MATH 571, ANALYTIC NUMBER THEORY, SPRING 2025, PROBLEMS 6

Due Monday February 24th

Let χ denote a character modulo q and define the Gauss sum by $\tau(\chi) = \sum_{x=1}^{q} e(x/q)$.

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

(ii) Prove that if the c_x are arbitrary complex numbers, then $\frac{1}{q}\sum_{a=1}^{q}\left|\sum_{x=1}^{q} c_x e(ax/q)\right|^2 = \sum_{x=1}^{q} |c_x|^2$.
(Compare Homework 1, question 2(ii).)
(iii) Prove that $|\tau(\chi)| \leq q^{1/2}$, and that equality occurs when q is prime and $\chi \neq \chi_0$.

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

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

This is the Pólya-Vinogradov inequality discovered by them independently in 1919. The above is Schur's [1919] proof, and was discovered independently by Vinogradov [1920]. Burgess in his Ph.D. thesis in 1959 showed that this bound can be replaced by εN whenever $N \gg p^{1/4+\varepsilon}$.

3. Given an odd prime p let $n(p)$ denote the least quadratic non-residue modulo p, i.e the smallest positive n such that $x^2 \equiv n \pmod{p}$ is insoluble.
(i) Prove that $n(p)$ is prime.
(ii) Prove that there is an r with $1 \leq r < n(p)$ such that $n(p)|p + r$, and show that $(p + r)/n(p)$ is a quadratic non-residue modulo p. Deduce that $n(p) \leq \frac{1}{2} + \sqrt{p - 3/4}$.

4. Let χ denote the Legendre symbol modulo p, the non-principal character χ modulo p with $\chi^2 = \chi_0$. It has the property that $1 + \chi(n)$ is the number of solutions of $x^2 = n \pmod{p}$.
(i) Suppose that Q is an integer with $n(p) < Q < n(p)^2$. Prove that if $a \leq Q$ and $\chi(a) = -1$, then a is divisible by exactly one prime p' with $n(p) \leq p' < Q$ and that $\chi(p') = -1$. Deduce that $\sum_{a\leq Q} \chi(a) \geq Q - \sum_{n(p)\leq p'\leq Q} 2\lfloor Q/p'\rfloor$ and that the right hand side is $Q - 2Q \log \frac{\log Q}{\log n(p)} + O\big(\frac{Q}{\log Q}\big)$.
(Merten's theorem is useful here.)
(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 note this is also true when $n(p) \leq Q^{1/2}$).

Vinogradov discovered this argument. Burgess obtained $n(p) \ll p^{\frac{1}{4\sqrt{e}}+\varepsilon}$. Vinogradov had conjectured that $n(p) \ll p^{\varepsilon}$. Ankeny [1952] proved that on the assumption of the RH for $L(s; \chi)$ one has $n(p) \ll (\log p)^2$. Perhaps $n(p) \ll \log p$ is true. There is a probabilistic argument which suggests this. Linnik [1941] has shown that the number $N(X)$ of primes $p \leq X$ such that $n(p) \gg p^{\delta}$ satisfies $N(X) \ll_{\delta} \log\log X$.