Notation Note: There are two uses of (mod n). The first is as a *function*: given an integer, we can reduce it modulo n, e.g.

$$20 \pmod 7 = 6.$$

Note that we're using an $=$, not a $\equiv$, because the left hand side is *literally the same* as the right hand side. The second use of (mod n) is as a signifier that we're not requiring equality but are only requiring congruence, e.g.

$$20 \equiv 6 \pmod 7 \qquad 20 \equiv 34 \pmod 7 \qquad 20 \equiv -1 \pmod 7$$

The first use of the notation inspires the following:

Definition: $\mathbb{Z}_n := \{0, 1, 2 \ldots, n-1\}$.
So then for any $a \in \mathbb{Z}$, $a \pmod n \in \mathbb{Z}_n$.

Last time we proved

Fermat's Little Theorem: For any $a \not\equiv 0 \pmod p$, we have $a^{p-1} \equiv 1 \pmod p$.

Example: What is $3^{2018} \pmod 7$?
Kimberly: $3^{2018} = (3^6)^{336} \cdot 3^2 \equiv 3^2 \equiv 2 \pmod 7$
Max: Notice that 2016 is a multiple of 6: it's even, and adding the digits yields a multiple of 3. So $3^{2016} = (3^6)^x$ for some x. Thus $3^{2018} = (3^6)^x 3^2 \equiv 9 \equiv 2 \pmod 7$ by Fermat's Little Thm.

Recall the idea of the proof.
Proof of FLT: (little not last)
Idea: Pick $a \not\equiv 0 \pmod p$, consider the ath row in the multiplication table of $\mathbb{Z}_p$. This is $1a, 2a, 3a, \ldots, (p-1)a$, all mod p. By the Sudoku Rule, the row is a permutation of $1, 2, \ldots, , p-1$. Multiply all of na and all of n together, for $1 \le n \le p-1$. These must be the same by the Sudoku rule, so

$$a^{p-1}(p-1)! = (1a)(2a)\cdots((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \equiv (p-1)! \pmod p$$

Dividing by $(p-1)!$ we get $a^{p-1} \equiv 1 \pmod p$. □

Recall the formal statement of the Sudoku rule:
Proposition: If $ak \equiv bk \pmod n$, and k is relatively prime to n, then $a \equiv b \pmod n$.
Equivalently, the contrapositive says that $a \not\equiv b \pmod n \implies ak \not\equiv bk \pmod n$ as long as k is relatively prime to n. This shows that the kth row of the multiplication table of $\mathbb{Z}_n$ is a permutation of $1, 2, \ldots, n-1$. Sudoku!

Note that the above argument only holds when $(k, n) = 1$. What if we relax this condition? In other words, is the Sudoku Rule still a thing in the kth row when k isn't relatively prime

to n? Oliver points out that we could take $k = n$, in which case the sudoku rule breaks very badly since every element of the row will be 0. Max gave another example: the 3rd row of the (mod 6) multiplication table consists of 0's and 3's. In fact, looking back at the multiplication table (mod 6) we see that the *only* rows in which the Sudoku Rule holds are the ones that are relatively prime to 6.

This leads to the fundamental question: can we do all our usual arithmetic (mod n)?

Answer: Basically, yes. You can add, subtract, and multiply just fine. But you have to be careful with division: it's ok to divide (mod n) whenever we're dividing by something relatively prime to n, but otherwise you might run into problems. It's thus useful to restrict our attention to the relatively prime numbers:

Definition: $\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n : (a, n) = 1\}$. (note: read aloud as "Z-n-cross".)

Examples: $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. $\mathbb{Z}_6^\times = \{1, 5\}$. $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$. To get a better sense of what's happening, let's write the multiplication table (mod 8):

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Note that the sudoku rule holds in every row and column now – not a surprise, since we restricted to the rows and columns where we already knew that it must work!

Staring at this, we realize we can adapt the proof of Fermat's Little Theorem to this new setting: given any $a \in \mathbb{Z}_n^\times$, we can multiply all the elements in the ath row together and interpret the result in two different ways:

$$a^{|\mathbb{Z}_n^\times|} \prod_{k \in \mathbb{Z}_n^\times} k = \prod_{k \in \mathbb{Z}_n^\times} (ak) \equiv \prod_{k \in \mathbb{Z}_n^\times} k \pmod{n}$$

Canceling the product of k's from both sides, we get the following:

Euler's Theorem: $a^{|\mathbb{Z}_n^\times|} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}_n^\times$.

Example: For all $a \in \mathbb{Z}_8^\times$, $a^4 \equiv 1 \pmod{8}$.
Ben points out that this is not optimal, since $a^2 \equiv 1 \pmod{8}$ for all $a \in \mathbb{Z}_8^\times$ (see table above). We shall return to this observation in later lectures, but suffice to say that it is still an open problem to predict the optimal choice of k such that $a^k \equiv 1 \pmod{n}$ for every $a \in \mathbb{Z}_n^\times$.

Euler's theorem looks a bit clunky, because it uses $|\mathbb{Z}_n^\times|$ in the exponent. This motivates

Definition: $\varphi(n) := |\mathbb{Z}_n^\times|$. (called the "Euler totient function")

Examples: $\varphi(8) = 4$. $\varphi(5) = 4$. $\varphi(4) = 2$.

Using this function, we can rewrite Euler's Theorem:

Euler's Theorem 2.0: $a^{\varphi(n)} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}_n^\times$.

Next time we will return to study this function more carefully.