# Math 445 Number Theory

October 6, 2004

The *Legendre symbol*; for $p$ an odd prime,

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases}$$

By Euler's criterion, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

*Lemma of Gauss:* Let $p$ be an odd prime and $(a,p)=1$. For $1 \le k \le \frac{p-1}{2}$ let $ak = pt_k + a_k$ with $0 \le a_k \le p-1$ . Let $A = \{k : a_k > \frac{p}{2}\}$ , and let $n = |A|$ = the number of elements in $A$ . Then $\left(\frac{a}{p}\right) = (-1)^n$ .

To see this, first note that $a_k \neq 0$ for every $k$, since $p \not| ak$ . Let $q_1, \dots, q_n$ be the $a_k$'s greater then $p/2$, and let $r_1, \dots, r_m$ be the other $a_k$'s. Then $p-q_1, \dots, p-q_n, r_1 \dots, r_m$ are all $\le \frac{p-1}{2}$, and are all *distinct*; $q_i = q_j$ or $r_i = r_j$ implies $p|ak_i - ak_j$, so $p|k_i - k_j$, contradicting that $-\frac{p}{2} < k_i - k_j < \frac{p}{2}$, and $p - q_i = r_j$ implies $p = q_i + r_j$ so $p|ak_i + ak_j$, contradicting that $0 < k_i + k_j \le p-1$ . This means that the sequence $p-q_1, \dots, p-q_n, r_1 \dots, r_m$ is identical to $1, 2, \dots, \frac{p-1}{2}$, just written in a different order. But then

$$(p-q_1)\cdots(p-q_n)r_1\cdots r_m = \left(\tfrac{p-1}{2}\right)!$$

But, mod $p$, $(p-q_1)\cdots(p-q_n)r_1\cdots r_m \equiv (-q_1)\cdots(-q_n)r_1\cdots r_m = (-1)^n q_1\cdots q_n r_1 \cdots r_m \equiv (-1)^n (a\cdot 1)(a\cdot 2)\cdots(a\cdot\frac{p-1}{2})$, since the $q_i$'s and $r_i$'s are together a reordering of the $a_k$, each of which is $\equiv ak$. So

$$\left(\tfrac{p-1}{2}\right)! \equiv (-1)^n a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)!$$

and since $(p, (\frac{p-1}{2})!) = 1$, we have, mod $p$, $1 \equiv (-1)^n a^{\frac{p-1}{2}}$, so $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n$ . But since $p$ is an odd prime, $p \ge 3$, and since each of the two terms above are $\pm 1$, this implies $\left(\frac{a}{p}\right) = (-1)^n$ , as desired.

*Theorem:* Let $p$ be an odd prime and $(a, 2p) = 1$ (i.e., $(a,p)=1$ and $a$ is odd). Let $t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{aj}{p} \rfloor$ . Then $\left(\frac{a}{p}\right) = (-1)^t$ .

To see this, we write $aj = pt_j + a_j$ as in the lemma above. Then $\lfloor \frac{aj}{p} \rfloor = t_j$ and so $t = \sum_{j=1}^{\frac{p-1}{2}} t_j$ . But (*) $a\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} aj = \sum_{j=1}^{\frac{p-1}{2}} pt_j + a_j = p\sum_{j=1}^{\frac{p-1}{2}} t_j + \sum_{i=1}^{n} q_i + \sum_{i=1}^{m} r_i = pt + \sum_{i=1}^{n} q_i + \sum_{i=1}^{m} r_i$ , using the notation of the lemma. But since, as in the lemma, $p-q_1, \dots, p-q_n, r_1 \dots, r_m$ is a reordering of $1, \dots, \frac{p-1}{2}$, we have

(**) $\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n}(p-q_i) + \sum_{i=1}^{m} r_i = pn - \sum_{i=1}^{n} q_i + \sum_{i=1}^{m} r_i$ . Subtracting (**) from (*), we get:

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p(t-n) + 2\sum_{i=1}^{n} q_i$$

Consequently, since, mod 2, $a - 1 \equiv 0$ ($a$ is odd) and $2\sum_{i=1}^{n} q_i \equiv 0$, we have $2|p(t-n)$, and so since $p$ is odd, $2|t-n$ . So $(-1)^t = (-1)^n$ ; together with the lemma above, this gives our result.

For next time, it is worth noting that $\sum_{j=1}^{\frac{p-1}{2}} j = \frac{1}{2}(\frac{p-1}{2})(\frac{p-1}{2}+1) = \frac{p^2-1}{8}$ .