Throughout $e(z) = e^{2\pi iz}$, $p$ is an odd prime and $\chi(x)$ the Legendre symbol modulo $p$. Also $\tau_p = \sum_{n=1}^p \chi(n)e(n/p)$, the Gauss sum formed from $\chi$. $L = L(p)$ is the least positive quadratic non-residue modulo $p$ and $U$ is the number of quadratic non-residues in $[1, N]$. 1. Show that if $m \in \mathbb{N}$ and $h \in \mathbb{Z}$, then $m^{-1} \sum_{n=1}^m e(ah/m) = 1$ when $m \mid h$ and 0 when $m \nmid h$. $m|h \Rightarrow (ah/m) = 1 \forall a \Rightarrow m^{-1} \sum_{n=1}^m e(ah/m) = 1$. $m \mid h \Rightarrow e(h/m) \neq 1$ so $\sum_{n=1}^m e(ah/m) = e((m+1)h/m) - e(h/m)/(1-e(h/m)) = 0$. 2. Let $c_1, \ldots, c_p$ be complex numbers. Show that $\sum_{n=1}^p |\sum_{n=1}^m e(\chi(n)e(n/p))|^2 = p \sum_{n=1}^p |c_n|^2$. On multiplying out and interchanging the order the multiple sum is $\sum_{n=1}^m \sum_{n=1}^m c_n c_n \sum_{n=1}^m e(\chi(m-n))/m$ does. But $\chi(a^2) = 1$. Thus $(p-1)|\tau_p|^2 = \sum_{n=1}^m \chi(c_n)^2$. By definition of $\sigma_p(a)$ and question 2 this is $p \sum_{n=1}^m |\chi(n)|^2 = p(p-1)$. Thus $|\tau_p|^2 = p$. 4. Let $M \in \mathbb{Z}$, $N \in \mathbb{N}$, $a \in \mathbb{Z}$, $p \nmid a$ and $T(M, N, a) = \sum_{n=1}^{M+N} e(an/p)$. Show that $T(M, N, a) = e(a(M + \frac{1}{2}N + \frac{1}{2})/p) \sin(\pi a N/p) \sin(\pi a N/p)$. $p \mid a \Rightarrow e(a/p) \neq 1$. Thus $T(M, N, a) = e(a(M + \frac{1}{2}N + \frac{1}{2})/p) = e(a(M + \frac{1}{2}) - e(\pi a N/2p)) = (e(a(2p)) - e(a/2p))$. 5. Let $M \in \mathbb{Z}$, $N \in \mathbb{N}$ and $S(M, N) = \sum_{n=1}^{M+N} \chi(n)$. Show that $S(M, N) = \sum_{n=1}^{M+N} \chi(n) = \sum_{n=1}^M \chi(m-n)/n$ and deduce that $S(M, N) = \frac{1}{p} \sum_{n=1}^M \chi(n-1/2)\chi(n)\chi(n-1/2)\chi(n)\chi(n+1/2)$ since the innermost sum in the triple sum is 0 unless $n \equiv m \pmod p$, in which case it is $p$, the triple sum is $M$. Interchanging the two inner sums gives $\sum_{n=1}^M e(an/p) \sum_{n=1}^M \chi(n-1/2)\chi(n)\chi(n-1/2)\chi(n)\chi(n+1/2)$. When $p \mid a$ the inner sum here is $\sigma_p(a) = \chi(-a)\tau_p$ and when $p \mid a$ it is $0 = \chi(-a)\tau_p$ any way. Thus interchanging the sums over $m$ and $a$ gives $S(M, N) = \frac{1}{p} \sum_{n=1}^M \chi(-a)T(M, N, a)$. Now, as $p \mid a$, question 4 gives the desired conclusion. 