Wednesday, April 24

(Note: The final is a 24 hour take home exam. We can pick it up at any point starting the Saturday after classes end and ending the Sunday after the Sunday after classes end. However, Professor Goldmakher strongly encourages not taking the exam the first Saturday or Sunday, as he's planning a review session for Monday morning.)

Let's talk about the sudoku rule from last time!

Sudoku Rule: Given p a prime, fix any $a \in \{1, 2, \dots, p-1\}$. The a^{th} row of the multiplication table (mod p) consists of all the numbers in $\{1, 2, \dots, p-1\}$, each appearing exactly once. (The rule also covers columns, but since multiplication is commutative, if it's true for the rows, it's true for the columns.)

That's a relatively long definition of the rule. Let's tighten it up by writing it with mathematical symbols. But how? We need a way to say that any two elements of the a^{th} row are distinct. Note that every element of the a^{th} row is a times some number between 1 and $p-1$, mod p. If we want to say two elements are unique, then, we get:

$$\forall k, l \in \{1, 2, \dots, p-1\} \text{ s.t. } k \neq l,\ ak \pmod p \neq al \pmod p.$$

We don't even need to restrict k and l to being in this set! k and l can be any integers — they just have to be distinct (mod p). Thus, we can condense this further:

$$k \not\equiv l \pmod p \Rightarrow ak \not\equiv al \pmod p.$$

If this is true, every element in the a^{th} row must be distinct. However, there are $p-1$ possible elements and $p-1$ spaces, so each is used exactly once.

This means:

$$k \not\equiv l \pmod p \Rightarrow ak \not\equiv al \pmod p$$

$$\Updownarrow$$

$$\forall k, l \in \{1, 2, \dots, p-1\} \text{ s.t. } k \neq l,\ ak \pmod p \neq al \pmod p$$

$$\Updownarrow$$

The Sudoku Rule.

That one line is equivalent to the sudoku rule, and it's much faster to write! Note that that statement is equivalent to its contrapositive:

$k \not\equiv l \pmod p \Rightarrow ak \not\equiv al \pmod p \Leftrightarrow$ Given $a \not\equiv 0 \pmod p$, if $ak \equiv al \pmod p$, then $k \equiv l \pmod p$.

To prove this, it'd be rather nice to just say $ak \equiv al \pmod p \Rightarrow ak - al \equiv 0 \pmod p \Rightarrow a(k-l) \equiv 0 \pmod p$ $\Rightarrow a \equiv 0 \pmod p$ or $k - l \equiv 0 \pmod p$. How can we show that last step?

All we need to do to prove that contrapositive is show the last step in the wishful thinking cloud.

Proposition: given $a \not\equiv 0 \pmod p$, if $ak \equiv al \pmod p$, then $k \equiv l \pmod p$ $\Leftrightarrow$

Proposition: If $wq \equiv 0 \pmod p$, then $w \equiv 0 \pmod p$ or $q \equiv 0 \pmod p$.

Exercise for you: why are the previous two propositions equivalent?

Next, we observe that the latter proposition is equivalent to the following result about prime numbers:

Proposition: $p \mid wq \Rightarrow p \mid w$ or $p \mid q$.

Let's prove this! (The proof is wild!)

Proof: Suppose $p \mid wq$ but $p \nmid w$. Then $\gcd(p, w) = 1$ (since p only has 2 factors). By Bézout's theorem (which is on the homework, this means $\exists x, y \in \mathbb{Z}$ s.t. $px + wy = 1$.

Multiply both sides by q: we get

This means $pxq + wqy = q$. $p \mid pxq$ and $p \mid wqy$ (since $p \mid wq$), so $p \mid (pxq + wqy)$. Thus, $p \mid q$. $\blacksquare$

Hooray! The Sudoku rule is true!

<u>Awesome consequence of this:</u>

What's the product of all the elements appearing in the a^{th} row of the multiplication table (mod p)?

On one hand, it's $(p-1)! \pmod{p}$ since the Sudoku rule is true.

On the other hand, by definition, it's $a(2a)(3a)\ldots(p-1)a \pmod{p}$.

Thus, $(p-1)! \equiv a(2a)(3a)\ldots(p-1)a \equiv a^{p-1}(p-1)! \pmod{p}$

$\Rightarrow 1 \equiv a^{p-1} \pmod{p}$.

We've proved Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \pmod{p} \;\; \forall a \not\equiv 0 \pmod{p}.$$