MATH 571, SPRING 2025, SOLUTIONS 6

χ denotes a character modulo q and $\tau(\chi) = \sum_{x=1}^{q} e(x/q)$.

1. (i) Prove that if either $(a,q)=1$ or q is prime and $\chi \neq \chi_0$, then $\displaystyle\sum_{x=1}^{q} \chi(x)e(ax/q) = \overline{\chi}(a)\tau(\chi)$.

(ii) Prove that if the c_x are arbitrary complex numbers, then $\displaystyle\frac{1}{q}\sum_{a=1}^{q}\left|\sum_{x=1}^{q} c_x e(ax/q)\right|^2 = \sum_{x=1}^{q}|c_x|^2$.

(iii) Prove that $|\tau(\chi)| \le q^{1/2}$, and that equality occurs when q is prime and $\chi \neq \chi_0$.

(i) When $(q,a)=1$, multiply the LHS by $\chi(a)$ and replace ax by x. If q is prime and $(a,q)>1$, so that $(a,q)=q$ the LHS and RHS are both 0. (ii) Mutliply out the LHS and observe that $\sum_{a=1}^{q} e(a(x-y)/q)$ is q or 0 according as to whether $q|x-y$ or not. (iii) Take $c_x = \chi(x)$ in (ii). The RHS $=\phi(q)$. The LHS $\ge q^{-1}\sum_{(a,q)=1}|\tau(\chi)|^2$. If q is prime, then the LHS is $q^{-1}\sum_{a=1}^{q-1}|\tau(\chi)|^2 + q^{-1}\left|\sum_{x=1}^{q}\chi(x)\right|^2$ and the second expression is 0.

2. Suppose that $M,N \in \mathbb{N}$ and χ is a non-principal character modulo p. (i) Prove that $\sum_{a=M+1}^{M+N} e(ax/p) = \frac{e(Nx/p)-1}{e(x/p)-1}e\big((M+1)x/p\big)$.

(ii) Prove that $\displaystyle\tau(\overline{\chi})\sum_{M<a\le M+N}\chi(a) = \sum_{x=1}^{p-1}\overline{\chi}(x)\frac{e(Nx/p)-1}{e(x/p)-1}e\big((M+1)x/p\big)$.

(iii) Prove $\displaystyle\sum_{x=1}^{p-1}\frac{1}{\sin(\pi x/p)} = \frac{2}{\pi}p\log p + O(p)$ and $\displaystyle\left|\sum_{M<a\le M+N}\chi(a)\right| \le \frac{2}{\pi}p^{1/2}\log p + O(p^{1/2})$.

(i) the LHS is the sum of the terms of a g.p. with c.r. $e(ax/p)$. (ii) By 1(i), $\tau(\overline{\chi})\chi(a) = \sum_{x=1}^{p-1}\overline{\chi}(x)e(ax/p)$. Apply (i). (iii) Since χ is non-principal, p is odd. We have two copies of $\sum_{1\le x<p/2}\frac{1}{\sin(\pi x/p)}$. When $0<\alpha$ we have $\alpha-\alpha^3/6<\sin\alpha<\alpha$, so when $\alpha\le\pi/2$, $(\sin\alpha)^{-1} = \alpha^{-1}+O(\alpha)$. Now use Euler's estimate.

3. Given an odd prime p let $n(p)$ denote the least quadratic non-residue modulo p. (i) Prove that $n(p)$ is prime. (ii) Prove that there is an r with $1\le r<n(p)$ such that $n(p)|p+r$, and show that $(p+r)/n(p)$ is a quadratic non-residue modulo p. Deduce that $n(p)\le\frac{1}{2}+\sqrt{p-1}$.

(i) Since the Legendre symbol is multiplicative at least one of the prime factors of $n(p)$ has to be a quadratic non-residue. (ii) Since p is a prime differing from $n(p)$ the division algorithm applied to $-p$ gives this at once. $p+r$ has to be a quadratic residue, since r is. Hence $n(p)^2\le p+r\le p+n(p)-1$. Now complete the square.

4. Let χ denote the Legendre symbol modulo p and suppose that Q is an integer with $n(p)<Q<n(p)^2$. (i) Prove that if $a\le Q$ and $\chi(a)=-1$, then a is divisible by exactly one prime p' with $n(p)\le p'<Q$ and that $\chi(p')=-1$. Deduce that $\sum_{a\le Q}\chi(a)\ge Q-\sum_{n(p)\le p'\le Q}2\lfloor Q/p'\rfloor$ and that the right hand side is $Q-2Q\log\frac{\log Q}{\log n(p)}+O\big(\frac{Q}{\log Q}\big)$. (ii) Let $Q=p^{1/2}(\log p)^2$ and assume that $n(p)>Q^{1/2}$. Prove that $n(p)\ll p^{\frac{1}{2\sqrt{e}}}(\log p)^{\frac{2}{\sqrt{e}}}$ (and this is also true when $n(p)\le Q^{1/2}$).

(i) At least one of the prime factors of p' of a is a quadratic non-residue. But then $p'\ge n(p)$, so there cannot be two. Thus the sum is $Q-2N$ where N is the number of $a\le Q$ with a quadratic non-residue prime factor. We have $N\le\sum_{n(p)\le p'\le Q}\lfloor Q/p'\rfloor$. The final estimate follows from Mertens or the prime numbe theorem. (ii) By Pólya-Vinogradov the LHS (i) is $\ll p^{1/2}\log p\ll Q/\log Q$. Thus dividing the estimate given by (i) by $2Q$ we have $\log\frac{\sqrt{e}\log n(p)}{\log Q}\ll 1/\log p$ and so $\sqrt{e}\log n(p)\le\log Q+O(1)$ whence $n(p)\ll Q^{1/\sqrt{e}}$.