# 9

# Primitive characters and Gauss sums

## 9.1 Primitive characters

Suppose that $d \mid q$ and that $\chi^\star$ is a character (mod $d$), and set

$$\chi(n) = \begin{cases} \chi^\star(n) & (n,q) = 1; \\ 0 & \text{otherwise.} \end{cases} \tag{9.1}$$

Then $\chi(n)$ is multiplicative and has period $q$, so by Theorem 4.7 we deduce that $\chi(n)$ is a Dirichlet character (mod $q$). In this situation we say that $\chi^\star$ *induces* $\chi$. If $q$ is composed entirely of primes dividing $d$, then $\chi(n) = \chi^\star(n)$ for all $n$, but if there is a prime factor of $q$ not found in $d$, then $\chi(n)$ does not have period $d$. Nevertheless, $\chi$ and $\chi^\star$ are nearly the same in the sense that $\chi(p) = \chi^\star(p)$ for all but at most finitely many primes, and hence

$$L(s,\chi) = L(s,\chi^\star)\prod_{p\mid q}\left(1 - \frac{\chi^\star(p)}{p^s}\right). \tag{9.2}$$

Our immediate task is to determine when one character induces another.

**Lemma 9.1** *Let $\chi$ be a character* (mod $q$). *We say that $d$ is a* quasiperiod *of $\chi$ if $\chi(m) = \chi(n)$ whenever $m \equiv n \pmod d$ and $(mn, q) = 1$. The least quasiperiod of $\chi$ is a divisor of $q$.*

*Proof* Let $d$ be a quasiperiod of $\chi$, and put $g = (d, q)$. We show that $g$ is also a quasiperiod of $\chi$. Suppose that $m \equiv n \pmod g$ and that $(mn, q) = 1$. Since $g$ is a linear combination of $d$ and $q$, and $m - n$ is a multiple of $g$, it follows that there are integers $x$ and $y$ such that $m - n = dx + qy$. Then $\chi(m) = \chi(m - qy) = \chi(n + dx) = \chi(n)$. Thus $g$ is a quasiperiod of $\chi$. □

With more effort (see Exercise 9.1.1) it can be shown that if $d_1$ and $d_2$ are quasiperiods of $\chi$, then $(d_1, d_2)$ is also a quasiperiod, and hence the least



Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

quasiperiod divides all other quasiperiods, and in particular it divides $q$ (since $q$ is a quasiperiod of $\chi$).

The least quasiperiod $d$ of $\chi$ is called the *conductor* of $\chi$. Suppose that $d$ is the conductor of $\chi$. If $(n, d) = 1$, then $(n + kd, d) = 1$. Also, if $(r, d) = 1$ then there exist values of $k \pmod r$ for which $(n + kd, r) = 1$. Hence there exist integers $k$ for which $(n + kd, q) = 1$. For such a $k$ put $\chi^\star(n) = \chi(n + kd)$. Although there are many such $k$, there is only one value of $\chi(n + kd)$ when $(n + kd, q) = 1$. We extend the definition of $\chi^\star$ by setting $\chi^\star(n) = 0$ when $(n, d) > 1$. It is readily seen that $\chi^\star$ is multiplicative and that $\chi^\star$ has period $d$. Thus by Theorem 4.7, $\chi^\star$ is a character modulo $d$. Moreover, if $\chi_0$ is the principal character modulo $q$, then $\chi(n) = \chi^\star(n)\chi_0(n)$. Thus $\chi^\star$ induces $\chi$. Clearly $\chi^\star$ has no quasiperiod smaller than $d$, for otherwise $\chi$ would have a smaller quasiperiod, contradicting the minimality of $d$. In addition, $\chi^\star$ is the only character $(\mathrm{mod}\ d)$ that induces $\chi$, for if there were another, say $\chi_1$, then for any $n$ with $(n, d) = 1$ we would have $\chi^\star(n) = \chi^\star(n + kd) = \chi(n + kd) = \chi_1(n + kd) = \chi_1(n)$, on choosing $k$ as above.

A character $\chi$ modulo $q$ is said to be *primitive* when $q$ is the least quasiperiod of $\chi$. Such $\chi$ are not induced by any character having a smaller conductor. We summarize our discussion as follows.

**Theorem 9.2** *Let $\chi$ denote a Dirichlet character modulo $q$ and let $d$ be the conductor of $\chi$. Then $d \mid q$, and there is a unique primitive character $\chi^\star$ modulo $d$ that induces $\chi$.*

We now identify the primitive characters in such a way that we can describe them in terms of the explicit construction of Section 5.2.

