Math 568, Analytic Number Theory I, Spring 2020, Problems 6

Due Tuesday 25th February

As in homework 5 question 2 let $S(q,a)=\sum_{x=1}^{q} e(ax^2/q)$. The conclusions of that homework will be useful here. Throughout we suppose that $p\nmid a$. We call a a quadratic residue (QR) when $x^2\equiv a \pmod p$ is soluble, and quadratic non-residue (QNR) when it is insoluble. We define the Legendre symbol by $\left(\frac{x}{p}\right)_L$ to be 0 when $p|x$, 1 when x is a QR and -1 when x is a QNR.

1. Recall the Fermat-Euler theorem that states that $a^{p-1}\equiv 1 \pmod p$.
   (i) Prove that $a^{\frac{p-1}{2}}\equiv \pm 1 \pmod p$.
   (ii) Prove that a is a QR iff $a^{\frac{p-1}{2}}\equiv 1 \pmod p$, and hence that $\left(\frac{x}{p}\right)_L\equiv x^{\frac{p-1}{2}} \pmod p$.
   (iii) Prove that $\left(\frac{x}{p}\right)_L$ is a totally multiplicative function of x.
   (iv) Prove that if $xa\equiv 1 \pmod p$, then $\left(\frac{x}{p}\right)_L=\left(\frac{a}{p}\right)_L$.

2. Throughout p and q are different odd primes, $p\nmid a$, $q\nmid b$.
   (i) Prove that

$$S(p,a)=\sum_{y=1}^{p}\left(1+\left(\frac{y}{p}\right)_L\right)e(ay/p)=\left(\frac{a}{p}\right)_L S(p,1).$$

   (ii) Prove that $S(pq,aq+bp)=S(p,a)S(q,b)$.
   (iii) Choose a,b so that $aq\equiv 1 \pmod p$ and $bp\equiv 1 \pmod q$. Prove that $S(pq,aq+bp)=S(pq,1)$.
   (iv) Prove that if n is odd, then

$$S(n,1)=\begin{cases} n^{1/2} & n\equiv 1 \pmod 4,\\ n^{1/2}e(1/4) & n\equiv 3 \pmod 4.\end{cases}$$

   (v) Deduce the law of quadratic reciprocity, $\left(\frac{q}{p}\right)_L\left(\frac{p}{q}\right)_L=(-1)^{\frac{(p-1)(q-1)}{4}}$.
   This is Dirichlet's variation of one of Gauss' proofs.

3. Throughout p is an odd prime.
   (i) Prove that $S(8,p)S(p,8)=S(8p,1)$.
   (ii) Prove that $S(p,8)=\left(\frac{2}{p}\right)_L S(p,1)$.
   (iii) Prove that $S(8,p)=4e(p/8)$.
   (iv) Prove that $S(8p,1)=4p^{1/2}e(1/8)$.
   (v) Prove that $\left(\frac{2}{p}\right)_L=\begin{cases} 1 & p\equiv \pm 1 \pmod 8,\\ -1 & p\equiv \pm 3 \pmod 8.\end{cases}$ Of course, this is the "2-adic" part of the law of quadratic reciprocity.