6. Show that if $a \in \mathbb{N}$, then $\frac{1}{2} \leq \log\frac{\sqrt{a} + 1}{\sqrt{a} - 1}$. Deduce that $\sum_{n=1}^M \frac{1}{\sin(\pi a N/p)} = 2 \sum_{n=1}^{M+N} \frac{1}{\sin(\pi a N/p)} \leq \sum_{n=1}^{M+N} \frac{p}{\sin(\pi a N/p)} \leq p \log p$. Prove that if $M \in \mathbb{Z}$, $N \in \mathbb{N}$, then $|S(M, N)| \leq \sqrt{p} \log p$. $\log\frac{\sqrt{a} + 1}{\sqrt{a} - 1} = \int_0^1 \left( \frac{1}{a + v} - \frac{1}{a - v} \right) dv = \int_0^1 \frac{2a}{a^2 - v^2} dv > \int_0^1 \frac{2}{a} dv$. When $0 \leq x \leq \frac{1}{2}$ we have $\sin \pi x \geq 2x$. [One proof of this is to observe that $f(x) = \sin \pi x - 2x$ satisfies $f''(x) < 0$ when $0 < x < \frac{1}{2}$ and that $f''(0) > 0 > f''(1/2)$ and $f(0) = f(1/2) = 0$, so there is an $x_0 \in (1/2, 1)$ so that $f$ is increasing on $(0, x_0)$ and decreasing on $(x_0, 1/2)$. Thus, as $\pi \approx \pi = \sin \pi y = \sin y, \sum_{n=1}^{M+N} \frac{1}{\sin(\pi a N/p)} = 2 \sum_{n=1}^{M+N} \frac{1}{\sin(\pi a N/p)} \leq \sum_{n=1}^{M+N} \frac{p}{\sin(\pi a N/p)} \leq p \log p$ of $\sqrt{a} \leq \sqrt{a} \log p$. (ii) Let $N = \sqrt{p} \log^2 p$. Prove that either $L < N^{1/2}$ or $\frac{1}{2} \leq \log \log N + O(1/\log N)$. Deduc the latter case that $\sqrt{a} \leq \sqrt{a} \log p + O(1/\log L)$, i.e. there is a constant $C_0$ such that $L^{1/2} \leq CN$. Show that in either case $L(p) \leq p^{1/2}(\log p)^{C_0}$. (i) If $\chi(a) = -1$, then the total number of prime factors $q$ of $n$ with $\chi(q) = -1$ is odd. Thus if there were more than one we would have $L \leq L \leq L^2$. But $L \geq 2$. Now every $n$ with $L \leq n \leq L^2$ and $\chi(n) = -1$ can be arranged according to the unique prime $q$ with $\chi(q) = -1$ which divides it and the number of such $n$ is $\frac{N}{\sqrt{q}}$. Thus $U = \sum_{n \leq q} \frac{N}{q} \leq N \sum_{n \leq q} \frac{N}{q} \leq N \sum_{n \leq q} \frac{1}{q}$ and the desired bound follows from Mertens’ theorem. [Note $\log \log N \geq L \geq \frac{1}{2} \log L^2 \geq \frac{1}{2} \log N$. On the other hand $U = \sum_{n \leq \sqrt{N}} \frac{1}{n} \leq \frac{1}{\sqrt{N}} \sqrt{N} \log \log N$ by question 6. (ii) If $L \leq N^{1/2}$, then $L \leq \frac{1}{2} \log \log p = N(\frac{1}{2} + O(1/\log p)) \leq N + O(N/\log N)$. Thus, by (i), $\frac{1}{2} N + O(N/\log N) \leq N \log \log N + O(N/\log N)$, so $\frac{1}{2} \leq \log \log N \leq O(1/\log L)$. Exponentiating gives $e^{1/2} \leq \frac{N}{\log N}(1 + O(1/\log L)) = \frac{N}{\log N}(1 + O(1/\log L))$. Hence $\sqrt{a} \leq \log CN$ for some positive constant $C$. Exponentiating once more gives $L \leq (CN)^{1/\sqrt{a}}$. Since $\frac{1}{2} \leq 1/\sqrt{a}$ this follows also when $L \geq N^{1/2}$. Inserting the definition of $N$ gives the conclusion.