Last time we introduced the Legendre symbol, $\left(\frac{a}{p}\right)$:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \equiv x^2 \pmod{p}, a \not\equiv 0 \pmod{p} \\ -1 & \text{if } a \not\equiv x^2 \pmod{p} \\ 0 & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

We used this to prove:
Thm (Euler's Criterion): For all $a \in \mathbb{Z}$, $p \geq 3$, we have that $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Euler's criterion has some nice consequences. For example, it allows us to quickly and easily deduce whether or not -1 is a perfect square (mod p):

Corollary: $\left(\dfrac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv -1 \pmod{4}. \end{cases}$

Thus, for example, -1 is not a perfect square (mod 19).

We also used Euler's criterion to prove some nice properties of the Legendre symbol:
Proposition: Given an odd prime p and any $a, b \in \mathbb{Z}$, we have:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (i.e. the Legendre symbol is *completely multiplicative*, and
- $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (i.e. the Legendre symbol is periodic with period p).

In combination, the above tools are quite powerful and allow us to compute the Legendre symbol in many circumstances. Let's look at a few examples.

1) $\left(\frac{9}{17}\right) =?$ This one's easy: since $9 = 3^2$ in $\mathbb{Z}$, we must have $9 \equiv 3^2 \pmod{17}$.

2) $\left(\frac{13}{17}\right) =?$
Alex: By Euler's criterion, we have $\left(\frac{13}{17}\right) \equiv 13^8 = (13^2)^4 \equiv (-1)^4 = 1 \pmod{17}$.
Oliver: $\left(\frac{13}{17}\right) \equiv \left(\frac{-4}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{4}{17}\right) = 1 \cdot 1 = 1$, since $17 \equiv 1 \pmod{4}$.
Jacob: $\left(\frac{13}{17}\right) = \left(\frac{30}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right)\left(\frac{5}{17}\right)$ and use Euler's criterion for each.

3) $\left(\frac{40}{71}\right) =?$ Ben: $\left(\frac{40}{71}\right) = \left(\frac{4}{71}\right)\left(\frac{10}{71}\right) = \left(\frac{10}{71}\right) = \left(\frac{81}{71}\right) = \left(\frac{9^2}{71}\right) = 1$.

4) $\left(\frac{41}{71}\right) =?$ $\left(\frac{40}{71}\right) = \left(\frac{-30}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{30}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{10}{71}\right)\left(\frac{3}{71}\right) = -\left(\frac{3}{71}\right)$

Note that in many cases we reduced the calculation of $\left(\frac{n}{p}\right)$ to computing $\left(\frac{q}{p}\right)$ with q a small prime. More generally, by the complete multiplicativity of the Legendre symbol, to figure out

$\left(\frac{n}{p}\right)$ it suffices to know the values of $\left(\frac{q}{p}\right)$ for all primes q. Mathematicians started by working this out in cases, e.g. they discovered the nice formula $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, then another formula for $\left(\frac{3}{p}\right)$, then another formula for $\left(\frac{5}{p}\right)$, etc. The problem was, all these formulas looked pretty different from one another, so it wasn't clear what the formula for the general $\left(\frac{q}{p}\right)$ might be. Then Euler and Legendre (independently) tackled the problem. They realized that even though there's no clear formula for computing $\left(\frac{q}{p}\right)$, there *is* a beautiful formula connecting $\left(\frac{q}{p}\right)$ to $\left(\frac{p}{q}\right)$:

Law of Quadratic Reciprocity: For all odd primes p and q,

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

Despite conjecturing it, neither Euler nor Legendre were able to prove this, which should give you a sense of just how hard the proof must be. After considerable effort, Gauss (at the ripe old age of 19) was able to prove Quadratic Reciprocity. It became one of his favorite theorems, and he returned to it many times, giving 7 additional proofs of QR. These days there are hundreds of different proofs, although some are more different than others.

We will defer the proof of QR to next class, and instead will focus on applications of QR. Let's return to an earlier example, in which we reduced the problem to finding $\left(\frac{3}{71}\right)$. We use QR to accomplish this. First observe that QR gives

$$\left(\frac{3}{71}\right)\left(\frac{71}{3}\right) = (-1)^{1\cdot 35} = -1.$$

Multiplying both sides by $\left(\frac{71}{3}\right)$ yields

$$\left(\frac{3}{71}\right) = (-1)\left(\frac{71}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

Thus, QR allowed us to recast the problem of figuring out whether 3 is a perfect square (mod 71) into the problem of whether 71 is a perfect square (mod 3) – a vastly easier problem to solve!

Of course, this worked so well because 3 is small. What if the original Legendre symbol had two primes, neither of which was particularly small? The key observation is that, using similar manipulations to the ones we came up with earlier this class, we can always rewrite the Legendre symbol in terms of small primes. For example, what is $\left(\frac{71}{151}\right)$? We first manipulate the symbol to involve small primes:

$$\left(\frac{71}{151}\right) = \left(\frac{-80}{151}\right) = \left(\frac{-1}{151}\right)\left(\frac{16}{151}\right)\left(\frac{5}{151}\right) = -\left(\frac{5}{151}\right)$$

Now we have a small prime (5), so QR becomes effective: we have

$$\left(\frac{5}{151}\right)\left(\frac{151}{5}\right) = (-1)^{2\cdot(\text{doesn't matter})} = 1 \qquad \Longrightarrow \qquad \left(\frac{5}{151}\right) = \left(\frac{151}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Putting this all together, we've shown that $\left(\frac{71}{151}\right) = -1$, or in other words, that 71 isn't a perfect square (mod 151).

