Recall that our method of solving power congruences failed for quadratic congruences, i.e. congruences of the form $x^2 \equiv a \pmod{n}$. How do we solve such a congruence? It turns out that no one knows an efficient way to accomplish this for a general n.[1] Following Pólya's dictum – *If you can't solve a problem, find an easier version of the problem that you* can *solve* – we turn to a more basic question:

Question: Given $a \pmod{p}$, can we efficiently predict whether or not the congruence $x^2 \equiv a \pmod{p}$ has a solution? Or equivalently: given p, can we predict the perfect squares are modulo p?

For example, what are the perfect squares modulo 7? Apart from the trivial 0, we have $1^2 = 1$, $2^2 = 4$, and $3^2 \equiv 2$. Note that we won't get any other squares, since $4^2 \equiv (-3)^2 = 3^2$, etc. Thus modulo 7 we have:
Perfect Squares: 1, 2, 4
Non-squares: 3, 5, 6

Modulo 11:
Perfect Squares: 1, 3, 4, 5, 9
Non-squares: 2, 6, 7, 8, 10

Modulo 13:
Perfect Squares: 1, 3, 4, 9, 10, 12
Non-squares: 2, 5, 6, 7, 8, 11

Jacob's Question: Are there as many (nonzero) squares as non-squares? This inspired

Conjecture (Akhil): There are exactly $\frac{p-1}{2}$ perfect squares and $\frac{p-1}{2}$ non-squares for $p \geq 3$.
Jeff: It's enough to show that if $a^2 \equiv b^2 \pmod{p}$ then $a \equiv \pm b \pmod{p}$, since then all the squares $\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$ consists of distinct numbers $\pmod{p}$.

Proposition: If $a^2 \equiv b^2 \pmod{p}$ then $a \equiv \pm b \pmod{p}$.
Proof: Since $a^2 \equiv b^2 \pmod{p}$, then $p \mid a^2 - b^2 = (a+b)(a-b)$. So either $p \mid a+b$ or $p \mid a-b$, whence $a \equiv \pm b \pmod{p}$. □

Thus,

$$\left|\left\{a \in \mathbb{Z}_p^\times : a \equiv x^2 \pmod{p}, x \neq 0\right\}\right| = \left|\left\{1^2, 2^2, \ldots, \left(\tfrac{p-1}{2}\right)^2 \pmod{p}\right\}\right| = \tfrac{p-1}{2}$$

since each square in the set is distinct. As a result, all the other elements are non-squares, so there are $\frac{p-1}{2}$ of them. This proves Akhil's Conjecture.

[1] The *Tonelli-Shanks algorithm* gives a way to efficiently solve quadratic congruences modulo a prime power. However, solving a quadratic congruence (mod pq) is equivalent to factoring pq, a fact that's at the heart of the Rabin cryptosystem.

We've thus found our way into the problem of quadratic congruences: we've successfully solved the problem of counting the number of squares (mod p). Next we tackle the harder question: given $a \in \mathbb{Z}_p^\times$, is a a perfect square (mod p)? Suppose $a \equiv x^2 \pmod{p}$. Konnor suggested raising both sides to the $p-1$, which yields $1 \equiv 1 \pmod{p}$; true but not particularly illuminating. However, this inspired Jacob to suggest raising to $\frac{p-1}{2}$, which gives us:

Lemma: If a is a square (mod p), then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Could this happen if a is not a perfect square? Note that if the converse of the Lemma is true, then this would produce a nice test for whether a given $a \in \mathbb{Z}_p^\times$ is a perfect square (mod p): simply compute $a^{\frac{p-1}{2}} \pmod{p}$. Miranda points out that since $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$, we must have $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ no matter what a is.

