# Chapter 4.1: Modular Arithmetic

Wednesday, July 8

## Divisibility Recap

1. Using the fact that 1 is the smallest positive integer, prove that if $a|b$ then $|a| \leq |b|$.
2. Prove that if $a|b$ and $b|a$ then $|a| = |b|$ (or, $a = \pm b$).

## Modular Arithmetic

Evaluate the following:

1. $44 \pmod 3$
2. $171 \pmod{12}$
3. $-26 \pmod 5$
4. $199^2 \pmod 5$
5. $(2301 \pmod 3)^2 \pmod 5$
6. $23^{88} \pmod 2$
7. $2^{100} \pmod{10}$
8. $2737 \cdot 8184 \pmod 9$
9. $2^{64} \pmod{13}$
10. $88^5 \pmod{90}$
11. $97 \cdot 85 \pmod{100}$
12. $155 \cdot 822 \pmod{10}$

## Squares

1. Prove that an integer $a$ is divisible by 5 if and only if $a^2$ is divisible by 5 (proof by cases).
2. Prove that an integer $a^2$ is divisible by 3 if and only if it is divisible by 9.
3. Prove that 98765432 is not a perfect square.
4. Using the fact that $n^2 \equiv 0$ or $n^2 \equiv 1 \pmod 4$, prove that 111111 cannot be written as the sum of any two square numbers (what are the possibilities for $a^2 + b^2 \pmod 4$?)

## Method of Nines

1. Use the Method of Nines to show that $35121 \cdot 87122 \neq 3059911762$.
2. Find an example of an error in a multiplication problem that the Method of Nines fails to Catch.

## The Trouble With Division in $\mathbb{Z}_m$

1. Suppose that $4a \equiv 4b \pmod{16}$? What is the most you can say about $a$ and $b$?
2. Suppose that $7a \equiv 7b \pmod{16}$? What is the most you can say about $a$ and $b$?
3. A number $a \in \mathbb{Z}_m$ is called a *zero divisor* if there is some non-zero $b \in \mathbb{Z}_m$ such that $ab = 0$. Prove: if $a|m$ then $a$ is a zero divisor in $\mathbb{Z}_m$.
4. Prove that if $a$ is a zero divisor and $b$ is any number, then $ab$ is a zero divisor.
5. Prove that if there is some $d > 1$ such that $d|a$ and $d|m$, then $a$ is a zero divisor in $\mathbb{Z}_m$.
6. A number $a \in \mathbb{Z}_m$ is called a *unit* if there is some $b \in \mathbb{Z}_m$ such that $ab = 1$. Prove: the product of two units is a unit.
7. Prove that no number can be both a unit and a zero divisor.
8. (Harder) Prove that every number is $\mathbb{Z}_m$ is either a zero divisor or a unit.
9. What are the zero divisors in $\mathbb{Z}$? What are the units? What numbers are neither?
10. For what values of $m$ is every non-zero $a \in \mathbb{Z}_m$ a unit?