Math 445 Number Theory

October 8, 2004

Recap: we know that the *Legendre symbol*, for p an odd prime and $(a,p)=1$, satisfies $\left(\frac{a}{p}\right) = (-1)^n$, where $n = |A|$ = the number of elements in A, where $A = \{k : a_k > \frac{p}{2}\}$, where $ak = pt_k + a_k$ with $0 \le a_k \le p-1$. We have also seen that if a is *odd* and $(a,p)=1$, then $\left(\frac{a}{p}\right) = (-1)^t$, where $t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{aj}{p} \rfloor$. Along the way we learned that

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p(t-n) + 2\sum_{i=1}^{n} q_i \quad \text{and} \quad \sum_{j=1}^{\frac{p-1}{2}} j = \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right) = \frac{p^2-1}{8}$$

When $a=2$, this last equation tells us that, mod 2, $\frac{p^2-1}{8} \equiv p(t-n) \equiv (t-n)$. But in this case $t=0$, since each of $\lfloor \frac{aj}{p} \rfloor = \lfloor \frac{2j}{p} \rfloor = 0$, since $2j < p$ for $1 \le j \le \frac{p-1}{2}$. So $\frac{p^2-1}{8} \equiv -n \equiv n \pmod 2$, so

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$$

Finally, we have the means to prove *Gauss' Law of Quadratic Reciprocity:*

Theorem: If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$.

This is because $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{t_1}(-1)^{t_2} = (-1)^{t_1+t_2}$, where

$$t_1 = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \tfrac{qi}{p} \rfloor \text{ and } t_2 = \sum_{j=1}^{\frac{q-1}{2}} \lfloor \tfrac{pj}{q} \rfloor .$$

But for every pair (i,j), with $1 \le i \le \frac{p-1}{2}$ and $1 \le j \le \frac{q-1}{2}$, exactly one of $qi > pj$ or $qi < pj$ is true. So $S_1 = \{(i,j) : qi > pj\}$ and $S_2 = \{(i,j) : qi < pj\}$ are disjoint sets whose union is the set of all pairs. So $|S_1| + |S_2| = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$. But for each fixed i, the j's with $(i,j) \in S_1$ are those which satisfy $j < \frac{qi}{p}$, so there are $\lfloor \frac{qi}{p} \rfloor$ of them, so S_1 has $\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{qi}{p} \rfloor = t_1$ elements. Similarly, for each fixed j, the i's with $(i,j) \in S_2$ are those which satisfy $i < \frac{pj}{q}$, so there are $\lfloor \frac{pj}{q} \rfloor$ of them, so S_2 has $\sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor = t_2$ elements. Consequently, $t_1 + t_2 = |S_1| + |S_2| = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$, as desired.

These facts,
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$ if p,q distinct odd primes, $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$, and $\left(\frac{-1}{p}\right) = (-1)^n = (-1)^{\frac{p-1}{2}}$
allow us to carry out the calculations of Legendre symbols much more simply than Euler's criterion would! For example

$\left(\frac{17}{31}\right)\left(\frac{31}{17}\right) = (-1)^{\left(\frac{17-1}{2}\right)\left(\frac{31-1}{2}\right)} = (-1)^{8\cdot 15} = 1$, so $\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right)$. But $\left(\frac{31}{17}\right) = \left(\frac{2\cdot 17-3}{17}\right) = \left(\frac{-3}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{3}{17}\right) = (-1)^8\left(\frac{3}{17}\right) = \left(\frac{3}{17}\right)$, while $\left(\frac{3}{17}\right)\left(\frac{17}{3}\right) = (-1)^{8\cdot 1} = 1$, so $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{3\cdot 6-1}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^1 = -1$, so $\left(\frac{17}{31}\right) = -1$, and so the equation $x^2 \equiv 17 \pmod{31}$ has no solutions.