Example: modulo 11
Consider the non-squares from mod 11 from before. Here $(p-1)/2 = 5$.
$2^5 \equiv -1 \pmod{11}$
$6^5 = 2^5 \cdot 3^5 \equiv -1 \pmod{11}$ because 3 is a perfect square, so $3^5 \equiv 1$.
$8^5 = (2^3)^5 = (2^5)^3 \equiv (-1)^3 \equiv -1 \pmod{11}$.

Theorem: If a is not a perfect square (mod p), then $a^{(p-1)/2} \equiv -1 \pmod{p}$.
Proof: Note that every $a \in \mathbb{Z}_p^\times$ is a root of the polynomial $x^{p-1} - 1 \equiv 0 \pmod{p}$. Thus, $x^{p-1} - 1$ has exactly $p-1$ roots $\pmod{p}$. Consider the factorization of this polynomial:

$$x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right).$$

Notice that each of the polynomials $\left(x^{\frac{p-1}{2}} \pm 1\right)$ has *at most* $\frac{p-1}{2}$ roots (mod p) by problem **6.4**. But together they have *exactly* $p-1$ roots $\pmod{p}$. Thus we conclude that each of $\left(x^{\frac{p-1}{2}} \pm 1\right)$ must have precisely $\frac{p-1}{2}$ roots $\pmod{p}$. We know that the perfect squares, of which there are $\frac{p-1}{2}$, are a set of solutions of $x^{\frac{p-1}{2}} - 1 \pmod{p}$. Thus all other elements of $\mathbb{Z}_p^\times$, i.e. the non-squares, must be roots of $x^{\frac{p-1}{2}} + 1 \pmod{p}$. But this means that $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$ whenever $a \in \mathbb{Z}_p^\times$ isn't a perfect square (mod p), which proves the theorem. □

This result motivates the following
Definition: (the Legendre symbol) Given $a \in \mathbb{Z}$, we set

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & \text{if } a \equiv \square \pmod{p} \text{ and } a \not\equiv 0 \pmod{p} \\ -1 & \text{if } a \not\equiv \square \pmod{p} \\ 0 & a \equiv 0 \pmod{p} \end{cases}$$

The symbol $\left(\frac{a}{p}\right)$ is pronounced "a on p".

Examples:

$$\left(\frac{2}{7}\right) = 1 \qquad \left(\frac{10}{7}\right) = -1 \qquad \left(\frac{-14}{7}\right) = 0$$

As Jeff observed, immediately from our work above we deduce
Proposition (Euler's Criterion):

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Properties of the Legendre Symbol:

(1) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) The function $\left(\frac{\cdot}{p}\right)$ is completely multiplicative, i.e. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ $\forall a, b \in \mathbb{Z}$.

Property (1) is easy to prove, and is left as an exercise. Property (2) is deceptively simple-looking. In some cases it's trivial: if both a and b are perfect squares (mod p), then it's not hard to see that ab must also be a perfect square (mod p). But property (2) also implies a much weirder fact: that if *neither* a nor b are perfect squares (mod p), then ab *must* be a perfect square (mod p). This is not at all obvious, but follows immediately from property (2). This demonstrates that there's really something non-trivial about this property of the Legendre symbol. We prove this property now. Note that the proof looks easy, but this is only because it builds on our previous work!

Proof of 2 (Miranda): By Euler's Criterion,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

Thus $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}$, but this isn't quite what we want – we claim actual equality of the two quantities. Fortunately, this isn't hard to deduce: since $-1 \le \left(\frac{\cdot}{p}\right) \le 1$, we see that $\left|\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \pmod{p}\right| \le 2$. But also, we just proved that $p \mid \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \pmod{p}$. We're assuming that $p \ge 3$, so the only multiple of p between -2 and 2 is 0. □

We concluded with a nice application of Euler's criterion. Is -1 a perfect square (mod p)?

Proposition: Given any $p \ge 3$, we have

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv -1 \pmod{4} \end{cases}$$

Thus, for example, -1 is a perfect square (mod 17) but isn't a perfect square (mod 19).