

### Math 567 Number Theory I, Solutions 10

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  $m^{-1} \sum_{a=1}^m e(ah/m) = 1$  when  $m \mid h$  and 0 when  $m \nmid h$ .  $m \mid h \Rightarrow (ah/m) = 1 \forall a \Rightarrow m^{-1} \sum_{a=1}^m e(ah/m) = 1$ .  $m \nmid h \Rightarrow e(h/m) \neq 1$  so  $\sum_{a=1}^m e(ah/m) = (e((m+1)h/m) - e(h/m))/(1 - e(h/m)) = 0$ .

2. Let  $c_1, \dots, c_p$  be complex numbers. Show that  $\sum_{a=1}^p |\sum_{n=1}^p c_n e(an/p)|^2 = p \sum_{n=1}^p |c_n|^2$ . On multiplying out and interchanging the order the multiple sum is  $\sum_{m=1}^p \sum_{n=1}^p c_m \bar{c}_n \sum_{a=1}^p e(a(m-n)/p)$ . The innermost sum is 0 unless  $m \equiv n \pmod{p}$ . The latter can occur iff  $m = n$ , and then the innermost sum is  $p$ . Thus we obtain  $\sum_{m=1}^p |c_m|^2 p$ .

3. Let  $\sigma_p(a) = \sum_{n=1}^p \chi(n)e(an/p)$ . Show that if  $a \in \mathbb{Z}$  and  $p \nmid a$ , then  $\sigma_p(a) = \chi(a)\tau_p$  and that  $(p-1)|\tau_p|^2 = \sum_{a=1}^p |\sigma_p(a)|^2$ . By using Q. 2, show that  $|\tau_p| = \sqrt{p}$ .  $p \nmid a \Rightarrow \chi(a)\sigma_p(a) = \sum_{n=1}^p \chi(an)e(an/p) = \tau_p$  since  $an$  runs over a complete set of residues modulo  $p$  as  $n$  does. But  $\chi(a)^2 = 1$ . Thus  $(p-1)|\tau_p|^2 = \sum_{a=1}^p |\chi(a)\tau_p|^2 = \sum_{a=1}^p |\sigma_p(a)|^2$ . By definition of  $\sigma_p(a)$  and question 2 this is  $p \sum_{n=1}^p |\chi(n)|^2 = p(p-1)$ . Thus  $|\tau_p|^2 = p$ .

4. Let  $M \in \mathbb{Z}$ ,  $N \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $p \nmid a$  and  $T(M, N, a) = \sum_{n=M+1}^{M+N} e(an/p)$ . Show that

$$T(M, N, a) = e\left(a\left(M + \frac{1}{2}N + \frac{1}{2}\right)/p\right) \frac{\sin(\pi a N/p)}{\sin(\pi a/p)}.$$

$p \nmid a \Rightarrow e(a/p) \neq 1$ . Thus  $T(M, N, a) = e(a(M+1)/p)(e(aN/p) - 1)(e(a/p) - 1) = e(a(M + \frac{1}{2} + \frac{N}{2})/p)(e(aN/(2p)) - e(-aN/(2p)))/(e(a/(2p)) - e(-a/(2p)))$ .

5. Let  $M \in \mathbb{Z}$ ,  $N \in \mathbb{N}$  and  $S(M, N) = \sum_{n=M+1}^{M+N} \chi(n)$ . Show that  $S(M, N) = \sum_{m=M+1}^{M+N} \sum_{n=1}^p \chi(n)p^{-1} \sum_{a=1}^p e(a(m-n)/p)$  and deduce that  $S(M, N) = \frac{1}{p} \sum_{a=1}^{p-1} \chi(-a)\tau_p T(M, N, a)$  and  $|S(M, N)| \leq \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \frac{1}{|\sin(\pi a/p)|}$ . 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  $S(M, N)$ . Interchanging the two inner sums gives  $p^{-1} \sum_{a=1}^p e(am/p) \sum_{n=1}^p \chi(n)e(-an/p)$ . When  $p \nmid a$  the inner sum here is  $\sigma_p(-a) = \chi(-a)\tau_p$  and when  $p \mid a$  it is  $0 = \chi(-a)\tau_p$  anyway. Thus interchanging the sums over  $m$  and  $a$  gives  $S(M, N) = \frac{\tau_p}{p} \sum_{a=1}^{p-1} \chi(-a)T(M, N, a)$ . Now, as  $p \nmid a$ , question 4 gives the desired conclusion.

