Homework 5: Number Theory and Induction

Version 3: Updated 2/2 4 PM. Added extra credit problem.
Version 2: Updated 2/1 9 AM. Question 6 should be $T(n) = 3^n n!$
Due date: **Wednesday** February 7th at 11:59 PM
If you work with others (and you should!), remember to follow the collaboration policy outlined in the syllabus.
In general, you are graded on both the clarity and accuracy of your work. Your solution should be clear enough that someone in the class who had not seen the problem before would understand it.
We sometimes describe approximately how long our explanations are. These are intended to help you understand approximately how much detail we are expecting. You are allowed to have longer explanations, but explanations significantly longer than necessary may receive deductions.

Be sure to read the grading guidelines on the assignments page for more information on what we're looking for.

In order to assist with the transition from formal proofs to English proofs, we've published a style guide on the website containing some tips. This guide contains references to proof materials that we haven't taught yet, so don't worry if some of these terms are unfamiliar.

This homework comes in two parts. Part one is practice with modular arithmetic; part two is practice with induction.

We will have two separate gradescope submission boxes. Using one late day allows you to submit **both** parts one day later (e.g. one late day lets you submit both parts on Thursday February 8th).

The staff will focus on grading part 2 first. If you don't use any late days, we will get you feedback on part two before the midterm (we want to be really sure you get feedback on at least one induction problem in time). We will likely **not** get the part 1 feedback returned before the midterm.

Part I

1. Backwards Proofs [6 points]

A common error now that we're doing a lot of algebra is to write a "backwards" or "U-shaped" proof. For a proof to be valid, we must start from facts we know (either givens, or accepted facts, or supposing hypotheses to prove implications), and derive from them the statement we desire.
We cannot start from the equation to be shown and simplify it to something "obviously true."

Read the slides and watch the video on panopto and/or read the reading about backwards proofs. Then do these problems

(a) Complete the Backwards Proof Practice assignment on gradescope. This part will feel like a concept check (explanations appear when correct, problem is graded automatically, etc.) but counts in the homework category for grades. [4 points]

(b) On the practice, question 4 is an incorrect proof that $5|(9^2 - 4^2)$, which is the base case in an induction proof of $5|(9^n - 4^n)$ for integers $n \geq 2$. Write a correct proof of **only** the base case (this should be very short). [2 points]

2. Like -2 but better! [22 points]

In normal arithmetic, $a + 2 + (-2) = a$ for every integer a. So we say that -2 "undoes" 2. In modular arithmetic, a similar statement might be that $a+2+3 \equiv a \pmod 5$, so 3 "undoes 2 for $\pmod 5$ addition." More generally, given an integer n, we say that an integer b "undoes 2 for $\pmod n$ addition" if and only if for all integers a, $a + 2 + b \equiv a \pmod n$.

In this problem, you will show that for every integer n (where $n > 2$), there exists some integer b, where $1 \leq b \leq n$, which undoes 2 for $\pmod n$ addition.

(a) Write the statement "for every integer n (where $n > 2$), there exists some integer b, where $1 \leq b \leq n$, which undoes 2 for $\pmod n$ addition." in predicate logic. You should use the predicate "$\texttt{Undoes2}(b, n)$ to say "b undoes 2 in $\pmod n$ arithmetic" [2 points]

(b) You (hopefully!) have a statement which starts $\forall n \exists b$. Recall that since the $\exists$ come second, the value of b is allowed to depend on n. Give a formula for the b (in range $1 \leq b \leq n$) for which $\texttt{Undoes2}(b, n)$ evaluates to true. The formula will depend on n. [2 points]

(c) Now do the actual proof. You'll start the proof by introducing an arbitrary variable (you're proving a $\forall$) then you'll be doing an exists proof (tell us what value of b you want and argue that it makes $\texttt{Undoes2}()$ evaluate to true). Be sure you don't do a backwards proof! **For this part, you may not use facts about modular equivalences**, you may only use the definitions of divides and equivalence mod n and algebra (applied to equations or individual numbers, not to equivalences). [8 points]
Hint: Don't forget that the definition of $\texttt{Undoes2}$ has another $\forall$ quantifier inside of it!

Now that we've shown there is a way to undo 2, next we're going to try to show there's not a bunch of different ways. In this problem, you'll show that for every integer n (where $n > 2$), for all integers b, b' where both b and b' undo 2 for $\pmod n$ addition, that $b \equiv b' \pmod n$. Note that we've gotten rid of the $1 \leq b \leq n$ requirement in this part! [6 points]

(d) Write the statement above in predicate logic. Use the predicate $\texttt{Undoes2}(b, n)$ for "b undoes 2 for $\pmod n$ arithmetic." [2 points]

(e) Now write an English proof of the statement. For this part you may use theorems shown in class and on the Number Theory Reference Sheet. [8 points]
You may also use the following fact:

Theorem 1 (Transitivity of Equivalence)**.** *For all integers a, b, c, n with $n > 0$:*
if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$.

