571 Analytic number Theory I, Spring Term 2025, Problems 10

Return by Monday 7th April

Throughout

$$S(q,a)=\sum_{x=1}^{q} e(ax^k/q)$$

and given k and p we define τ by $p^\tau \| k$ and

$$\gamma=\begin{cases}\tau+1 & \text{when } p>2, \text{ or } p=2 \text{ and } \tau=0,\\ \tau+2 & \text{when } p=2 \text{ and } \tau>0.\end{cases}$$

Then we will show in class that when $t\ge\gamma$, a reduced residue modulo p^t is a k-th power residue if and only if it is one modulo p^γ. Much of the material below was worked out by Hardy and Littlewood in one of their papers “On some problems of paritio numeroroum”.

1. Show that $\gamma\le k$ unless $k=p=2$ in which case $\gamma=3$.

2. Suppose that $(a,p)=1$ and $t>\gamma$. Show that

$$S(p^t,a)=\begin{cases}p^{t-1} & \text{when } t\le k,\\ p^{k-1}S(p^{t-k},a) & \text{when } t>k.\end{cases}$$

3. Suppose that $(q,r)=(qr,a)$. Prove that

$$S(qr,a)=S(q,r^{k-1}a)S(r,q^{k-1}a).$$

4. Prove that if $k=2$ and $(q,a)=1$, then

$$|S(q,a)|^2\le 2q.$$

5. Suppose that $(p,a)=1$ and $k\ge3$. Let $t=uk+v$ with $1\le v\le k$ and $u\ge0$. (i) Prove that

$$S(p^t,a)=p^{(k-1)u}S(p^v,a).$$

(ii) Prove that if $v>1$, then

$$S(p^t,a)\le\begin{cases}p^{t-t/k} & (p>k),\\ kp^{t-t/k} & (p\le k).\end{cases}$$

(iii) Prove that if $v=1$, then

$$|S(p^l,a)|\le\begin{cases}p^{t-t/k} & (p>k^6),\\ kp^{t-t/k} & (p\le k^6).\end{cases}$$

6. Prove that if $(q,a)=1$, then $S(q,a)\ll q^{1-1/k}$.