$ trivially. So $\gcd(a, b)$ is a common divisor of a and $\gcd(a, b)$. But since $\gcd(a, \gcd(a, b))$ is the *greatest* common divisor of those two values, we must have $\gcd(a, b) \leq \gcd(a, \gcd(a, b))$.

So these values are both less than or equal to and greater than or equal to each other. The only way for these both to occur is if the values are in fact equal. So $\gcd(a, b) = \gcd(a, \gcd(a, b))$ as desired.

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. Always. We know $n \not\equiv 0 \pmod 3$ by assumption. So either $n \equiv 1 \pmod 3$, in which case $n^2 \equiv 1 \pmod 3$ and the claim holds; or $n \equiv 2 \pmod 3$, in which case $n^2 \equiv 4 \equiv 1 \pmod 3$ and the claim again holds. Since $\{0, 1, 2\}$ is a complete set of representatives mod 3, these cases are exhaustive.

Problem 2

Normally explorers are not allowed to wander around Jurassic Park unsupervised. But 10 brave CS22 TAs have left the normal tourist paths. Incredibly, they have stumbled onto a nest that is full of dinosaur eggs!

a. Using their deep knowledge of dinosaurs from TA camp, they determine that each egg is either a tyrannosaurus or brontosaurus egg, and there are twice as many brontosaurus eggs as there are tyrannosaurus eggs.

   The TAs decide to divide the tyrannosaurus eggs between themselves such that TA number n gets t_n tyrannosaurus eggs. For fairness and number-theoretic reasons, they require that for each pair of TAs m and n, 10 does not divide $t_m - t_n$.

   Is it possible for them to distribute the brontosaurus eggs with the same restriction? Why or why not?

b. The TAs eventually deliver the eggs to Rob, who decides to play a game. He arranges the eggs into three rows: the first row has 51 eggs, the second has 49, and the third has 5. In each move of this game, he can combine any two rows into one row, or he can split a row with $2n$ eggs into two rows each with n eggs. (This second move, of course, only works on rows with an even number of eggs.)

   Rob's goal is to create 105 rows, each with one single egg. Can he achieve this goal, or will he end the day disappointed? Justify your answer!

HINT: Think about Rob's possible first moves; then remember that we've been talking a lot about greatest common divisors!

Solution:

a. We claim that if n eggs can be divided satisfying the "10 does not divide" condition, then $n \equiv 5 \pmod{10}$. The condition means that all of the t_i must be distinct mod 10. So $n = \sum_{i=1}^{10} t_i \equiv 0 + 1 + 2 + \cdots + 9 \equiv 5 \pmod{10}$.

   This means that the number of t-rex eggs is 5 mod 10. Since there are twice as many brontosaurus eggs, the number of brontosaurus eggs is $2 \cdot 5 \equiv 0$ mod 10. So the brontosaurus eggs cannot be divided satisfying the condition.

b. We will prove this by case analysis on the first move, which must be to combine two rows, since none of the rows are even. After this first move we are in one

of three situations with two rows: (100, 5), (51, 54), or (56, 49).

It would be a bad move to combine again—that would end the game. So in all cases, the next move should be to divide. In each case, the numbers of eggs in the two rows will have a common divisor that is odd and greater than 1. Splitting a row in two will preserve this divisor: if k is odd and $k \mid 2n$ then $k \mid n$. Similarly, combining two rows will preserve this: if $k \mid n_1$ and $k \mid n_2$ then $k \mid n_1 + n_2$ (the linear combination property). So in all three cases, there will always be an odd $k > 1$ that divides the number of eggs in each row. This means that no row could possibly have 1 egg, and Rob will be disappointed.

Problem 3

It's spring break! Time to introduce a fun new game to play with a friend, while you're bored and missing cs22.

On a piece of paper, write down two natural numbers $m, n > 0$.

The two of you will take turns following this rule: choose two (distinct) numbers that are written on the paper, and write down the difference of those two numbers. This should be positive (subtract the smaller one from the bigger one), and you can't repeat numbers that are already on the page.

You take the first turn, followed by your friend. Eventually someone will get stuck, unable to write down a new number. That person loses the game.

a. Prove that every number written down on the page is divisible by $\gcd(m, n)$.

b. Prove that all of the (positive) multiples of $\gcd(m, n)$ up to $\max(m, n)$ must be written down on the page by the time the game is over.

c. Your friend is very confident: they tell you that they can choose infinitely many pairs of starting numbers m and n that guarantee them a win. But you can do the same! Describe how you could choose pairs of numbers that guarantee you, the first player, will win the game.

Solution:

a. We can formulate this as an induction problem. Let $\langle a_i \rangle_{i \in \mathbb{N}}$ be the sequence of numbers written down on the page, with $a_0 = m$, $a_1 = n$, and a_i being the number written down on the $(i-1)$th turn. Let the predicate $P(k) := \gcd(m, n) \mid a_k$. We will show that $P(k)$ holds for all $k \in \mathbb{N}$ by strong induction.