**Lemma 9.3** *Suppose that $(q_1, q_2) = 1$ and that $\chi_1$ and $\chi_2$ are characters modulo $q_1$ and $q_2$, respectively. Put $\chi(n) = \chi_1(n)\chi_2(n)$. Then the character $\chi$ is primitive modulo $q_1q_2$ if and only if both $\chi_1$ and $\chi_2$ are primitive.*

*Proof* For convenience write $q = q_1q_2$. Suppose that $\chi$ is primitive modulo $q$, and for $i = 1, 2$ let $d_i$ be the conductor of $\chi_i$. If $(mn, q) = 1$ and $m \equiv n \pmod{d_1d_2}$ then $\chi_i(m) = \chi_i(n)$ for $i = 1, 2$, and hence $d_1d_2$ is a quasiperiod of $\chi$. Since $\chi$ is primitive, this means that $d_1d_2 = q$. But $d_i \mid q_i$, so this implies that $d_i = q_i$, which is to say that the characters $\chi_i$ are primitive.

Now suppose that $\chi_i$ is primitive modulo $q_i$ for $i = 1, 2$, and let $d$ be the conductor of $\chi$. Put $d_i = (d, q_i)$. We show that $d_1$ is a quasiperiod of $\chi_1$. Suppose that $m \equiv n \pmod{d_1}$ and that $(mn, q_1) = 1$. Choose $m'$ so that $m' \equiv m \pmod{q_1}$, $m' \equiv 1 \pmod{q_2}$. Similarly, choose $n'$ so that $n' \equiv n \pmod{q_1}$ and $n' \equiv 1 \pmod{q_2}$. Thus $m' \equiv n' \pmod d$ and $(m'n', q) = 1$, and hence $\chi(m') = \chi(n')$. But $\chi(m') = \chi_1(m)$ and $\chi(n') = \chi_1(n)$, so $\chi_1(m) = \chi_1(n)$. Thus

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

$d_1$ is a quasiperiod of $\chi_1$. Since $\chi_1$ is primitive, it follows that $d_1 = q_1$. Similarly $d_2 = q_2$. Thus $d = q$, which is to say that $\chi$ is primitive. □

By Lemma 9.3 we see that in order to exhibit the primitive characters explicitly it suffices to determine the primitive characters (mod $p^\alpha$). Suppose first that $p$ is odd, and let $g$ be a primitive root of $p^\alpha$. Then by (4.16) we know that any character $\chi \pmod{p^\alpha}$ is given by

$$\chi(n) = e\left(\frac{k \operatorname{ind}_g n}{\varphi(p^\alpha)}\right)$$

for some integer $k$. If $\alpha = 1$, then $\chi$ is primitive if and only if it is non-principal, which is to say that $(p-1) \nmid k$. If $\alpha > 1$, then $\chi$ is primitive if and only if $p \nmid k$. Now consider primitive characters (mod $2^\alpha$). When $\alpha = 1$ we have only the principal character, which is imprimitive. When $\alpha = 2$ we have two characters, namely the principal character, which is imprimitive, and the primitive character $\chi$ given by $\chi(4k+1) = 1$, $\chi(4k-1) = -1$. When $\alpha \geq 3$, we write an odd integer $n$ in the form $n \equiv (-1)^\mu 5^\nu \pmod{2^\alpha}$, and then characters (mod $2^\alpha$) are of the form

$$\chi(n) = e\left(\frac{j\mu}{2} + \frac{k\nu}{2^{\alpha-2}}\right)$$

where $j$ is determined (mod 2) and $k$ is determined (mod $2^{\alpha-2}$). Here $\chi$ is primitive if and only if $k$ is odd.

We now give two useful criteria for primitivity.

**Theorem 9.4** *Let $\chi$ be a character modulo $q$. Then the following are equivalent:*

(1) *$\chi$ is primitive.*

(2) *If $d \mid q$ and $d < q$, then there is a $c$ such that $c \equiv 1 \pmod{d}$, $(c, q) = 1$, $\chi(c) \neq 1$.*

(3) *If $d \mid q$ and $d < q$, then for every integer $a$,*

$$\sum_{\substack{n=1 \\ n \equiv a \pmod{d}}}^{q} \chi(n) = 0.$$

*Proof* (1) ⇒ (2). Suppose that $d \mid q$, $d < q$. Since $\chi$ is primitive, there exist integers $m$ and $n$ such that $m \equiv n \pmod{d}$, $\chi(m) \neq \chi(n)$, $\chi(mn) \neq 0$. Choose $c$ so that $(c, q) = 1$, $cm \equiv n \pmod{q}$. Thus we have (2).

(2) ⇒ (3). Let $c$ be as in (2). As $k$ runs through a complete residue system (mod $q/d$), the numbers $n = ac + kcd$ run through all residues (mod $q$) for

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

which $n \equiv a \pmod{d}$. Thus the sum $S$ in question is

$$S = \sum_{k=1}^{q/d} \chi(ac + kcd) = \chi(c)S.$$

Since $\chi(c) \neq 1$, it follows that $S = 0$.

