# Homework 4: Number Theory, Induction

**Due date: Friday, July 19th 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 your work's clarity and accuracy. 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 expect. You can have longer explanations, but explanations significantly longer than necessary may receive deductions.

## 1. Contradiction [16 points]

Prove the following claims by contradiction.

(a) There does not exist integers $a, b$ such that $3a - 9b = 2$. [8 points]

(b) For all real numbers $x > 0$, $x + \frac{1}{x} \geq 2$. [8 points]

## 2. Like $-3$ but Better! [16 points]

(a) For any integer $n$ (where $n > 3$), we say that an integer $b$ "undoes 3 for $\pmod{n}$ addition" if and only if for all integers $a$, $a + 3 + b \equiv a \pmod{n}$. We say $b$ "undoes" 3 because adding $b$ takes you back to $a$ (where you would have been without adding 3).

Show that for any integer $n$ (where $n > 3$), there exists some integer $b$, where $1 \leq b \leq n$, which undoes 3 for $\pmod{n}$ addition. [8 points]

(b) In this problem, you'll show that for any integer $n$ (where $n > 3$), for all integers $b, b'$ where both $b$ and $b'$ undo 3 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! [8 points]

- Write the statement above in predicate logic. Use the predicate `Undoes3`$(b, n)$ for "$b$ undoes 3 for $\pmod{n}$ arithmetic."
- Now write an English proof of the statement.

(c) For similar concepts in modular arithmetic, people will say things like "There is a unique number that undoes 3 mod $n$." 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. First Induction [20 points]

Prove, by induction, that

$$\sum_{i=0}^{n}(3i+1) = \frac{3n^2+5n+2}{2}$$

holds for all $n \in \mathbb{N}$.

Write an *English* inductive proof, following the template given in lecture.

## 4. Diving In (duction) [20 points]

Prove, by induction, that $2n^3 + n$ is divisible by 3 for any $n \in \mathbb{N}$.

Write an *English* inductive proof, following the template given in lecture.

## 5. Prove or Disprove [20 Points]

For each of the following problems, either prove the above statement or disprove the above statement with a counterexample.

(a) Prove or Disprove that for arbitrary sets $A$, $B$, that $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$

(b) Prove or Disprove that for arbitrary sets $A$, $B$, that $\mathcal{P}(A \setminus (A \cap B)) = \mathcal{P}(A \cap \overline{B})$

## 6. Extra Credit: Walk Like an Encryption

We know that we can reduce the base of an exponent modulo $m : a^k \equiv a \mod m$. But the same is not true of the exponent! That is, we cannot write $a^k \equiv a^{k \mod m} \mod m$. This is easily seen to be false in general. Consider, for instance, that $2^{10} \mod 3 \equiv 1$ but $2^{10 \mod 3} \equiv 2^1 \mod 3 \equiv 2$. The correct law for the exponent is more subtle. We will prove it in steps....

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

(b) Consider the product of all the elements in $R$ modulo $m$ and the elements in $aR$ modulo $m$. By comparing those two expressions, conclude that, for all $a \in R$, we have $a^{\varphi(m)} \equiv 1 \mod m$, where $\varphi(m) = |R|$.

(c) Use the last result to show that, for any $b \geq 0$ and $a \in R$, we have $a^b \equiv a^{b \mod \varphi(m)} \mod m$.

(d) Finally, prove the following two facts about the function $\varphi$ above. First, if $p$ is prime, then $\varphi(p) = p - 1$. Second, for any primes $a$ and $b$ with $a \neq b$, we have $\varphi(ab) = \varphi(a)\varphi(b)$. (Or slightly more challenging: show this second claim for all positive integers $a$ and $b$ with $\text{gcd}(a, b) = 1$.

The second fact of part (d) implies that, if $p$ and $q$ are primes, then $\varphi(pq) = (p - 1)(q - 1)$. That along with part (c) prove the final claim from lecture about RSA, completing the proof of correctness of the algorithm.

## 7. Feedback [1 point]

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?