MATH 571 ANALYTIC NUMBER THEORY, SPRING 2025, PROBLEMS 4

Due Monday 10th February

1. Given $k, q \in \mathbb{N}$, let $\rho(q;n)$ denote the number of solutions of $x^k \equiv n \pmod{q}$ and define $S(q,a) = \sum_{x=1}^{q} e(ax^k/q)$.

(i) Prove that if $(n,q)=1$, then $\rho(q;n) = \sum_{x=1}^{q} \frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \overline{\chi}(n)\chi(x)^k$

(ii) Deduce that if $(n,q)=1$, then $\rho(q;n) = \sum_{\substack{\chi \pmod{q} \\ \chi^k = \chi_0}} \chi(n)$.

(iii) Given a prime number p, let $\mathcal{A}$ denote the set of characters χ modulo p such that $\chi^k = \chi_0$ but $\chi \neq \chi_0$. Prove that if $p \nmid a$, then

$$S(p,a) = \sum_{\chi \in \mathcal{A}} \overline{\chi}(a)\tau(\chi).$$

(iv) Let g be a primitive root modulo p. Prove that every character modulo p can be defined by $\chi_h(g^y) = e\Big(\frac{hy}{p-1}\Big)$.

(v) Prove that $\operatorname{card}(\mathcal{A}) = (k,p-1)-1$ and deduce that

$$|S(p,a)| \le \big((k,p-1)-1\big)p^{\frac{1}{2}}.$$

2. Here is a proof of a slightly weaker result avoiding characters.

(i) With the same notation, prove that if $1 \le y \le p-1$, then $S(p,a) = S(p,ay^k)$.

(ii) Prove that if $p \nmid n$, then there is an m with $1 \le m \le p-1$ such that $\rho(p;n) = \operatorname{card}\{y : 1 \le y \le p-1, g^{yk} \equiv g^m\}$ and that $\rho(p;n) \le (k,p-1)$.

(iii) Prove that if $p \nmid a$, then

$$(p-1)|S(p,a)|^2 = \sum_{z=1}^{p-1} \rho(p;z)|S(p,az)|^2 \le (k,p-1)\sum_{t=1}^{p-1} |S(p,t)|^2$$

(iv) Prove that

$$\sum_{t=1}^{p} |S(p,t)|^2 = \sum_{x=1}^{p} p\rho(p;x^k) \le p(p-1)(k,p-1)+p,$$

(v) Deduce that

$$|S(p,a)| \le \big((k,p-1)((k,p-1)-1)\big)^{1/2}p^{1/2}.$$

3. (Mordell c1930) (i) Let $N_k(p)$ denote the number of solutions in $x_1,\dots,x_k,y_1,\dots,y_k$ of the simultaneous congruences

$$\begin{aligned} x_1+\cdots x_k &\equiv y_1+\cdots y_k \pmod p\\ x_2+\cdots x_2 &\equiv y_2+\cdots y_k^2 \pmod p\\ &\vdots\\ x_1^k+\cdots x_k^k &\equiv y_1^k+\cdots y_k^k \pmod p \end{aligned}$$

Prove that if $k<p$, then $N_k(p)\le k!p^k$. In fact it can be shown that the $\mathbf{y}$ are a permutation of the $\mathbf{x}$. You might want to read up on Newton's identities connecting the symmetric functions of k variables and their power sums, and prove that if $P(x;\mathbf{u})=(x-u_1)\dots(x-u_k)$, then for any solution of the system one has $P(x;\mathbf{x})\equiv P(x;\mathbf{y}) \pmod p$.

(ii) Let $f(x)=a_1x+\cdots+a_kx^k$ and

$$S(p;f)=S(p;\mathbf{a})=\sum_{x=1}^{p} e\big(f(x)/p\big).$$

Show that

$$\sum_{a_1}^{p}\dots\sum_{a_k}^{p}|S(p;\mathbf{a})|^{2k}=p^kN_k(p)$$

(iii) Show that if $p\nmid y$ and $z\in\mathbb{Z}$, then

$$S(p;\mathbf{a})=S(p;\mathbf{b})$$

where $b_k=a_ky^k$ and $b_{k-1}=(ka_kz+a_{k-1})y^{k-1}$ and hence that

$$p\frac{p-1}{(k,p-1)}|S(p;\mathbf{a})|^{2k}\le k!p^{2k}.$$

(iv) Prove Mordel's theorem that if f is a polynomial with integer coefficients of degree k modulo p, then

$$|S(p;f)|\le kp^{1-1/k}.$$

These Gauss sums can be set up as zeros of L-functions for rational functions over finite fields. Later Weil proved RH for these L-functions and consequently

$$|S(p;f)|\le kp^{1/2}.$$

Also Vinogradov then imitated Mordel's argument to treat much more general exponential sums (the Vinogradov Mean Value Theorem).