The above examples should convince you that Quadratic Reciprocity is awesome. But going back to the statement, there's one clear weakness: it only applies to *odd* primes. What if we need to figure out $\left(\frac{2}{p}\right)$? For example, what is $\left(\frac{2}{71}\right)$? It turns out that there's a trick for making QR apply to this as well: we have

$$\left(\frac{2}{71}\right) = \left(\frac{-69}{71}\right)$$

and since 69 is odd we can use our usual tricks and QR to figure this out. More generally, given any odd prime p, we have

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p-2}{p}\right)$$

and since $p-2$ is odd we can apply QR to the compute the right hand side.

Having convinced ourselves with the utility of QR, we turn to its proof. As mentioned earlier, there are now hundreds of proofs available. We'll follow a proof that seems to have been originally discovered by George Rousseau in 1991, and then independently rediscovered by Dmitriy (Tim) Kunisky – then a high-schooler! – in 2008. Although neither the simplest nor the shortest proof, it is by far the easiest-to-remember proof that I have encountered.

For the rest of today we'll set up and a discuss one important (and familiar!) ingredient:

<u>Chinese Remainder Theorem v1:</u> Given $(m, n) = 1$. For any $a, b \in \mathbb{Z}$, there exists a unique $x \in \mathbb{Z}_{mn}$ such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

The name comes from the statement's historic roots in an ancient (3rd-century) text *Sunzi Suanjing*, but the theorem wasn't formally proved until centuries later. The Chinese Remainder Theorem turns out to be of practical importance, with applications to radar (send out pulses of different frequencies, so that if two pulses return simultaneously you can use the CRT to decompose the frequency into the two original frequencies) as well as to parallel computing (to perform a complicated computation, run it (mod p_1) on one processor, run it (mod p_2) on another processor, etc.; then use the CRT to reassemble the results into an output of the original computation).

Needless to say, the statement looks extremely familiar! Indeed, we've previously proved the following version of it:

Chinese Remainder Theorem v2: Given $(m,n)=1$. The function $\beta:\mathbb{Z}_{mn}^\times\to\mathbb{Z}_m^\times\times\mathbb{Z}_n^\times$ given by $x\mapsto\big(x \pmod m, x \pmod n\big)$ is a bijection. Moreover, β is completely multiplicative, i.e. $\beta(xy)=\beta(x)\beta(y)$ for any $x,y\in\mathbb{Z}_{mn}^\times$.

For the last part of this to make sense, we need to define how to multiply two elements of $\mathbb{Z}_m^\times\times\mathbb{Z}_n^\times$. Fortunately, it's exactly what you might guess:

$$(x,y)\cdot(z,w):=(xz,yw),$$

where we're implicitly modding the first coordinate out so that it lives in $\mathbb{Z}_m^\times$ and mod the second coordinate out so that it lives in $\mathbb{Z}_n^\times$.

Notice both versions can be extended to m,n,ℓ which are pairwise coprime, or even $n_1,n_2,\ldots,n_k$, all pairwise coprime. In fact, there are even versions where m and n aren't coprime! However, we won't need any of these for our proof of QR: we'll simply use v2, which we've proved previously.

The idea of the proof of QR.

Given two distinct odd primes p and q. By the Chinese Remainder Theorem, we have a one-to-one correspondence between the elements of $\mathbb{Z}_{pq}^\times$ and the elements of $\mathbb{Z}_p^\times\times\mathbb{Z}_q^\times$:

$$\mathbb{Z}_{pq}^\times \quad\longleftrightarrow\quad \mathbb{Z}_p^\times\times\mathbb{Z}_q^\times.$$

Thus we expect

$$(\text{Half of } \mathbb{Z}_{pq}^\times) \quad\longleftrightarrow\quad (\text{Half of } \mathbb{Z}_p^\times\times\mathbb{Z}_q^\times).$$

Multiplying all the elements in the half on left, we expect the outcome to correspond to whatever we get when we multiply all the elements in the half on the right. Making this precise and doing some modular arithmetic magically produces the statement of QR!

Of course we have to define precisely what we mean by half of each set. Fortunately, any way you choose to define these will work. Here are the ways we came up with in class:

$$L=(\text{Half of } \mathbb{Z}_{pq}^\times):=\{n\in\mathbb{Z}_{pq}^\times : n<\tfrac{pq}{2}\}$$
$$R=(\text{Half of } \mathbb{Z}_p^\times\times\mathbb{Z}_q^\times):=\{(a,b)\in\mathbb{Z}_p^\times\times\mathbb{Z}_q^\times : b<\tfrac{q}{2}\}$$

In terms of this, we can express the expected one-to-one correspondence between the halves in a precise way:

Claim: For any $(a,b)\in R$, there exists a unique $k\in L$ such that $\beta(k)=\pm(a,b)$.

From here, the proof of QR is conceptually simple: from the claim we immediately obtain

$$\prod_{k\in L}\beta(k)=\prod_{(a,b)\in R}\pm(a,b)=\pm\prod_{(a,b)\in R}(a,b)$$

We then do a bunch of modular arithmetic to evaluate both sides; this gives us two congruences (one (mod m) from the first coordinate, and the other (mod n) from the second coordinate). Combining these two congruences will produce QR. Stay tuned for the details!