(3) $\Rightarrow$ (1). Suppose that $d \mid q$, $d < q$. Take $a = 1$ in (3). Then $\chi(1) = 1$ is one term in the sum, but the sum is 0, so there must be another term $\chi(n)$ in the sum such that $\chi(n) \neq 1$, $\chi(n) \neq 0$. But $n \equiv 1 \pmod{d}$, so $d$ is not a quasiperiod of $\chi$, and hence $\chi$ is primitive. □

### 9.1.1 Exercises

1. Let $f(n)$ be an arithmetic function with period $q$ such that $f(n) = 0$ whenever $(n, q) > 1$. Call $d$ a quasiperiod of $f$ if $f(m) = f(n)$ whenever $m \equiv n \pmod{d}$ and $(mn, q) = 1$.
   (a) Suppose that $d_1$ and $d_2$ are quasiperiods, put $g = (d_1, d_2)$, and suppose that $m \equiv n \pmod{g}$ and $(mn, q) = 1$. Show that there exist integers $a$ and $b$ such that $m = n + ad_1 + bd_2$ and $(n + ad_1, q) = 1$.
   (b) Show that if $d_1$ and $d_2$ are quasiperiods of $f$ then so also is $(d_1, d_2)$.
   (c) Show that the least quasiperiod of $f$ divides all quasiperiods.
2. Let $\mathcal{S}(q)$ denote the set of all Dirichlet characters $\chi \pmod{q}$, and put $\mathcal{T}(q) = \bigcup_{d|q} \mathcal{S}(d)$. Show that the members of $\mathcal{T}(q)$ form a basis of the vector space of all arithmetic functions with period $q$ if and only if $q$ is square-free.
3. For $d|q$ let $\mathcal{U}(d, q)$ denote the set of $\varphi(q/d)$ functions

$$f(a) = \begin{cases} \chi(a/d) & (a, q) = d, \\ 0 & \text{otherwise} \end{cases}$$

   where $\chi$ runs over all Dirichlet characters $\pmod{q/d}$. Set $\mathcal{V}(q) = \bigcup_{d|q} \mathcal{U}(d, q)$. Show that the members of $\mathcal{V}(q)$ form a basis for the vector space of arithmetic functions with period $q$.
4. For $i = 1, 2$ let $\chi_i$ be a character $\pmod{q_i}$ where $(q_1, q_2) = 1$, and suppose that $d_i$ is the conductor of $\chi_i$. Show that $d_1 d_2$ is the conductor of $\chi_1 \chi_2$.
5. For $i = 1, 2$ suppose that $\chi_i$ is a character $\pmod{q_i}$. Show that the following two assertions are equivalent:
   (a) The characters $\chi_1$ and $\chi_2$ are induced by the same primitive character.
   (b) $\chi_1(p) = \chi_2(p)$ for all but at most finitely many primes $p$.
6. Let $\varphi_2(q)$ denote the number of primitive characters $\pmod{q}$.
   (a) Show that $\varphi_2(q)$ is a multiplicative function.
   (b) Show that $\sum_{d|q} \varphi_2(d) = \varphi(q)$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(c) Show that

$$\varphi_2(q) = q \prod_{p \| q} \left(1 - \frac{2}{p}\right) \prod_{p^2 | q} \left(1 - \frac{1}{p}\right)^2.$$

(d) Show that $\varphi_2(q) > 0$ if and only if $q \not\equiv 2 \pmod 4$.

7. Suppose that $\chi$ is a character (mod $q$), and that $d$ is the conductor of $\chi$. Show that if $(a, q) = 1$, then

$$\left| \sum_{\substack{n=1 \\ n \equiv a (\mathrm{mod}\, d)}}^{q} \chi(n) \right| = \frac{\varphi(q)}{\varphi(d)}.$$

8. (Martin 2006; Vorhauer 2006) Let $d(\chi)$ denote the conductor of $\chi$.

(a) Use the identity $\log d = \sum_{r|d} \Lambda(r)$ to show that

$$\sum_{\chi} \log d(\chi) \;=\; \varphi(q) \log q \;-\; \sum_{r|q} \Lambda(r) \sum_{\substack{\chi \\ r \nmid d(\chi)}} 1 \,.$$

(b) Show that if $p^a \| q$ and $1 \le b \le a$, then the number of $\chi$ modulo $q$ such that $p^b \nmid d(\chi)$ is exactly $\varphi(q)\varphi(p^{b-1})/\varphi(p^a)$.

