MATH 597E PRIMES, SPRING 2008, SOLUTION 1

1. (The 'Larger Sieve' of Gallagher [1971]) Let $\mathcal{N}$ be a subset of Z of the integers in an interval $[M+1, M+N]$, and let $Z(q,h)$ denote the number of $n \in \mathcal{N}$ such that $n \equiv h \pmod q$. For any primepower q let $r(q)$ denote the number of $h \pmod q$ for which $Z(q,h) > 0$. (a) Explain why $Z^2 = \Big(\sum_{h=1}^q Z(q,h)\Big)^2 \le r(q)\sum_{h=1}^q Z(q,h)^2$. (b) Let $\mathcal{Q}$ be a finite set of prime powers. Deduce that $Z^2 \sum_{q\in\mathcal{Q}} \frac{\Lambda(q)}{r(q)} \le \sum_{q\in\mathcal{Q}} \Lambda(q) \sum_{\substack{n_1,n_2\in\mathcal{N}\\ n_1\equiv n_2\,(q)}} 1$. (c) Group pairs n_1, n_2 of members of $\mathcal{N}$ according to their common difference, and hence show that the right hand side above is $= \sum_{d=-N+1}^{N-1} \sum_{\substack{n_1,n_2\in\mathcal{N}\\ n_1-n_2=d}} \sum_{\substack{q\in\mathcal{Q}\\ q|d}} \Lambda(q)$. (d) Show that $\sum_{d\ne 0} \sum_{\substack{n_1,n_2\in\mathcal{N}\\ n_1-n_2=d}} 1 = Z^2 - Z$. (e) Deduce that the expression in (c) is $\le Z\sum_{q\in\mathcal{Q}} \Lambda(q) + (Z^2-Z)\log N$. (f) Conclude that $Z \le \frac{\sum_{q\in\mathcal{Q}}\Lambda(q) - \log N}{\sum_{q\in\mathcal{Q}}\Lambda(q)/r(q) - \log N}$ provided that the denominator is positive. (g) Suppose that $r(p) = (p+1)/2$ for each odd prime p. By choosing $\mathcal{Q}$ suitably deduce that $Z \ll N^{1/2}$.

(a) Let $\mathcal{H}$ denote the residue classes h modulo q for which $Z(q,h) > 0$. Then the sum on the left is $\sum_{h\in\mathcal{H}} Z(q,h)$ and card$\mathcal{H} = r(q)$. Hence the inequality follows from Cauchy's inequality. (b) The sum on th right in (a) is the sum over the pairs n_1, n_2 in $\mathcal{N}$ with n_1, n_2 in the same residue class modulo q. In the inequality in (a), divide through by $r(q)$, multiply by $\Lambda(q)$ and sum over the elements q of $\mathcal{Q}$. (c) In the inner double sum on the RHS in (b) sort the terms according to the value d of $n_1 - n_2$. Obviously $|n_1 - n_2| \le N-1$ and so the d lie in $[1-N, N-1]$. Since $n_1 \equiv n_2 \pmod q$ we also have $q|d$. Thus the RHS in (b) is $\sum_{q\in\mathcal{Q}} \Lambda(q) \sum_{|d|\le N-1, q|d} \sum_{n_1,n_2\in\mathcal{N}; n_1-n_2=d} 1$. Interchanging the order of summation gives the desired conclusion. (d) Summing over all d simple gives the number of ordered pairs n_1, n_2, which is Z^2. The number of ordered pairs with $n_1 = n_2$ is Z. (e) When $d \ne 0$, $\sum_{q\in\mathcal{Q}, q|d} \Lambda(q) \le \sum_{q|d}\Lambda(q) = \log|d| < \log N$. Hence the expression in (c) is $\le Z\sum_{q\in\mathcal{Q}}\Lambda(q) + (Z^2 - Z)\log N$. (f) By (b) and (e), $Z^2\sum_{q\in\mathcal{Q}}\frac{\Lambda(q)}{r(q)} \le Z\sum_{q\in\mathcal{Q}}\Lambda(q) + (Z^2-Z)\log N$. Thus $Z^2(\sum_{q\in\mathcal{Q}}\Lambda(q)/r(q) - \log N) \le Z(\sum_{q\in\mathcal{Q}}\Lambda(q) - \log N)$. If $Z = 0$, then we are done. Otherwise a Z can be cancelled on both sides. (g) Let $Q \ge 3$ be a parameter at our disposal and let $\mathcal{Q}$ be the set of odd primes not exceeding Q. Then $\sum_{q\in\mathcal{Q}}\Lambda(q)/r(q) \ge \sum_{2<p\le Q}\frac{2\log p}{p+1} = 2\sum_{p\le Q}\frac{\log p}{p} + O(1) = 2\log Q + O(1)$. Let $Q = CN^{1/2}$ for a suitably large constant C. Then $\sum_{q\in\mathcal{Q}}\Lambda(q)/r(q) - \log N \ge 1$. Moreover $\sum_{q\in\mathcal{Q}}\Lambda(q) - \log N \gg N^{1/2}$.