Lecture 11: Fermat's Little Theorem

Modular arithmetic is an incredibly useful tool. For us, it will solve:

1. Divisibility problems: Does $524$ divide $n - n$ for any $n \in \mathbb{N}$?

2. Questions about large numbers: What is the last digit of $(1739)^{1098}$?

3. Non-Existence of Solutions to Diophantine equations: Does $x^2 - 3y^2 = 15$ have a solution with $x, y \in \mathbb{Z}$?

8.4: Modular arithmetic is Arithmetic

Prop. 6.25: Let $n \in \mathbb{N}$. Suppose $a \equiv a' \mod n$ and $b \equiv b' \mod n$. Then

$a + b \equiv a' + b' \mod n$, $a \cdot b \equiv a' \cdot b' \mod n$

Example:

$49 \cdot 598 \equiv ? \mod 5$

Since $49 \equiv 4 \mod 5$, $598 \equiv 3 \mod 5$, then by Prop. 6.25, $4 \cdot 3 \equiv 12 \mod 5$ and $12 \equiv 2 \mod 5$. (Note: $4 \cdot 3 = 12 \equiv 2 \mod 5$)

Thm. 6.35: (Little Fermat's Theorem)

Let $p \in \mathbb{N}$ be a prime and $a \in \mathbb{Z}$ an integer.

$a \equiv a \mod p$

Exercise: Prove this! (Hint: by induction on $a \in \mathbb{N}$.)

Application: $p = 521$, then $521 \equiv 1 \mod 521$.

Now this means $a - a \equiv 0 \mod 521 \rightarrow 521 \mid (a - a)$, $a \in \mathbb{Z}$. (Which it does.)