14. Incomplete character sums

Let χ be a Dirichlet character mod q. We call the sum

$$S_\chi(N) = \sum_{n=M+1}^{M+N} \chi(n)$$

incomplete if $N < q$. The "trivial bound" is

$$|S_\chi(N)| \le \sum_{n=M+1}^{M+N} 1 = N.$$

Using Gauss sums we can show that $S_\chi(N) = o(N)$ provided that $\chi \neq \chi_0$ and N is not too small compared to q.

We set $S = S_\chi(N)$ for convenience. Suppose first that χ is a primitive character mod q, with $q > 1$. Then Corollary 13.5 implies that

$$S = \frac{1}{\tau(\bar\chi)} \sum_{a=1}^{q} \bar\chi(a) \sum_{n=M+1}^{M+N} e(an/q).$$

The inner sum is a geometric series:

$$\begin{aligned}\sum_{n=M+1}^{M+N} e(an/q) &= \frac{e(a(M+N+1)/q) - e(a(M+1)/q)}{e(a/q) - 1} \\ &= e\left(\frac{(2M+N+1)a}{2q}\right) \frac{\sin(\pi aN/q)}{\sin(\pi a/q)},\end{aligned}$$

on recalling that $\sin(z) = \frac{1}{2i}(e^{iz} - e^{-iz})$. The triangle inequality now yields

$$\begin{aligned}|S| \le \frac{1}{|\tau(\bar\chi)|} \sum_{a=1}^{q} \frac{|\bar\chi(a)|}{\sin(\pi a/q)} &= \frac{1}{\sqrt{q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{1}{\sin(\pi a/q)} \\ &= \frac{2}{\sqrt{q}} \sum_{\substack{1 \le a \le q/2 \\ (a,q)=1}} \frac{1}{\sin(\pi a/q)}.\end{aligned}$$

But if q is even then $4 \mid q$ since if $q \equiv 2 \bmod 4$ there is no primitive character mod q. In this case we have $(q/2, q) > 1$ and so

$$|S| \le \frac{2}{\sqrt{q}} \sum_{\substack{1 \le a \le (q-1)/2 \\ (a,q)=1}} \frac{1}{\sin(\pi a/q)}.$$

The function $\sin(\pi\alpha)$ is concave downward in the interval $[0, \frac{1}{2}]$ and lies about the chord joining $(0,0)$ to $(\frac{1}{2}, 1)$ (see Figure 1). Hence $\sin(\pi\alpha) \ge 2\alpha$ for all $\alpha \in [0, \frac{1}{2}]$. This therefore implies that

$$|S| \le \sqrt{q} \sum_{\substack{1 \le a \le (q-1)/2 \\ (a,q)=1}} \frac{1}{a}.$$

