Homework 5: Number Theory and Induction

Changelog: This is Version 3 (posted Monday Nov 8 10 PM). We updated the due date, and corrected an additional typo in extra credit part d (there is no "m" in the problem, and one of the mods were corrected to %.)

Due date: Wednesday November 11th at 11:59 PM (Seattle time, i.e. GMT-8)
Note the time zone change! Seattle ends daylight saving time on November 1.

If you work with others (and you should!), remember to follow the collaboration policy.
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.

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 slightly shorter than a normal homework. You should aim to finish it by Friday (just like a normal homework). You have all the tools you need to approach the problems in part 1 from the lecture slides available at the release of this homework. But it is officially due with part two.

Part two is practice with induction (which we will start to cover on Monday Nov. 2).

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 Tuesday Nov. 10).

The staff will focus on grading part 2 first, so that you can get that feedback in time for the midterm. We will likely not get the part 1 feedback returned before the midterm ends.

Part I

1. Euclid's algorithm [10 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) $\gcd(225, 65)$ [4 points]

(b) $\gcd(354, 123)$ [5 points]

(c) $\gcd(3^{30} + 1, 3)$ [1 point]

2. Inverses [20 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. [5 points]

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

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

You must show **all** your work for this part. See lecture 13 for an example of the work needed. [8 points]

(c) Prove there are no integer solutions to

$$10x \equiv 3 \pmod{15}$$

Note: it's not enough to say that 10 does not have a multiplicative inverse $\pmod{15}$. If that were enough, then you could say the same for $10x \equiv 10 \pmod{15}$, but $x = 1$ is a solution to that equivalence.

You'll want to use proof by contradiction (suppose that there is an integer solution and go from there). [7 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 $d = \gcd(m, n)$.

4. A Proof By Contradiction [7 points]

Let p be a prime number, show that $\sqrt{p}$ is irrational. You may want to adapt the proof that the $\sqrt{2}$ is irrational. You can use the following fact without proof: For integers a, b and a prime number p: if $p|(ab)$ then $p|a$ or $p|b$.

5. Modular Exponentiation [7 points]

Compute $3^{138}\%100$ using the efficient modular exponentiation algorithm. Show your intermediate results.

6. Find The Bug [16 points]

6.1. 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]

6.2. 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:

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

(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.

(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 $y = x^e\%n$ 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

7. 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.

8. 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 $n \geq 0$.

9. Well that just doesn't sound right [8 points]

Consider the following (very incorrect) induction proof:

① Let $P(n)$ be "$5n = 0$"
We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

② Base Case: $n = 0$
If $n = 0$ then $5n = 5 \cdot 0 = 0$, so $P(0)$ is true.

③ Inductive Hypothesis: Suppose $P(n)$ holds for $n = 0, \ldots, k$ for an arbitrary integer $k \geq 0$

④ Inductive Step:
Ⓐ We want to prove $P(k+1)$ is true, i.e. $5(k+1) = 0$.
Ⓑ Observe that $5(k+1) = 5(s) + 5(t)$. for integers s, t with $0 \leq s < k+1$ and $0 \leq t < k+1$.
Ⓒ Applying the inductive hypothesis twice, we have $5s = 0$ and $5t = 0$.
Ⓓ Substituting both into the original equation, we get: $5(k+1) = 0 + 0$, so $5(k+1) = 0$, as required.
⑤ The result follows for all $n \geq 0$ by induction.

(a) Find the smallest counterexample to the claim that $P(n)$ holds for all $n \in \mathbb{N}$. [3 points] You should both (1) show that your example is a counterexample and (2) argue why all smaller natural numbers are not counterexamples.

(b) Clearly identify the flaw in the proof; it will help to run through the proof with your smallest counterexample. For ease of explanation, we've taken the (unusual) step of labelling every sentence. [5 points]