CSE 311: Foundations of Computing I Winter 2026

Problem Set 3

Due: Friday, Feb 6th by **11:00pm**

Instructions

Write up carefully argued solutions to the following problems. Each solution should be clear enough that it can explain (to someone who does not already understand the answer) why it works.

Collaboration policy. You are required to submit your own solutions. You are allowed to discuss the homework with other students. However, the **write up** must clearly be your own, and moreover, you must be able to explain your solution at any time. We reserve ourselves the right to ask you to explain your work at any time in the course of this class.

Solutions submission. Submit your solution via Gradescope. In particular:

- Each numbered task should be solved on its own page (or pages). Do not write your name on the individual pages. (Gradescope will handle that.)
- When you upload your pages, make sure each one is **properly rotated**. If not, you can use the Gradescope controls to turn them to the proper orientation.
- Follow the Gradescope prompt to **link tasks to pages**.
- You are not required to typeset your solution, but your submission must be **legible**. It is your responsibility to make sure solutions are readable — we will *not* grade unreadable write-ups.
- Extra practice problems are included at the bottom of the assignment. These will not be graded, so don't submit solutions to them.

Task 1 – Acts of Mod [10 pts]

Let m and n be positive integers, with $\gcd(m, n) = 1$. Consider the following claim: for any integers a and b, there exists an integer x such that $x \equiv_m a$ and $x \equiv_n b$. [1]

a) Write a **formal** proof that the claim holds. The proof should begin with the following lines:

1.	$m > 0 \wedge n > 0$	Given
2.	$\gcd(m, n) = 1$	Given
	$\vdots$	

b) Translate your formal proof to an **English** proof.

Hints:

- An application of Bézout's theorem grants us integers s and t such that $sm + tn = 1$. Then, the number $x = bsm + atn$ is a solution to the system of congruences.
- In your formal proof, you should use the following formulation of Bézout's theorem:

  Bézout's Theorem: $\forall u, \forall v, \big((u > 0 \wedge v > 0) \rightarrow \exists s, \exists t, (su + tv = \gcd(u, v))\big)$

- The inference rules CITE or APPLY will be useful in your formal proof. Note that these inference rules can be used with theorems with any number of $\forall$-quantifiers.
- In your formal proof, you are allowed to Intro/Elim multiple $\forall$-quantifiers in one step. Likewise, you are allowed to Intro/Elim multiple $\exists$-quantifiers in one step.

[1] This claim is a simple version of (the existence part of) the Chinese Remainder Theorem.

Task 2 – Euclidean, My Dear Watson [10 pts]

We say that an equation is in "**standard form**" if it looks like $Ax \equiv_n B$ for some constants A, B, and n. The first equation below is in standard form, but the second is *not*.

Solve each of the below modular equations by following these steps, showing your work as described next.

1. If the modular equation is *not* in standard form, then **transform** it into standard form.

   Show the sequence of operations, either adding to both sides or simplifying (e.g., algebraically modifying terms on individual sides as done in lecture).

2. **Calculate** *one solution* to the modular equation in standard form using the Extended Euclidean Algorithm.

   Show your work by writing out the sequence of quotients and remainders, the resulting tableau, and the sequence of substitutions needed to calculate the relevant multiplicative inverse. Then, show how multiplying the initial equation on both sides by the multiplicative inverse gives you a solution to the equation.

3. **State** *all integer solutions* to the modular equation in standard form.

   Your answer should be of the form "$x = C + Dk$ for any integer k", where C and D are integers with $0 \leqslant C < D$.

4. If the original modular equation was *not* in standard form, justify briefly (in one sentence) why the solutions to the equation in standard form are the same as the solutions to the original equation.

5. Show that there is some solution $z \in \mathbb{Z}$ such that $z \geqslant 1000$.

a) $9x \equiv_{41} 7$

b) $54x - 6 \equiv_{42} 7 - 19x$

Task 3 – Sum Kind of Wonderful [10 pts]

Prove, by induction, that

$$\sum_{i=0}^{n}(11(12)^i + 2) = (12)^{n+1} + 2n + 1$$

holds for all integers $n \geqslant 0$.