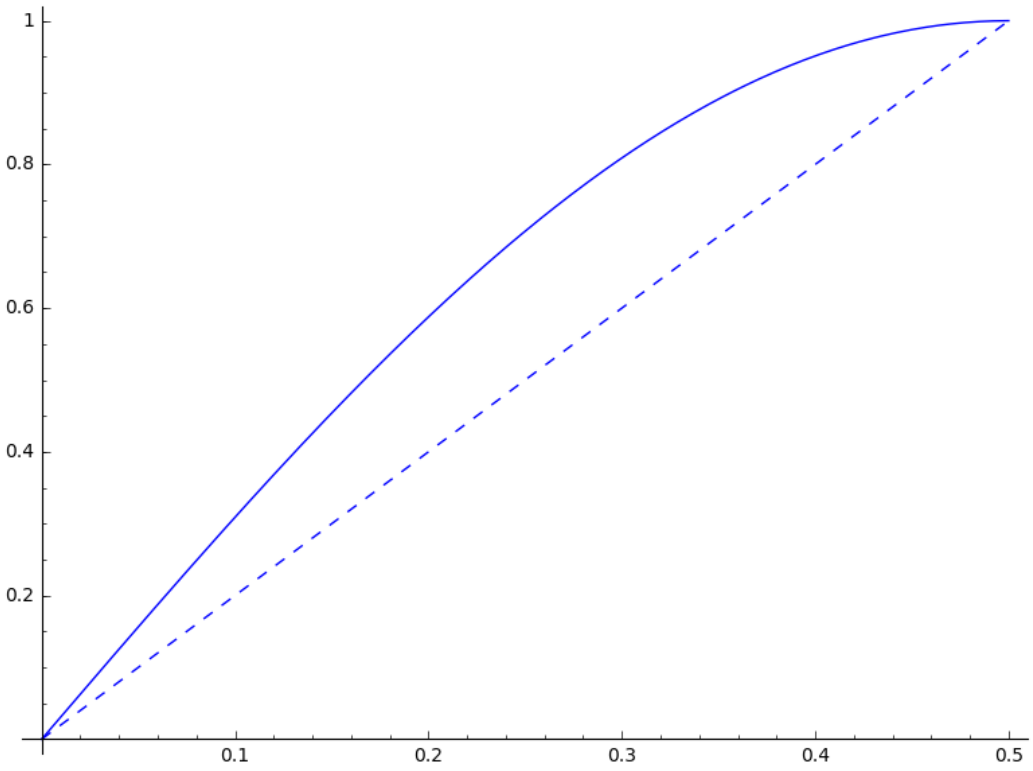

FIGURE 1. The function $\sin(\pi\alpha)$

Now

$$\begin{aligned}\log\frac{1+\frac{1}{2a}}{1-\frac{1}{2a}} &= \log\left(1+\frac{1}{2a}\right)-\log\left(1-\frac{1}{2a}\right)\\ &= \sum_{m=1}^{\infty}\frac{(-1)^{m+1}}{m}\left(\frac{1}{2a}\right)^m+\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{1}{2a}\right)^n\\ &\geq \frac{1}{a}.\end{aligned}$$

Thus

$$|S| \leq \sqrt{q}\sum_{1\leq a\leq(q-1)/2}\log\frac{2a+1}{2a-1} \leq \sqrt{q}\log q,$$

since

$$\sum_{1\leq a\leq(q-1)/2}\log\frac{2a+1}{2a-1} = \sum_{\substack{3\leq b\leq q\\ 2\nmid b}}\log b-\sum_{\substack{1\leq c\leq q-1\\ 2\nmid c}}\log c = \begin{cases}\log q & \text{if } q \text{ odd}\\ \log(q-1) & \text{if } q \text{ even}\end{cases}$$

$$\leq \log q.$$

Our work so far has shown that

$$|S_\chi(N)| \leq \sqrt{q}\log q,$$

if χ is a primitive character mod q.

Suppose now that χ is an imprimitive Dirichlet character mod q, induced by a primitive character χ^* mod d. Let

$$r = \prod_{\substack{p \mid q \\ p \nmid d}} p.$$

Then

$$S_\chi(N) = \sum_{n=M+1}^{M+N} \chi(n) = \sum_{\substack{n=M+1 \\ (n,r)=1}}^{M+N} \chi^*(n).$$

Recalling from Lemma 9.4 that $\mu * 1 = I$, we may write

$$\begin{aligned} S_\chi(N) &= \sum_{n=M+1}^{M+N} \chi^*(n) \sum_{k \mid (n,r)} \mu(k) \\ &= \sum_{k \mid r} \mu(k) \sum_{\substack{n=M+1 \\ k \mid n}}^{M+N} \chi^*(n) \\ &= \sum_{k \mid r} \mu(k)\chi^*(k) \sum_{M/k < m \le (M+N)/k} \chi^*(m). \end{aligned}$$

It now follows from combining the triangle inequality with our earlier estimate for primitive characters that

$$|S_\chi(N)| \le \sum_{k \mid r} |\mu(k)| \sqrt{d} \log d \le 2^{\omega(r)} \sqrt{d} \log d.$$

But $2^{\omega(r)} \le d(r) \ll \sqrt{r} \le \sqrt{q/d}$, by Lemma 9.13. This completes the proof of the following result:

Theorem 14.1 (Pólya–Vinogradov inequality)**.** *Let χ be a non-trivial Dirichlet character mod q. Then for any integers M, N with $N > 0$, we have*

$$\sum_{n=M+1}^{M+N} \chi(n) \ll \sqrt{q} \log q.$$

Note that this result is trivial if $N \ll \sqrt{q}$. The true bound is expected to be

$$S_\chi(N) \ll N^{1/2} q^\varepsilon, \tag{14.1}$$

for any $\varepsilon > 0$. This is non-trivial for $N > q^{3\varepsilon}$. However, we are a long way from being able to prove it!