Base Cases: We consider $k = 0$ and $k = 1$. We have $\gcd(m, n) \mid m = a_0$ and $\gcd(m, n) \mid n = a_1$ by the definition of GCD. So $P(0)$ and $P(1)$ hold.

Inductive Step: Fix some $k \in \mathbb{N}$ and suppose as our inductive hypothesis that for all $j < k$, we have $P(j)$. We want to show $P(k)$.

By the rules of the game, we know that $a_k = a_i - a_j$ where a_i and a_j are previously-written numbers, i.e., where $i, j < k$. By inductive hypothesis, $\gcd(m, n) \mid a_i$ and $\gcd(m, n) \mid a_j$. So we can write $a_i = q_i \gcd(m, n)$ and $a_j = q_j \gcd(m, n)$ for some $q_i, q_j \in \mathbb{Z}$. But then we can write

$$a_k = a_i - a_j = q_i \gcd(m, n) - q_j \gcd(m, n) = (q_i - q_j) \gcd(m, n)$$

so that (since $q_i - q_j \in \mathbb{Z}$) we have $\gcd(m, n) \mid a_k$, as desired.

Since we have shown $P(0)$, $P(1)$, and $\forall j \in \mathbb{N}, (\forall i \in \mathbb{N}, i < j \to P(i)) \to P(j)$, we have $P(k)$ for all $k \in \mathbb{N}$ by strong induction.

b. Without loss of generality, suppose $m > n$. Let s be the smallest number written on the page at the end of the game. It suffices for us to show that $s = gcd(m, n)$. If we can do this, we're done, since $m - s$, $m - 2s$, etc. will all be on the page. Since $s \mid m$, the lowest item in this list will be s itself, and thus this list is equivalently s, $2s$, $3s$, ..., m.

By the division theorem, we can write $m = qs + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < s$. So $r = m - qs$. Since $r < s$ and s is the smallest number on the page, r itself cannot be written on the page. But $m - s$, $m - 2s$, ... all can be; the only way that $m - qs$ could be ruled out is if it is 0. So $r = 0$. We thus have $m = qs$, so $s \mid m$.

A symmetric argument shows $s \mid n$. So $s \leq \gcd(m, n)$ by the definition of GCD. But we also know that s is a multiple of $\gcd(m, n)$ by part (a), so in fact we must have $s = \gcd(m, n)$. And we just showed that all multiples of $s = \gcd(m, n)$ up to $\max(m, n) = m$ are on the board.

c. By part (a), *only* positive multiples of $\gcd(m, n)$ are written down. (Positivity is required by the fact that we choose *distinct* numbers at each turn.) By part (b), *every* multiple of $\gcd(m, n)$ up to $\max(m, n)$ is written down. So we can conclude that the numbers written down in a game are all and only the positive multiples of $\gcd(m, n)$ less than or equal to $\max(m, n)$. If there are an even number of such multiples, the person who goes second wins; if there are an odd number, the person who goes first wins. So we simply need to generate values m and n such that there are an odd number of such multiples, i.e., such that $\frac{\max(m,n)}{\gcd(m,n)}$ is odd.

There are many possible strategies for doing this: one such strategy is to pick $m > n \geq 2$ such that m is prime; then $\gcd(m, n) = 1$ and $\max(m, n) = m$, so our quotient of interest is odd because m, being a prime greater than 2, must be.

Problem 4 (Mind Bender — *Extra Credit*)

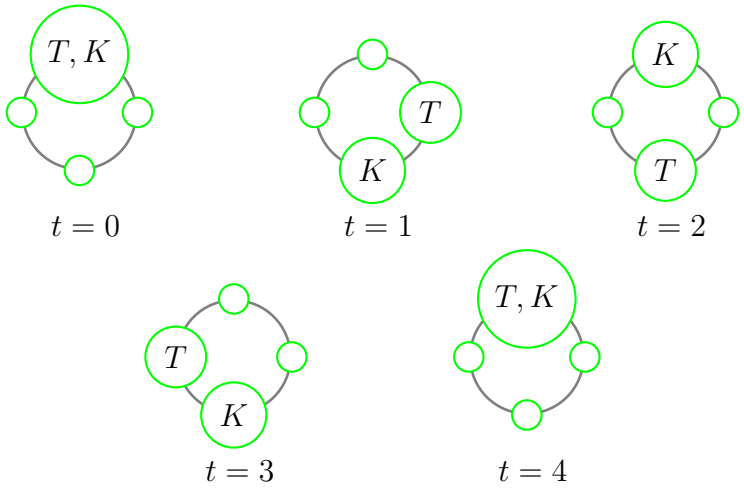
Fix a value $k \in \mathbb{N}^+$.

