Math 445 Number Theory

October 20, 2004

For Q odd and $(A,Q)=1$, if $Q=q_1\cdots q_k$ is the prime factorization of Q, then the *Jacobi symbol* $\left(\frac{A}{Q}\right)$ is defined to be $\left(\frac{A}{Q}\right)=\left(\frac{A}{q_1}\right)\cdots\left(\frac{A}{q_k}\right)$.

The use of the same notation as for Legendre symbols should cause no confusion, and is in fact deliberate; if Q is prime, then both symbols are equal to one another. Straight from the definition, some basic properties:

If $(A,Q)=1=(B,Q)$ then $\left(\frac{AB}{Q}\right)=\left(\frac{A}{Q}\right)\left(\frac{B}{Q}\right)$

If $(A,Q)=1=(A,Q')$ then $\left(\frac{A}{QQ'}\right)=\left(\frac{A}{Q}\right)\left(\frac{A}{Q'}\right)$

If $(PP',QQ')=1$ then $\left(\frac{P'P^2}{Q'Q^2}\right)=\left(\frac{P'}{Q'}\right)$

Warning! If Q is not prime, then $\left(\frac{A}{Q}\right)=1$ does *not* mean that $x^2\equiv A \pmod Q$ has a solution. For example, $\left(\frac{2}{9}\right)=(\left(\frac{2}{3}\right))^2=1$, but $x^2\equiv 2 \pmod 9$ has no solution, because $x^2\equiv 2 \pmod 3$ has none. But $\left(\frac{A}{Q}\right)=-1$ does mean that $x^2\equiv A \pmod Q$ has *no* solution, because $\left(\frac{A}{Q}\right)=-1$ implies $\left(\frac{A}{q_i}\right)=-1$ for some prime factor of Q, so $x^2\equiv A \pmod{q_i}$ has no solution.

Some less basic properties:

If Q is odd, then $\left(\frac{-1}{Q}\right)=(-1)^{\frac{Q-1}{2}}$: If $Q=q_1\cdots q_k$ is the prime factorization, then $\left(\frac{-1}{Q}\right)=\left(\frac{-1}{q_1}\right)\cdots\left(\frac{-1}{q_k}\right)=(-1)^{\frac{q_1-1}{2}}\cdots(-1)^{\frac{q_k-1}{2}}=(-1)^{\sum_{i=1}^k\frac{q_i-1}{2}}$, and this equals$(-1)^{\frac{Q-1}{2}}$, provided, mod 2, $\sum_{i=1}^k\frac{q_i-1}{2}\equiv\frac{Q-1}{2}=\frac{q_1\cdots q_k-1}{2}$. This in turn can be established by induction; the inductive step is

$\frac{q_1\cdots q_kq_{k+1}-1}{2}=(q_{k+1}-1)\frac{q_1\cdots q_k-1}{2}+\frac{q_1\cdots q_k-1}{2}+\frac{q_{k+1}-1}{2}\equiv(q_{k+1}-1)\frac{q_1\cdots q_k-1}{2}+\frac{q_{k+1}-1}{2}+\sum_{i=1}^k\frac{q_i-1}{2}\equiv(q_{k+1}-1)\frac{q_1\cdots q_k-1}{2}+\sum_{i=1}^{k+1}\frac{q_i-1}{2}\equiv\sum_{i=1}^{k+1}\frac{q_i-1}{2}$, since Q is odd, so $q_{k+1}-1$ is even.

If Q is odd, then $\left(\frac{2}{Q}\right)=(-1)^{\frac{Q^2-1}{8}}$: as before, $\left(\frac{2}{Q}\right)=\left(\frac{2}{q_1}\right)\cdots\left(\frac{2}{q_k}\right)$

$=(-1)^{\frac{q_1^2-1}{8}}\cdots(-1)^{\frac{q_k^2-1}{8}}=(-1)^{\sum_{i=1}^k\frac{q_i^2-1}{8}}$ and this equals$(-1)^{\frac{Q^2-1}{8}}$, provided, mod 2, $\sum_{i=1}^k\frac{q_i^2-1}{8}\equiv\frac{Q^2-1}{8}=\frac{q_1^2\cdots q_k^2-1}{8}$, i.e., mod 16, $\sum_{i=1}^k(q_i^2-1)\equiv\frac{Q^2-1}{8}=\frac{q_1^2\cdots q_k^2-1}{8}$. This can also be established by induction; the inductive step is

$q_1^2\cdots q_{k+1}^2-1=q_{k+1}^2q_1^2\cdots q_k^2-1=(q_{k+1}^2-1)(q_1^2\cdots q_k^2-1)+(q_1^2\cdots q_k^2-1)+(q_{k+1}^2-1)\equiv(q_{k+1}^2-1)+(q_1^2\cdots q_k^2-1)\equiv(q_{k+1}^2-1)+\sum_{i=1}^k(q_i^2-1)=\sum_{i=1}^{k+1}(q_i^2-1)$, since both (q_{k+1}^2-1) and $(q_1^2\cdots q_k^2-1)$ are multiples of 8, so $(q_{k+1}^2-1)(q_1^2\cdots q_k^2-1)$ is divisible by 64, hence by 16.

Finally, if P and Q are both odd, and $(P,Q)=1$, then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{(\frac{P-1}{2})(\frac{Q-1}{2})}$: if $P=p_1\cdots p_r$ and $Q=q_1\cdots q_s$ are their prime factorizations, then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=\left(\frac{p_1\cdots p_r}{Q}\right)\left(\frac{Q}{p_1\cdots p_r}\right)$

$=\left(\frac{p_1}{Q}\right)\cdots\left(\frac{p_r}{Q}\right)\left(\frac{Q}{p_1}\right)\cdots\left(\frac{Q}{p_r}\right)=$

$[(\left(\frac{p_1}{q_1}\right)\cdots\left(\frac{p_1}{q_s}\right))\cdots(\left(\frac{p_r}{q_1}\right)\cdots\left(\frac{p_r}{q_s}\right))][(\left(\frac{q_1}{p_1}\right)\cdots\left(\frac{q_s}{p_1}\right))\cdots(\left(\frac{q_1}{p_r}\right)\cdots\left(\frac{q_s}{p_r}\right))]=$

$\prod_{i,j}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)=\prod_{i,j}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}=(-1)^{\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}}=(-1)^{(\sum_{i=1}^r\frac{p_i-1}{2})(\sum_{j=1}^s\frac{q_j-1}{2})}$.

This equals $(-1)^{(\frac{P-1}{2})(\frac{Q-1}{2})}$, provided, mod 2, $(\sum_{i=1}^r\frac{p_i-1}{2})(\sum_{j=1}^s\frac{q_j-1}{2})\equiv(\frac{P-1}{2})(\frac{Q-1}{2})$. But our first proof above established this, for each of the two parts, and so it is also true for their product!