The following result is one of the classical applications of the Pólya–Vinogradov inequality.

Corollary 14.2. *Let χ be a non-trivial character mod p and let n_χ be the least $n \in \mathbb{N}$ such that $\chi(n) \ne 1$. Then $n_\chi \ll_\varepsilon p^{\frac{1}{2\sqrt{e}} + \varepsilon}$ for any $\varepsilon > 0$.*

Proof. Recall that a number n is said to be y-smooth if it is composed entirely of primes $q \le y$. Suppose $\chi(n) = 1$ for $n \le y$. Then $\chi(n) = 1$ whenever n is y-smooth. Let $\Psi(x, y)$ denote the number of y-smooth numbers up to x. Then for $x \in [y, y^2]$ we have

$$\sum_{n \le x} \chi(n) = \Psi(x, y) + \sum_{\substack{q \text{ prime} \\ y < q \le x}} \chi(q)[x/q],$$

since n/q is y-smooth for any $q \in (y, x]$ and $n \le x$. We note that

$$\Psi(x, y) \ge [x] - \sum_{\substack{q \text{ prime} \\ y < q \le x}} [x/q].$$

Hence

$$\begin{aligned} \left| \sum_{n \le x} \chi(n) \right| &\ge \Psi(x, y) - \sum_{\substack{q \text{ prime} \\ y < q \le x}} [x/q] \\ &\ge [x] - 2 \sum_{\substack{q \text{ prime} \\ y < q \le x}} [x/q] \qquad (14.2) \\ &\ge x \left(1 - 2 \log \left(\frac{\log x}{\log y} \right) + O\left(\frac{1}{\log x} \right) \right), \end{aligned}$$

using the prime number theorem, together with the estimates $[t] = t + O(1)$ and

$$\sum_{p \le t} \frac{1}{p} = \log \log t + c_1 + O\left(\frac{1}{\log t} \right),$$

for some constant c_1. If $x = \sqrt{p}(\log p)^2$ then the left hand side of (14.2) is at most $\sqrt{p} \log p = o(x)$ by Pólya–Vinogradov. While if $y > x^{\frac{1}{\sqrt{e}} + \varepsilon}$, then

$$1 - 2 \log \left(\frac{\log x}{\log y} \right) > 1 + 2 \log \left(\varepsilon + \frac{1}{\sqrt{e}} \right) = 2 \log(1 + \varepsilon \sqrt{e}) > \varepsilon.$$

Hence the right hand side of (14.2) is $\gg \varepsilon x$. Thus it follows that

$$n_\chi \le x^{\frac{1}{\sqrt{e}} + \varepsilon} = p^{\frac{1}{2\sqrt{e}} + \frac{\varepsilon}{2}} (\log p)^{\frac{2}{\sqrt{e}} + 2\varepsilon} \ll_\varepsilon p^{\frac{1}{2\sqrt{e}} + \varepsilon},$$

as required. □

In a series of papers, Burgess established a series of bounds for relatively short character sums. The most famous is the following, which should be compared with the expectation (14.1).

Theorem 14.3 (The Burgess bound)**.** *Let χ be a non-trivial primitive Dirichlet character modulo a prime p. Then we have*

$$S_\chi(N) \ll N^{1/2} p^{3/16} (\log p)^{1/2}.$$

The rest of this section is devoted to a proof of this result. The proof is fairly intricate and relies on powerful bounds for complete exponential sums over finite fields — a result that we shall use as a "black box".

