Due Date: Thursday, September 8 at 5PM EDT

Carefully read and provide solutions to the problems below, showing all work required to justify any conclusions you make. You are encouraged to collaborate with your classmates, but all solutions turned in should be your own work. If you do collaborate, please record the names of those other students on your submitted work. Finally, your work should be submitted as a PDF on Gradescope before the listed due date.

Textbook problems: 2.4, 2.5, 3.2, 5.1

*Optional problem: 3.4**

* *The curve $y^2 = x^3 + 8$ is an example of an elliptic curve. Curves like this are useful for cryptography because their rational points (points whose coordinates are rational numbers) can be combined in ways that are difficult for even computers to untangle.*

Problem 1. (Lecture 2.1, Exercise 1) Use the Axioms of Arithmetic to prove the following statements for any $a, b, c \in \mathbb{Z}$

(a) If $a + c = b + c$ then $a = b$.

(b) $a \cdot 0 = 0$.

(c) $(-a) \cdot b = -(ab)$.

(d) $(-a) \cdot (-b) = ab$.

(e) If $ab = 0$ then $a = 0$ or $b = 0$. *Hint: use induction (axiom 2) or reduce to the case where $a, b \geq 0$ and explain what ab represents in that case.*

(f) If $ac = bc$ and $c \neq 0$, then $a = b$.

Problem 2. (Lecture 2.1, Exercise 3) Prove the following statements for any $a, b, c, d \in \mathbb{Z}$.

(a) If $a \mid b$ and $a \mid c$ then a also divides $b + c, b - c$ and bc.

(b) If $a \mid b$ and $a \mid c$ then $a^2 \mid bc$.

(c) $a \equiv a \pmod{d}$.

(d) If $a \equiv b \pmod{d}$ then $b \equiv a \pmod{d}$.

(e) If $a \equiv b \pmod{d}$ and $b \equiv c \pmod{d}$, then $a \equiv c \pmod{d}$.

Problem 3. (a) Use induction to prove that for all $k \in \mathbb{N}$, 3 divides $10^k - 1$.

(b) Use this to prove the "divisible by 3" detector: for any $n \in \mathbb{N}$, with digits a_0 (the 1s digit), a_1 (the 10s digit), a_2 (the 100s digit), etc., if $m = a_0 + a_1 + a_2 + \ldots + a_k$ (where a_k is the first digit of n) then $n \equiv m \pmod{3}$. That is, n is divisible by 3 if and only if the sum of its digits is also divisible by 3.