571 ANALYTIC NUMBER THEORY I, FALL 2007, PROBLEMS 9

Return by Monday 29th October

1. Suppose that χ is a character (mod q), and that d is the conductor of χ. Show that if $(a,q)=1$ then

$$\Bigg|\sum_{\substack{n=1\\ n\equiv a \pmod d}}^{q} \chi(n)\Bigg| = \frac{\varphi(q)}{\varphi(d)}.$$

2. Let $G_k(a)=\displaystyle\sum_{n=1}^{p} e\Big(\frac{an^k}{p}\Big)$ and $N_r(h)$ denote the number of solutions of the congruence $x^r\equiv h \pmod p$.

(a) Prove that $G_r(a)=\displaystyle\sum_{h=1}^{p} N_r(h)e\Big(\frac{ah}{p}\Big)$.

(b) Let $l=(k,p-1)$. Show that if k is a positive integer then $N_k(h)=N_l(h)$ for all h, and hence that $G_k(a)=G_l(a)$.

(c) Suppose that $k \mid (p-1)$. Prove that $\displaystyle\sum_{a=1}^{p}|G_k(a)|^2 = p\sum_{h=1}^{p}N_k(h)^2$.

(d) Suppose that $k\mid(p-1)$. Show that there are $(p-1)/k$ residues h (mod p) for which $N_k(h)=k$, that $N_k(0)=1$, and that $N_k(h)=0$ for all other residue classes (mod p). Hence show that the right hand side above is $p(1+(p-1)k)$.

(e) Let k be a divisor of $p-1$. Suppose that $p\nmid a$, $p\nmid c$, and that $b\equiv ac^k \pmod p$. Show that $G_k(a)=G_k(b)$.

(f) Suppose that $k\mid(p-1)$. Show that if $p\nmid a$ then $|G_k(a)|<k\sqrt{p}$.

3. Suppose that $k\mid\varphi(q)$ and that $(h,q)=1$. (a) Prove that

$$\frac{1}{\varphi(q)}\sum_{\chi}\chi(x^k)\overline{\chi}(h)=\begin{cases}1 & \text{if } x^k\equiv h \pmod q,\\ 0 & \text{otherwise.}\end{cases}$$

(b) Let $N_k(h)$ be as in Exercise 2(a). Show that

$$N_k(h)=\sum_{\substack{\chi\\ \chi^k=\chi_0}}\chi(h).$$

4. Suppose that $k\mid(p-1)$, that $N_k(h)$ is as in Exercise 2(a), and let χ be a character of order k, say $\chi(n)=e((\operatorname{ind} n)/k)$. (a) Show that for all h,

$$N_k(h)=1+\sum_{j=1}^{k-1}\chi^j(h).$$

(b) Show that if $p\nmid a$ then

$$G_k(a)=\sum_{j=1}^{k-1}\overline{\chi}^j(a)\tau(\chi).$$

(c) Show that if $p\nmid a$ then $|G_k(a)|\le(k-1)\sqrt{p}$.