We argue by induction on N, proving that

$$|S_\chi(N)| \le cN^{1/2}p^{3/16}(\log p)^{1/2},$$

for an absolute constant c. We first note that Theorem 14.3 is either trivial or it follows from the Pólya–Vinogradov inequality, unless

$$c^2 p^{3/8}\log p \le N \le p^{5/8}\log p, \tag{14.3}$$

a condition that we now assume. Applying a shift $n \mapsto n+h$ with $1 \le h \le H < N$, we obtain

$$S_\chi(N) = \sum_{M<n\le M+N} \chi(n+h) + 2\theta E(H), \tag{14.4}$$

where $|\theta| \le 1$ and

$$E(H) = cH^{1/2}p^{3/16}(\log p)^{1/2}.$$

Here we have applied the induction hypothesis to the two character sums of length h which do not overlap with the original segment. Let $H = AB$, for $A, B \in \mathbb{N}$. We use shifts of the type

$$h = ab, \quad \text{with } 1 \le a \le A \text{ and } 1 \le b \le B.$$

Averaging (14.4) over a, b we deduce that

$$S_\chi(N) = \frac{1}{H}\sum_{\substack{1\le a\le A\\ 1\le b\le B}} \sum_{M<n\le M+N} \chi(n+ab) + 2\theta E(H),$$

where $|\theta| \le 1$. Now $\chi(n+ab) = \chi(a)\chi(\bar{a}n+b)$, where $\bar{a}$ is the multiplicative inverse of a modulo p. (Note that $\max\{A,B\} < p$ by (14.3), so that a, b are coprime to p.) Hence

$$|S_\chi(N)| \le \frac{V}{H} + 2E(H),$$

where

$$V = \sum_{x \bmod p} \nu(x) \left| \sum_{1\le b\le B} \chi(x+b) \right|$$

and $\nu(x)$ is the number of representations of x as $\bar{a}n \bmod p$ with $1 \le a \le A$ and $M < n \le M+N$. We shall estimate V without using the induction hypothesis, so that the implied constant will be independent of c.

The next step is to ease the dependence on $\nu(x)$ in V by an application of Hölder's inequality. This gives $V \le V_1^{\frac12} V_2^{\frac14} W^{\frac14}$, where

$$V_1 = \sum_{x \bmod p} \nu(x)$$

$$V_2 = \sum_{x \bmod p} \nu^2(x)$$

$$W = \sum_{x \bmod p} \left| \sum_{1\le b\le B} \chi(x+b) \right|^4.$$

Since $\nu(x)$ is often expected to be zero, the extension to a complete set of residues modulo p is quite wasteful in W. However it seems hard to take advantage of a condition like $\nu(x) \neq 0$ in the sum over x.

Lemma 14.4. *We have $V_1 \leq AN$ and $V_2 \ll AN(AN/p + \log A)$.*

Proof. It is obvious that $V_1 \leq AN$. Next, V_2 is the number of quadruples (a_1, a_2, n_1, n_2) with $1 \leq a_1, a_2 \leq A$ and $M < n_1, n_2 \leq M + N$ such that $a_1 n_2 \equiv a_2 n_1 \bmod p$. Fix a_1, a_2 and put $a_1 n_2 - a_2 n_1 = kp$. We have

$$\left| k - (a_1 - a_2)\frac{M}{p} \right| = \left| \frac{a_1(n_2 - M) - a_2(n_1 - M)}{p} \right| \leq \frac{2AN}{p}$$

and $(a_1, a_2) \mid k$. Given a_1, a_2, k as above we find that the number of pairs (n_1, n_2) satisfying the equation $a_1 n_2 - a_2 n_1 = kp$ is bounded above by $2N(a_1, a_2)/\max\{a_1, a_2\}$. Hence

$$\begin{aligned} V_2 &\leq 2N \sum_{1 \leq a_1, a_2 \leq A} \frac{(a_1, a_2)}{\max\{a_1, a_2\}} \left(1 + \frac{4AN}{(a_1, a_2)p}\right) \\ &\leq 2N \sum_{1 \leq a_1, a_2 \leq A} \frac{(a_1, a_2)}{\max\{a_1, a_2\}} + 2N \sum_{1 \leq a_1, a_2 \leq A} \frac{4AN}{p \max\{a_1, a_2\}}. \end{aligned}$$

Now

$$\sum_{1 \leq a_1, a_2 \leq A} \frac{1}{\max\{a_1, a_2\}} \leq 2A$$

and

$$\sum_{1 \leq a_1, a_2 \leq A} \frac{(a_1, a_2)}{\max\{a_1, a_2\}} \leq \sum_{d \leq A} d \sum_{\substack{1 \leq a_1, a_2 \leq A \\ d \mid a_1,\ d \mid a_2}} \frac{1}{\max\{a_1, a_2\}} \leq 2 \sum_{d \leq A} \frac{1}{d} \ll \log A.$$

