Homework 5: Number Theory and Induction

Due date: Wednesday February 9th at 10 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.

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.

Additionally, last quarter we recognized some common mistakes that students made on HW4. We made a document discussing common mistakes and how they can be avoided. This document was tailored to last quarter and potentially contains a lot of overlap with the above style guide. However, you may find it useful if you feel particularly stuck or uncertain about your English proofs.

Finally, be sure to read the grading guidelines for more information on what we're looking for.

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 10).

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 ends (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 ends, but as you've already done proofs involving modular arithmetic on prior homeworks, that feedback is lower-priority.

Part I

1. Euclid's algorithm [8 points]

Compute each of the following using Euclid's Algorithm. Show your intermediate results both as a sequence of gcd() calls, and with the tableau of values.

(a) $\gcd(362, 112)$ [6 points]

(b) $\gcd(3^{30} + 1, 3)$ [2 points]

2. Inverses [14 points]

(a) Compute the multiplicative inverse of $15 \pmod{103}$. Use the Extended Euclidean algorithm, showing the tableau and the sequence of substitutions.

Express your final answer as an integer between 0 and 102 inclusive. [6 points]

(b) Find **all** integer solutions to

$$15x \equiv 11 \pmod{103}$$

You may use part (a) without repeating explanation, but make sure you have algebra to justify your set of possible answers. That justification must include applying the definition of equivalence $\pmod{103}$. [8 points]

3. GCD proof [6 points]

Show that if $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$ then $b \equiv c \pmod{d}$ where $d = \text{gcd}(m, n)$.

4. Find The Bug [16 points]

4.1. I'm not FIBbing

Your friend is doing a proof with the Fibonacci numbers. Recall that $f(0) = f(1) = 1$ and for all $n \geq 2$, $f(n) = f(n-1) + f(n-2)$.

They are trying to show that $f(4) = 5$ – here is the proof they show you:

$$\begin{aligned} f(4) &= 5 \\ f(3) + f(2) &= 5 \\ [f(2) + f(1)] + f(2) &= 5 \\ 2f(2) + 1 &= 5 \\ 2f(2) &= 4 \\ 2(f(1) + f(0)) &= 4 \\ 2(1+1) &= 4 \\ 4 &= 4 \end{aligned}$$

(a) Clearly explain why the proof is incorrect. Your explanation must deal with the proof directly, not just the statement they are showing (e.g. just providing a counter-example is not sufficient for this part). [3 points]

(b) If the statement is correct, then write a correct proof. If it is incorrect, provide a counter example. [5 points]

4.2. Well...maybe I'm fibbing

Another friend wishes to show $(x-3)(-x+4) = x^2 - 7x + 12$ is true for all x. They show you their proof:

$$\begin{aligned} &(x-3)(-x+4) = x^2 - 7x + 12 \\ &[(x-3)(-x+4)]^2 = (x^2 - 7x + 12)^2 \\ &(x^2 - 6x + 9)(x^2 - 8x + 16) = (x^4 - 7x^3 + 12x^2) + (-7x^3 + 49x^2 - 84x) + (12x^2 - 84x + 144) \\ &(x^4 - 8x^3 + 16x^2) + (-6x^3 + 48x^2 - 96x) + (9x^2 - 72x + 144) = x^4 - 14x^3 + 73x^2 - 168x + 144 \\ &x^4 - 14x^3 + 73x^2 - 168x + 144 = x^4 - 14x^3 + 73x^2 - 168x + 144 \end{aligned}$$

(a) Clearly explain why the proof is incorrect. Your explanation must deal with the proof directly, not just the statement they are showing (e.g. just providing a counter-example is not sufficient for this part). [3 points]

(b) If the statement is correct, then write a correct proof. If it is incorrect, provide a counter example. [5 points]

Extra Credit: Exponentially increasing fun [0 points]

Since $a\%n \equiv a \pmod{n}$, 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 $2^{10}\%3 = 1$ but $2^{10\%3}\%3 = 2^1\%3 = 2$. 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 $\%n$) and consider the product of all the elements in aR (again, taken $\%n$). 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. Induction Divides [20 points]

Prove that $7 \mid (8^n - 1)$ for all $n \in \mathbb{N}$, by induction on n.

Hint: In your inductive step, you'll need to be creative to apply your inductive hypothesis. Focus on forcing the right expression to appear.

6. Induction Code [20 points]

Consider the following code snippet.

```
public int Mystery(int n){
    if(n < 0)
        throw new InvalidInputException();
    if(n == 0)
        return 2;
    if(n == 1)
        return 7;
    return Mystery(n-1) + 2*Mystery(n-2);
}
```

Use induction to show that `Mystery(n)`$= 3 \cdot 2^n + (-1)^{n+7}$ for all integers $n \geq 0$.