(f) For similar concepts in modular arithmetic, people will say things like "There is a unique number that undoes 2 $\pmod n$." Ponder why this use of "unique" makes sense, but also why this is a little different from the example of "unique" we saw in class. You do not have to write anything for this part [0 points]

3. GCD Proof [12 points]

Bezout's Theorem (one of the theorems in the optional number theory content) tells us that if a and b are positive integers, then there exist some integers s and t such that $\gcd(a, b) = sa + tb$.

However, the converse isn't always true: there could exist some integers s and t such that $d = sa + tb$, but d isn't necessarily $\gcd(a, b)$. In this problem, we will see a special case where the converse does hold.

(a) For all **positive** integers a and b, prove the following claim: if there exist some integers s and t such that $sa + tb = 1$, then $\gcd(a, b) = 1$. [9 points]

You may use without proof that if any integer k satisfies $k|1$, then k must be either 1 or -1.

Hint: The facts about GCD that you will need for this problem are that if $a = \gcd(b, c)$ then $a|b$ and $a|c$, and it is the largest integer that does this.

(b) Use part (a) to show that $\gcd(n, n + 1) = 1$ for all positive integers n. [3 points]

4. Transitivity [8 points]

Prove that for all integers a, b, c, and n, where $n > 0$: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

Extra Credit: Exponentially increasing fun [0 points]

Since $a \equiv a \,\%\, n \pmod{n}$, we know that we can reduce the base of an exponent in $\pmod{n}$ arithmetic. That is:

$$a^k \equiv (a \,\%\, n)^k \pmod{n}.$$

But the same is **not** true of the exponent! That is, we cannot say that $a^k \equiv a^{(k \,\%\, n)} \pmod{n}$. Consider, for instance, that $2^{10} \equiv 1 \pmod{3}$ but $2^{(10 \,\%\, 3)} \equiv 2 \pmod{3}$. The correct way to simplify exponents is quite a bit more subtle. In this problem you'll prove it in steps.

For these proofs you may use any theorem on the number theory reference sheet, even the ones we haven't proven yet in class.

(a) Let $R = \{t \in \mathbb{Z} : 1 \leq t \leq n-1 \wedge \gcd(t, n) = 1\}$. Define the set $aR = \{(ax) \,\%\, n : x \in R\}$. Prove that $aR = R$ for every integer $a > 0$ with $\gcd(a, n) = 1$.

(b) Consider the product of all elements in R (taken $\pmod{n}$) and consider the product of all the elements in aR (again, taken $\pmod{n}$). By comparing these two expressions, conclude that for all $a \in R$ we have $a^{\varphi(n)} \equiv 1 \pmod{n}$ where $\varphi(n) = |R|$.

(c) Use the previous part to show that for any $b \geq 0$ and $a \in R$ we have $a^b \equiv a^{(b \,\%\, \varphi(n))} \pmod{n}$.

(d) Now suppose that $y = x^e \pmod{n}$ for some x with $\gcd(x, n) = 1$ and e some integer ≥ 0 such that $\gcd(e, \varphi(n)) = 1$. Let $d = e^{-1} \pmod{\varphi(n)}$. Prove that $y^d \equiv x \pmod{n}$.

(e) Prove the following two facts about φ: First, if p is prime then $\varphi(p) = p - 1$. Second, for any positive integers a and b with $\gcd(a, b) = 1$, we have $\varphi(ab) = \varphi(a)\varphi(b)$.

These facts together are the basis for the most-widely used "public key encryption system." One chooses $n = pq$ for large primes p and q, and a value of e. The numbers n and e are made public to anyone who wants to send a message securely. To send a message x, the sender computes $y = x^e \,\%\, n$ and sends y (the "encrypted text"). To decrypt, one computes $y^d \,\%\, n$ (note that the recipient must be the one who chose p, q so they can calculate d). The security of the system relies on it being hard to compute d from just e and m.

Part II

5. First Induction [20 points]

Prove that for all positive integers n, the following equality is true:

$$4 \cdot 1^3 + 4 \cdot 2^3 + 4 \cdot 3^3 + \cdots + 4 \cdot n^3 = n^2(n+1)^2$$

You must use induction for this problem. Be sure to start by defining your predicate $P()$.

6. More Induction [20 points]

Suppose we have the following recursively defined function, $T(n)$:

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ 3 & \text{if } n = 1 \\ (9n^2 - 9n) \cdot T(n-2) & \text{if } n \text{ is a natural number and } n \geq 2 \end{cases}$$

Use induction to prove that for all integers n with $n \geq 0$, $T(n) = 3^n n!$.
Recall that for a positive integer n, $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1$, and that $0! = 1$.

7. Feedback [1 point]

Answer these questions on the separate gradescope box for this question.

Please keep track of how much time you spend on this homework and answer the following questions. This can help us calibrate future assignments and future iterations of the course, and can help you identify which areas are most challenging for you.

- How many hours did you spend working on this assignment (excluding any extra credit questions, if applicable)? Report your estimate to the nearest hour.
- Which problem did you spend the most time on?
- Any other feedback for us?