A t-rex and a kotasaurus are playing a game that involves hopping around a circular track of lily pads.[1] At the start, they stand on the same lily pad. Then, every second, the slow t-rex jumps one lily pad clockwise, while the swift kotasaurus jumps k 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 t-rex and kotasaurus to finish their game.

You may cite without proof the *coprime divisibility lemma*: for any integers a, b, and c, if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

As an example, here's how the game would go on a track of four lily pads if the kotasaurus can jump two lily pads per second (t is the number of seconds elapsed, and T represents the t-rex and K the kotasaurus):



[1] These are some *very* resilient lily pads.

HINT: One possible approach to this problem involves proving Lemma 1 below and using Lemma 1 to prove Lemma 2:

Lemma 1: For any integers n and k, we have $\gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}\right) = 1$.

Lemma 2: Let n be a positive natural number. Fix an integer k. If $s \in \mathbb{Z}$ is a solution to the congruence $kx \equiv 0 \pmod{n}$, then $\frac{n}{\gcd(n,k)} \mid s$.

Solution:

We first prove the two recommended lemmas, then prove the main claim. Note that by "Bézout's Lemma" we mean Corollary 8.3 from the course text (which was also presented in lecture).

(i) We first prove Lemma 1. Let n and k be integers.

Note that by the backward direction of Bézout's Lemma, there exist integer solutions to

$$nx + ky = \gcd(n, k),$$

since $\gcd(n, k) \mid \gcd(n, k)$ trivially. Dividing through by $\gcd(n, k)$, we find that the same x and y are integer solutions to

$$\frac{n}{\gcd(n,k)}x + \frac{k}{\gcd(n,k)}y = 1.$$

Since such solutions exist, it follows by the forward direction of Bézout's Lemma that $\gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}\right) \mid 1$. But the only positive integer divisor of 1 is itself, so we must have $\gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}\right) = 1$, as desired.

(ii) We now prove Lemma 2. Fix a positive modulus $n \in \mathbb{N}^+$ and a value $k \in \mathbb{Z}$. Let $s \in \mathbb{Z}$ be a solution to $kx \equiv 0 \pmod{n}$. So we have that $ks \equiv 0 \pmod{n}$, and thus by the definition of congruence that $n \mid ks$. By the definition of divisibility, there thus exists some $c \in \mathbb{Z}$ such that $nc = ks$.

Observe that $k = \frac{k}{\gcd(n,k)} \cdot \gcd(n, k)$, by which the preceding becomes

$$nc = \frac{k}{\gcd(n,k)} \cdot \gcd(n, k)s.$$

We divide through by $\gcd(n, k)$ (which is nonzero by definition), noting that $\frac{n}{\gcd(n,k)}$ is an integer:

$$\frac{n}{\gcd(n,k)} \cdot c = \frac{k}{\gcd(n,k)} \cdot s.$$

By the definition of divisibility, we therefore have that $\frac{n}{\gcd(n,k)} \mid \frac{k}{\gcd(n,k)} \cdot s$.

Since $\gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}\right) = 1$ by Lemma 1, it then follows by the coprime-divisibility lemma that $\frac{n}{\gcd(n,k)} \mid s$, as desired.

(iii) Now we proceed to the main claim. Label the lily pads 0 to $n-1$ starting at the lily pad on which the dinosaurs start. Observe that the t-rex will be on lily pad $t \bmod n$ after t seconds, while the kotasaurus will be on lily pad $kt \bmod n$ after t seconds. We thus want to find the smallest nonzero value of t for which $t \equiv kt \pmod{n}$. Subtracting through by t and factoring, this is equivalently $t(k-1) \equiv 0 \pmod{n}$.

By Lemma 2, we know that any nonzero solution $t = s$ to this congruence is such that $\frac{n}{\gcd(n,k-1)} \mid s$, so in particular (since both values are nonzero) $\frac{n}{\gcd(n,k-1)} \leq s$. Moreover, observe that $\frac{n}{\gcd(n,k-1)}$ is itself a solution to this congruence:

$$\begin{aligned} \frac{n}{\gcd(n,k-1)} \cdot (k-1) &\equiv n \cdot \frac{k-1}{\gcd(n,k-1)} \\ &\equiv 0 \cdot \frac{k-1}{\gcd(n,k-1)} \\ &\equiv 0 \pmod{n} \end{aligned}$$

since $\frac{k-1}{\gcd(n,k-1)}$ is an integer.

So we see that $\frac{k-1}{\gcd(n,k-1)}$ is both a lower bound on any nonzero solution and is itself a solution to the congruence. Therefore, we conclude that it must be the minimal nonzero solution. So the kotasaurus and t-rex will reunite after $\frac{k-1}{\gcd(n,k-1)}$ seconds.