The statement of the lemma is now obvious. □

Lemma 14.5. *We have $W \leq 2B^2 p + 3B^4 p^{1/2}$.*

The estimate of W lies at the heart of the proof of Burgess' bound. Lets see how it suffices to complete the proof of Theorem 14.3. We choose $A = [Np^{-\frac{1}{4}}/2]$ and $B = [p^{\frac{1}{4}}]$, giving $W \leq 5p^{\frac{3}{2}}$. Recall from (14.3) that $c^2 p^{3/8} \log p \leq N \leq p^{5/8} \log p$. Thus it follows that $A \geq 1$ and

$$AN \leq \frac{N^2}{2p^{\frac{1}{4}}} \leq p(\log p)^2.$$

Hence Lemma 14.4 gives $V_1 \leq AN$ and $V_2 \ll AN(\log p)^2$. Thus

$$V \leq V_1^{\frac{1}{2}} V_2^{\frac{1}{4}} W^{\frac{1}{4}} \ll (AN)^{\frac{3}{4}} p^{\frac{3}{8}} (\log p)^{\frac{1}{2}} \ll N^{\frac{3}{2}} p^{\frac{3}{16}} (\log p)^{\frac{1}{2}}.$$

Since $N \ll AB = H \leq N$ the statement of Theorem 14.3 now follows from the inequality

$$|S_\chi(N)| \leq \frac{V}{H} + 2cH^{1/2} p^{3/16} (\log p)^{1/2},$$

that we established previously.

Proof of Lemma 14.5. We may assume that $B < p$. Opening up the absolute value and interchanging the order of summation we find that

$$\begin{aligned} W &= \sum_{x \bmod p} \left| \sum_{1 \le b \le B} \chi(x+b) \right|^4 \\ &= \sum_{1 \le b_1, b_2, b_3, b_4 \le B} \sum_{x \bmod p} \chi(x+b_1)\chi(x+b_2)\bar{\chi}(x+b_3)\bar{\chi}(x+b_4) \\ &= \sum_{1 \le b_1, b_2, b_3, b_4 \le B} \sum_{x \bmod p} \chi(f(x)), \end{aligned}$$

where $f(x) = (x+b_1)(x+b_2)(x+b_3)^{p-2}(x+b_4)^{p-2}$ is a polynomial defined over the finite field $\mathbb{Z}/p\mathbb{Z}$. If $\{b_1, b_2\} = \{b_3, b_4\}$ then $f(x) = 1$ and the inner sum over x is equal to p. There are at most $2B^2$ ways in which this can happen and so the overall contribution from this case is $2B^2 p$. For the remaining values of $b_1, \dots, b_4$, for which $\{b_1, b_2\} \neq \{b_3, b_4\}$, we appeal to Weil's *Riemann hypothesis for curves over finite fields* as a black box result:

Theorem 14.6 (Riemann hypothesis for curves over finite fields)**.** *Let $\mathbb{F}_q$ be a finite field with q elements and let $\chi : \mathbb{F}_q^* \to \mathbb{C}$ be a non-trivial multiplicative character of order $d > 1$. Suppose that $f \in \mathbb{F}_q[x]$ has m distinct roots and is not equal to a dth power. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(f(x)\right) \right| \le (m-1)q^{1/2}.$$

We apply this to $f(x) = (x+b_1)(x+b_2)(x+b_3)^{p-2}(x+b_4)^{p-2}$. For the $b_1, \dots, b_4$ under consideration one of the b_i is a root of f of order either 1 or $p-2$, which is coprime with the order of $d \mid (p-1)$ of χ. Thus Theorem 14.6 applies with $m \le 4$ and it follows that

$$\left| \sum_{x \bmod p} \chi(f(x)) \right| \le 3\sqrt{p}$$

in our expression for W. Since there are at most B^4 values of $b_1, \dots, b_4$ that contribute to this case, the statement of the lemma follows. □

Exercise. By choosing different Hölder exponents show that the proof of Theorem 14.3 can be generalised to give

$$S_\chi(N) \ll_\varepsilon N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}+\varepsilon},$$

for any $\varepsilon > 0$ and any $r \ge 1$.