Today we will prove the law of quadratic reciprocity. Recall its statement:
Law of Quadratic Reciprocity: Given any distinct odd primes p and q,

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

There are 200⁺ proofs, but this is the most conceptually simple, albeit computational.
Proof of QR (by George Rousseau '91 and Tim Kunisky '08):
Recall from last time that we set

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

The Chinese Remainder Theorem gives a bijection between $\mathbb{Z}_{pq}^\times$ and $\mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$, so we expect it to give a bijection between L and R as well. Of course, this might not be literally true: perhaps the bijection β given by the CRT matches up L with some way to view half of $\mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$ that's quite different from the set R. As it turns out, β behaves very nicely (see Step 1). Here's the broad outline of our proof of QR:
Step 1: For any $(a,b) \in R$, there exists a unique $k \in L$ such that $\beta(k) = \pm(a,b)$. From this, it immediately follows that

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

Step 2: Evaluate $\prod_{k\in L} \beta(k) = \prod_{k\in L} (k \pmod p, k \pmod q) = \left(\prod_{k\in L} k \pmod p, \prod_{k\in L} k \pmod q\right)$.

Step 3: Evaluate $\prod_{(a,b)\in R} (a,b)$.

Step 4: Compare the results from Steps 2 and 3 and win.

Actual proof:
Step 1: On homework.
Step 2: We saw $\prod_{k\in L} \beta(k) = \left(\prod_{k\in L} k \pmod p, \prod_{k\in L} \pmod q\right)$. We start by working out the first coordinate:

$$\prod_{\substack{k\in\mathbb{Z}_{pq}^\times \\ k<pq/2}} k \equiv \frac{\text{prod of all } k < \frac{pq}{2} \text{ s.t. } k \not\equiv 0 \pmod p}{\text{prod of all } k < \frac{pq}{2} \text{ s.t. } k \equiv 0 \pmod q} \equiv \frac{\Big(1\cdot 2\cdot 3\cdots(p-1)\Big)\Big((p+1)(p+2)\cdots(2p-1)\Big)\cdots}{(q)(2q)(3q)\cdots(\frac{p-1}{2}q)}$$

$$\equiv \frac{\left(\prod_{0<k<p} k\right)\left(\prod_{p<k<2p} k\right)\cdots\left(\prod_{\frac{q-3}{2}p<k<\frac{q-1}{2}p} k\right)\left(\prod_{\frac{q-1}{2}p<k\le\frac{pq-1}{2}} k\right)}{q^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!} \equiv \frac{(p-1)!\cdots(p-1)!\left(\frac{p-1}{2}\right)!}{q^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!} \pmod p$$

Recall from problem **4.3** that $(p-1)! \equiv -1 \pmod{p}$; this is called "Wilson's Theorem". Continuing our calculation from above:

$$\prod_{\substack{k\in\mathbb{Z}_{pq}^\times \\ k<pq/2}} k \equiv \frac{(-1)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} = \frac{(-1)^{\frac{q-1}{2}}}{\left(\frac{q}{p}\right)} = (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$$

The final step is justified because $\left(\frac{q}{p}\right) = \pm 1$, so dividing by it is the same as multiplying.

Note that we've made no assumptions that distinguish p from q, which means that the above result must also hold if we exchange the values of p and q. In other words:

$$\prod_{\substack{k\in\mathbb{Z}_{pq}^\times \\ k<pq/2}} k \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}$$

We've thus found relatively expressions for both the first and second coordinates of $\prod_{k\in L} \beta(k)$. This completes Step 2!

<ins>Step 3:</ins> We have

$$\begin{aligned}
\prod_{(a,b)\in R} (a,b) = \prod_{\substack{a\in\mathbb{Z}_p^\times \\ b\in\mathbb{Z}_q^\times \\ b<q/2}} (a,b) = \prod_{a\in\mathbb{Z}_p^\times} \prod_{\substack{b\in\mathbb{Z}_q^\times \\ b<q/2}} (a,b) &= \prod_{a\in\mathbb{Z}_p^\times} \Big((a,1)(a,2)\cdots(a,\tfrac{q-1}{2})\Big) \\
&= \prod_{a\in\mathbb{Z}_p^\times} \Big(a^{(q-1)/2}, \big(\tfrac{q-1}{2}\big)!\Big) = \Big(\big((p-1)!\big)^{(q-1)/2}, \big(\big(\tfrac{q-1}{2}\big)!\big)^{p-1}\Big) \\
&= \Big((-1)^{(q-1)/2}, \big(\big(\tfrac{q-1}{2}\big)!\big)^{p-1}\Big).
\end{aligned}$$

Recall that the first coordinate is $\pmod{p}$ and the second is $\pmod{q}$. The first coordinate is pretty straightforward; can we simplify the second? We know by Wilson's theorem that $(q-1)! \equiv -1 \pmod{q}$, but what is $\left(\frac{q-1}{2}\right)! \pmod{q}$?

$$\begin{aligned}
\big(\tfrac{q-1}{2}\big)! &= 1\cdot 2\cdot\dots\cdot \tfrac{q-1}{2} \\
(q-1)! &= 1\cdot 2\cdot\dots\cdot \tfrac{q-1}{2}\cdot\tfrac{q+1}{2}\cdot\dots\cdot(q-2)(q-1) \\
&\equiv 1\cdot 2\cdot\dots\cdot \tfrac{q-1}{2}\cdot\big(-\tfrac{q-1}{2}\big)\cdot\dots\cdot(-2)(-1) \pmod{q} \\
&\equiv (-1)^{(q-1)/2}\big(\big(\tfrac{q-1}{2}\big)!\big)^2 \pmod{q} \\
\implies \qquad \big(\big(\tfrac{q-1}{2}\big)!\big)^2 &\equiv (-1)^{(q-1)/2}(q-1)! \equiv -(-1)^{(q-1)/2} \pmod{q}
\end{aligned}$$

Continuing where we'd left off earlier, we find

$$\prod_{(a,b)\in R} (a,b) = \Big((-1)^{(q-1)/2}, \big(\big(\tfrac{q-1}{2}\big)!\big)^{2\cdot(p-1)/2} \pmod{q}\Big) = \Big((-1)^{(q-1)/2}, (-1)^{(p-1)/2}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\Big).$$

Both coordinates are pretty straightforward; we've finished Step 3!

Step 4: Putting together all our work, we've proved

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

where $\varepsilon = \pm 1$. Comparing first and second coordinates separately,

$$(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \equiv \varepsilon(-1)^{\frac{q-1}{2}} \pmod p \implies \varepsilon \equiv \left(\frac{q}{p}\right) \pmod p \implies \varepsilon = \left(\frac{q}{p}\right)$$
$$(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \equiv \varepsilon\,(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod q \implies \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod q.$$

Multiplying both sides by $\left(\frac{q}{p}\right)$ yields

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

as claimed. Q.E.F.D.