6. Show that if  $a \in \mathbb{N}$ , then  $\frac{1}{a} \leq \log \frac{a+\frac{1}{2}}{a-\frac{1}{2}}$ . Deduce that  $\sum_{a=1}^{p-1} \frac{1}{|\sin(\pi a/p)|} = 2 \sum_{a=1}^{(p-1)/2} \frac{1}{\sin \pi a/p} \leq \sum_{a=1}^{(p-1)/2} \frac{p}{a} \leq p \log p$ . Prove that if  $M \in \mathbb{Z}$ ,  $N \in \mathbb{N}$ , then  $|S(M, N)| \leq \sqrt{p} \log p$ .  $\log \frac{a+\frac{1}{2}}{a-\frac{1}{2}} = \int_0^{\frac{1}{2}} \left(\frac{1}{a+v} + \frac{1}{a-v}\right) dv = \int_0^{\frac{1}{2}} \frac{2a}{a^2-v^2} dv > \int_0^{\frac{1}{2}} \frac{2}{a} dv$ . 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  $x_0 \in (0, 1/2)$  so that  $f$  is increasing on  $(0, x_0)$  and decreasing on  $(x_0, 1/2)$ .] Thus, as  $\sin(\pi - y) = \sin y$ ,  $\sum_{a=1}^{p-1} \frac{1}{|\sin(\pi a/p)|} = 2 \sum_{a=1}^{(p-1)/2} \frac{1}{\sin \pi a/p} \leq \sum_{a=1}^{(p-1)/2} \frac{p}{a} \leq p \sum_{a=1}^{(p-1)/2} \log \frac{a+\frac{1}{2}}{a-\frac{1}{2}} = p(\log(p/2) - \log(1/2))$ .

7. (i) Show that if  $L \leq n \leq N \leq L^2$  and  $\chi(n) = -1$ , then there is exactly one prime  $q$  dividing  $n$  such that  $\chi(q) = -1$ , and  $L \leq q \leq N$ , and show that  $U = \sum_{L \leq q \leq N} \left[\frac{N}{q}\right] \leq N \log \frac{\log N}{\log L} + O\left(\frac{N}{\log N}\right)$ , where the sum is restricted to primes  $q$  with  $\chi(q) = -1$ . Show also that  $U \geq \frac{1}{2}N - \frac{1}{2}\sqrt{p} \log p$ . (ii) Let  $N = \lfloor \sqrt{p} \log^2 p \rfloor$ . Prove that either  $L < N^{1/2}$  or  $\frac{1}{2} \leq \log \frac{\log N}{\log L} + O(1/\log N)$ . Deduce in the latter case that  $\sqrt{e} \leq \frac{\log N}{\log L} + O(1/\log L)$ , i.e. there is a constant  $C$  such that  $L^{\sqrt{e}} \leq CN$ . Show that in either case  $L(p) \ll p^{\frac{1}{2\sqrt{e}}} (\log p)^{\frac{2}{\sqrt{e}}}$ . (i) If  $\chi(n) = -1$ , 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  $L^3 \leq n \leq N < L^2$ . 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  $\lfloor N/q \rfloor$ . Thus  $U = \sum_{L \leq q \leq N} \left[\frac{N}{q}\right] \leq N \sum_{L \leq q \leq N} \frac{1}{q}$  and the desired bound follows from Mertens' theorem. [Note  $\log N \geq \log L \geq \frac{1}{2} \log L^2 \geq \frac{1}{2} \log N$ .] On the other hand  $U = \sum_{n \leq N} \frac{1}{2}(1 - \chi(n)) \geq \frac{N}{2} - \frac{1}{2}\sqrt{p} \log p$  by question 6. (ii) If  $L \geq N^{1/2}$ , then  $\frac{1}{2}N - \frac{1}{2}\sqrt{p} \log p = N(\frac{1}{2} + O(1/\log p)) = \frac{1}{2}N + O(N/\log N)$ . Thus, by (i),  $\frac{1}{2}N + O(N/\log N) \leq N \log \frac{\log N}{\log L} + O(N/\log N)$ , so  $\frac{1}{2} \leq \log \frac{\log N}{\log L} + O(1/\log L)$ . Exponentiating gives  $e^{1/2} \leq \frac{\log N}{\log L} (1 + O(1/\log L)) = \frac{\log N}{\log L} + O(1/\log L)$ . Hence  $\sqrt{e} \log L \leq \log CN$  for some positive constant  $C$ . Exponentiating once more gives  $L \leq (CN)^{1/\sqrt{e}}$ . Since  $\frac{1}{2} \leq \frac{1}{\sqrt{e}}$  this follows also when  $L \leq N^{1/2}$ . Inserting the definition of  $N$  gives the conclusion.