

## MATH 567 NUMBER THEORY I, PROBLEMS 10

**To be submitted by Tuesday 4th November**

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  $\chi$ .

### Easier problems

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  $m \nmid h$ .
2. Let  $c_1, \dots, c_p$  be complex numbers. Show that  $\sum_{a=1}^p |\sum_{n=1}^p c_n e(an/p)|^2 = p \sum_{n=1}^p |c_n|^2$ .
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  $|\tau_p| = \sqrt{p}$ .
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  $T(M, N, a) = e(a(M + \frac{1}{2}N + \frac{1}{2})/p) \frac{\sin(\pi a N/p)}{\sin(\pi a/p)}$ .
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  $|S(M, N)| \leq \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \frac{1}{|\sin(\pi a/p)|}$ .
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  $|S(M, N)| \leq \sqrt{p} \log p$ . This is the Pólya-Vinogradov inequality [1917]. Assuming the generalized Riemann hypothesis we have  $|S(M, N)| \ll \sqrt{p} \log \log p$  (Montgomery & V [1977]) and this is essentially best possible (Paley [1932]).

### Harder problems

Let  $L = L(p)$  be the least positive quadratic non-residue modulo  $p$  and let  $U$  be the number of quadratic non-residues in  $[1, N]$ .

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  $U = \sum_{L \leq q \leq N}^* \left\lfloor \frac{N}{q} \right\rfloor \leq N \log \frac{\log N}{\log L} + O\left(\frac{N}{\log N}\right)$ , 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  $N = \lceil \sqrt{p} \log^2 p \rceil$ . 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  $L(p) \ll p^{\frac{1}{2\sqrt{e}}} (\log p)^{\frac{2}{\sqrt{e}}}$ . (Vinogradov [1927]. Burgess'  $L(p) \ll p^{\frac{1}{4\sqrt{e}} + \varepsilon}$  [1958] is an immediate consequence of his proof that  $|S(0, N)| < \varepsilon N$  whenever  $N > C(\varepsilon)p^{\frac{1}{4} + \varepsilon}$ .)