MA59800ANT ANALYTIC NUMBER THEORY. PROBLEMS 3

TO BE HANDED IN BY TUESDAY 21ST FEBRUARY 2023

Key: A-questions are short questions testing basic skill sets; B-questions integrate essential methods of the course; C-questions are more challenging for enthusiasts, with hints available on request.

Throughout, we write

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q).$$

A1. Suppose that $k \in \mathbb{N}$, and p is a prime number for which $(k, p-1)=1$.
(i) By making use of primitive roots modulo p, show that $\{x^k : x \in \mathbb{Z}/p\mathbb{Z}\} = \mathbb{Z}/p\mathbb{Z}$.
(ii) Prove that when $p \nmid a$, one has $S(p,a) = 0$.

A2. Suppose that $k \in \mathbb{N}$ and p is a prime number with $p \nmid k$.
(i) Show that

$$\sum_{r_1=0}^{p-1}\sum_{r_2=0}^{p-1} e\Big(\frac{a(r_1+r_2p)^k}{p^2}\Big) = \sum_{r_1=0}^{p-1} e\Big(\frac{ar_1^k}{p^2}\Big)\sum_{r_2=0}^{p-1} e\Big(\frac{kar_1^{k-1}r_2}{p}\Big).$$

(ii) Deduce that whenever $(a,p)=1$, one has $S(p^2,a) = p$.

B3. Suppose that $k \in \mathbb{N}$, that X is a large real number, and that Q is a real number with $1 \leqslant Q < \frac{1}{2}X^{k/3}$. Denote by $\mathfrak{M}(Q)$ the union of the arcs

$$\mathfrak{M}(q,a) = \{\alpha \in [0,1) : |\alpha - a/q| \leqslant QX^{-k}\},$$

with $0 \leqslant a \leqslant q \leqslant Q$ and $(a,q)=1$, and put $\mathfrak{m}(Q) = [0,1) \setminus \mathfrak{M}(Q)$.
(i) Suppose that $\alpha \in \mathfrak{M}(Q)$ and $r \in \mathbb{N}$. Show that $r\alpha \in \mathfrak{M}(rQ)$ (mod 1).
(ii) Suppose that $r\alpha \in \mathfrak{M}(Q)$ (mod 1) with $r \in \mathbb{N}$. Show that $\alpha \in \mathfrak{M}(rQ)$.
(iii) Suppose that $\alpha \in \mathfrak{m}(Q)$ and $r \in \mathbb{N}$. Show that $r\alpha \in \mathfrak{m}(Q/r)$ (mod 1).
(iv) Suppose that $r\alpha \in \mathfrak{m}(Q)$ (mod 1) with $r \in \mathbb{N}$. Show that $\alpha \in \mathfrak{m}(Q/r)$.

B4. Suppose that $k \in \mathbb{N}$ and that p is a prime number with $p \equiv 1 \pmod{k}$.
(i) By making use of orthogonality, show that

$$p^{-1}\sum_{a=1}^{p} |S(p,a)|^2 = k(p-1)+1.$$

(ii) Let g be a primitive root modulo p. Show that $S(p, ag^{kw}) = S(p,a)$ for $w \in \mathbb{Z}$.
(iii) Let a_0 be the value of a with $1 \leqslant a \leqslant p-1$ for which $|S(p,a)|$ is largest. Prove that

$$p^{-1}\sum_{w=1}^{(p-1)/k} |S(p, a_0g^{kw})|^2 = \frac{p-1}{kp}|S(p,a_0)|^2,$$

and hence deduce that whenever $(a,p)=1$, one has $|S(p,a)| \leqslant k\sqrt{p}$. [You can challenge yourself to refine this upper bound to $|S(p,a)| \leqslant (k-1)\sqrt{p}$ by considering the second largest value of $|S(p,a)|$, and the third largest value, and so on.]

B5. Suppose that $k \geqslant 2$ and that p is a prime number. Fix integers a, b and c with $p \nmid abc$, and consider the number $N(a,b,c;p)$ of solutions of the congruence

$$ax^k + by^k + cz^k \equiv 0 \pmod{p},$$

with $1 \leqslant x, y, z \leqslant p$.
(i) Show that

$$N(a,b,c;p) = p^{-1} \sum_{u=0}^{p-1} S(p,au)S(p,bu)S(p,cu).$$

(ii) By considering separately the contributions in the latter sum arising from the term with $u = 0$, and that arising from the terms u with $1 \leqslant u \leqslant p-1$, show that

$$|N(a,b,c;p) - p^2| \leqslant k^2 p^{3/2}.$$

Deduce that the above congruence has a solution $(x,y,z) \neq (0,0,0)$ whenever $p > k^4$.

C6. Suppose that $k \in \mathbb{N}$. When q is a natural number, write

$$S^*(q,a) = \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar^k/q).$$

By adapting the ideas of problem B4, show that when p is a prime and $h \in \mathbb{N}$, then

$$p^{-h} \sum_{a=1}^{p^h} |S^*(p^h,a)|^2 \leqslant 2k\varphi(p^h),$$

where $\varphi(\cdot)$ is Euler's function. Hence deduce that $S(q,a) \ll q^{1-1/k+\varepsilon}$ when $(a,q) = 1$.

C7. Define

$$\mathfrak{S}_{s,k}(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(q^{-1}S(q,a)\right)^s e(-na/q).$$

Prove that when $n \neq 0$, the singular series $\mathfrak{S}_{s,k}(n)$ converges absolutely for $s \geqslant \frac{3}{2}k + 1$.