Before we begin, there's a colloquium today regarding Fermat's Last Theorem.

Q: Can we find $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 = z^2$?

A: Yes! $(3, 4, 5)$, $(0, n, n)$ $(6, 8, 10)$, and $(5, 12, 13)$ all work. $(0, n, n)$ is called trivial since it contains a 0. $(3, 4, 5)$ is nontrivial and primitive since 3, 4, and 5 don't share factors greater than 1. $(6, 8, 10)$ is nontrivial and imprimitive since 6, 8, and 10 share a factor greater than 1.)

Q: Can we find $x, y, z \in \mathbb{Z}$ such that $x^n + y^n = z^n$, $n \geq 3$

A: Kind of... all we can find is $(0, n, n)$, $(n, 0, n)$, and $(n, -n, 0)$. These are all trivial. Are there any nontrivial solutions?

As it turns out, no. This was proposed by Fermat in 1650 (he said he had a proof, but it couldn't fit in the margins), and it wasn't proved until Andrew Wiles came up with a proof in 1993... that was wrong. He fixed it the following year, though!

(Note: Fermat claimed it couldn't be done for $x^n + y^n = z^n$, $n > 2$. People could prove it for individual values of n, but proving it in general was hard.)

There's something similar for functions — are there functions $f(x)$, $g(x)$, and $h(x)$ such that $f(x)^n + g(x)^n = h(x)^n$? — that is easier to prove. That's what the colloquium will cover.

Last time we looked at the mod 7 multiplication table:

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

There are a LOT of patterns in this table. What are some?

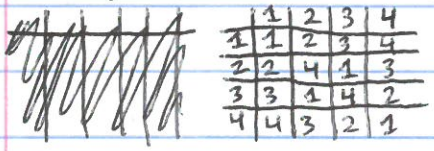
① Symmetry among the rows. For instance, the first row is the sixth row... backwards. (In general, the a^{th} row is the reverse of the $7-a^{th}$ row.)

② Every diagonal is a palindrome.

③ Each row has a symmetry: the k^{th} entry plus the $(7-k)^{th}$ entry equals 7.

④ Sudoku Rule: Each row (and each column) has all of $\{1, 2, 3, 4, 5, 6\}$ in it.

Cool! What about mod 5?



	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

All of the aforementioned patterns are here as well!

There's also a mod 11 multiplication table on the board (which I won't reproduce here for time's sake and also because my wrist is getting tired). All of the patterns are there, too! The patterns are ~~were~~ present for 5, 7, and 11. Does it work for all integers n? No! (We'll see that on the homework.) However, the above four patterns are all present in ~~the~~ multiplication tables mod a prime p. (From here on out, p denotes a prime.) We'll prove one of the first three symmetry patterns. (The other two proofs are ~~great~~ similar.)

Proof of ③ (mod p):

Want to prove $p = ak \pmod p + a(p-k) \bmod p$

Consider $ak + a(p-k) \equiv ak + ap - ak \equiv ap \pmod p \equiv 0 \pmod p$ (since $p \mid (ap - 0)$). This means $p \mid (ak + a(p-k))$. But also, $ak \pmod p + a(p-k) \pmod p \equiv ak + a(p-k) \pmod p \equiv 0 \pmod p$.

(Note that $ak \pmod p + a(p-k) \pmod p \equiv ak + a(p-k) \pmod p$ because we're just changing where we remove the ps.)
Therefore, $p \mid (ak \pmod p + a(p-k) \bmod p)$. However, $ak \pmod p$ and $a(p-k) \pmod p$ appear in the multiplication table. Thus, $ak \pmod p, a(p-k) \pmod p \in \{1, 2, \ldots, p-1\}$, so $ak \pmod p + a(p-k) \pmod p \in \{2, \ldots, 2p-2\}$. ▨
(Think about it... why can we end the proof here?)