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

Task 4 – Winnie the Two [10 pts]

Prove, by induction, that $3 \mid n^3 + 2n$ holds for all $n \geqslant 0$.

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

Hint: In this case, the claim is that $3 \mid n^3 + 2n$, so you need to prove that the definition of divides holds with 3 and $n^3 + 2n$. The definition is an equation, so once you prove that an equation of the right shape holds for n, you can say that you have proven $P(n)$.

Task 5 – Barking Up the Strong Tree [10 pts]

When you first learned **recursion** in CSE 123, a mysterious person gave you the following recursive Java method and claimed that it behaves like the natural-number version of Math.pow():

```
int mysteriousPow(int b, int m) {  /* Assumes: b >= 1 and m >= 0 */
    if (m == 0) {
        return 1;
    } else if (m == 1) {
        return b;
    } else {
        return (b - 1) * mysteriousPow(b, m - 1) + b * mysteriousPow(b, m - 2);
    }
}
```

You wrote some tests and realized that this method might be correct, but you didn't know how to prove it rigorously...until you are taking CSE 311 and learn strong induction! Now, let's try to prove the correctness of this method. Not sure what I mean? Let's put it another way:

Let b be a positive integer. The function $f(m)$ is defined for all integers $m \geqslant 0$ recursively as follows:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= b \\ f(m) &= (b-1) \cdot f(m-1) + b \cdot f(m-2) \qquad \text{if } m \geqslant 2 \end{aligned}$$

Use strong induction to prove that the following holds for all integers $n \geqslant 0$:

$$f(n) = b^n$$

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

Task 6 – Extra Credit: Stone By the Company He Keeps [0 pts]

Consider an infinite sequence of positions $1, 2, 3, \ldots$ and suppose we have a stone at position 1 and another stone at position 2. In each step, we choose one of the stones and move it according to the following rule: Say we decide to move the stone at position i; if the other stone is not at any of the positions $i+1, i+2, \ldots, 2i$, then it goes to $2i$, otherwise it goes to $2i+1$.

For example, in the first step, if we move the stone at position 1, it will go to 3 and if we move the stone at position 2 it will go to 4. Note: no matter how we move the stones, they will never be at the same position.

Use induction to prove that, for any given positive integer n, it is possible to move one of the stones to position n. For example, if $n = 7$ first we move the stone at position 1 to 3. Then, we move the stone at position 2 to 5 Finally, we move the stone at position 3 to 7.

Task 7 – Optional Practice Problems (Ungraded) [0 pts]

Note: The problems below are **optional practice problems** that are **not required and will not be graded**. They are provided to help you practice; you do not need to submit solutions to these problems.

Find solutions to each of the following modular equations.

a) $15x \equiv_{28} 14$

b) $13x - 3 \equiv_7 x$

Prove each of the following claims. It should not be necessary to use induction.

c) Let n and c be positive integers. For any integers a and b, if $a \equiv_n b$, then $ca \equiv_{cn} cb$. (Note that the subscript has changed from n to cn!)

d) Let n and k be positive integers, with $\gcd(n, k) = 1$. If $ka \equiv_n kb$, then $a \equiv_n b$, for any integers a and b.

e) For any positive integer a, $\gcd(a, a + 1) = 1$.

f) For any positive integers a and b, $\gcd(a, b) = \gcd(b, a)$

g) For any positive integers a, b, and c, $\gcd(ca, cb) = c \cdot \gcd(a, b)$.

Prove each of the following claims using induction. (You must decide by yourself whether to use weak or strong induction.)

h) $6 \mid (7^n - 1)$ for all integers $n \geqslant 1$.

i) Every positive integer is either even or odd.

j) If $a \equiv_n b$ for some positive integer n, then $a^k \equiv_n b^k$ for all integers $k \geqslant 0$.

k) $2^n > n^2$ for all integers $n \geqslant 5$.

l) Every amount of postage of $\geqslant 12$ cents can be formed using only 4-cent and 5-cent stamps.

m) Consider a sequence defined by $a_1 = 1$, $a_2 = 3$, and $a_n = 3a_{n-1} - 2a_{n-2}$ for $n \geqslant 3$. Prove that $a_n = 2^n - 1$ for all $n \geqslant 1$.