(c) Conclude that

$$\sum_{\chi} \log d(\chi) = \varphi(q) \left( \log q - \sum_{p|q} \frac{\log p}{p-1} \right).$$

## 9.2 Gauss sums

Given a character $\chi$ modulo $q$, we define the Gauss sum $\tau(\chi)$ of $\chi$ to be

$$\tau(\chi) = \sum_{a=1}^{q} \chi(a) e(a/q). \tag{9.3}$$

This may be regarded as the inner product of the multiplicative character $\chi(a)$ with the additive character $e(a/q)$. As such, it is analogous to the gamma function $\Gamma(s) = \int_0^\infty x^{s-1} e^{-x}\, dx$, which is the inner product of the multiplicative character $x^s$ with the additive character $e^{-x}$ with respect to the invariant measure $dx/x$. Gauss sums are invaluable in transferring questions concerning Dirichlet characters to questions concerning additive characters, and vice versa.

The Gauss sum is a special case of the more general sum

$$c_\chi(n) = \sum_{a=1}^{q} \chi(a) e(an/q). \tag{9.4}$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

When $\chi$ is the principal character, this is Ramanujan's sum

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(an/q), \tag{9.5}$$

whose properties were discussed in Section 4.1. We now show that the sum $c_\chi(n)$ is closely related to $\tau(\chi)$.

**Theorem 9.5** *Suppose that $\chi$ is a character modulo $q$. If $(n, q) = 1$, then*

$$\chi(n)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a)e(an/q), \tag{9.6}$$

*and in particular*

$$\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi}). \tag{9.7}$$

*Proof* If $(n, q) = 1$, then the map $a \mapsto an$ permutes the residues modulo $q$, and hence

$$\chi(n)c_\chi(n) = \sum_{a=1}^{q} \chi(an)e(an/q) = \tau(\chi).$$

On replacing $\chi$ by $\overline{\chi}$, this gives (9.6), and (9.7) follows by taking $n = -1$. □

**Theorem 9.6** *Suppose that $(q_1, q_2) = 1$, that $\chi_i$ is a character modulo $q_i$ for $i = 1, 2$, and that $\chi = \chi_1\chi_2$. Then*

$$\tau(\chi) = \tau(\chi_1)\tau(\chi_2)\chi_1(q_2)\chi_2(q_1).$$

*Proof* By the Chinese Remainder Theorem, each $a \pmod{q_1q_2}$ can be written uniquely as $a_1q_2 + a_2q_1$ with $1 \le a_i \le q_i$. Thus the general term in (9.3) is $\chi_1(a_1q_2)\chi_2(a_2q_1)e(a_1/q_1)\, e(a_2/q_2)$, so the result follows. □

For primitive characters the hypothesis that $(n, q) = 1$ in Theorem 9.5 can be removed.

**Theorem 9.7** *Suppose that $\chi$ is a primitive character modulo $q$. Then* (9.6) *holds for all $n$, and $|\tau(\chi)| = \sqrt{q}$.*

*Proof* It suffices to prove (9.6) when $(n, q) > 1$. Choose $m$ and $d$ so that $(m, d) = 1$ and $m/d = n/q$. Then

$$\sum_{a=1}^{q} \chi(a)e(an/q) = \sum_{h=1}^{d} e(hm/d) \sum_{\substack{a=1 \\ a\equiv h \pmod d}}^{q} \chi(a).$$

Since $d \mid q$ and $d < q$, the inner sum vanishes by Theorem 9.4. Thus (9.6) holds also in this case.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

We replace $\chi$ in (9.6) by $\overline{\chi}$, take the square of the absolute value of both sides, and sum over $n$ to see that

$$\varphi(q)|\tau(\chi)|^2 = \sum_{n=1}^{q}\left|\sum_{a=1}^{q}\chi(a)e(an/q)\right|^2 = \sum_{a=1}^{q}\sum_{b=1}^{q}\chi(a)\overline{\chi}(b)\sum_{n=1}^{q}e((a-b)n/q).$$

The innermost sum on the right is 0 unless $a \equiv b \pmod{q}$, in which case it is equal to $q$. Thus $\varphi(q)|\tau(\chi)|^2 = \varphi(q)q$, and hence $|\tau(\chi)| = \sqrt{q}$. □

If $\chi$ is primitive modulo $q$, then not only does (9.6) hold for all $n$ but also $\tau(\overline{\chi}) \neq 0$, and hence we have

**Corollary 9.8** *Suppose that $\chi$ is a primitive character modulo $q$. Then for any integer $n$,*

$$\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q}\overline{\chi}(a)e(an/q).$$

This is very useful, since it allows us to express the multiplicative character $\chi$ as a linear combination of additive characters $e(an/q)$. As a first application, we use this formula to express $L(1, \chi)$ in closed form.

**Theorem 9.9** *Suppose that $\chi$ is a primitive character modulo $q$ with $q > 1$. If $\chi(-1) = 1$, then*

$$L(1, \chi) = \frac{-\tau(\chi)}{q}\sum_{a=1}^{q-1}\overline{\chi}(a)\log(\sin \pi a/q), \tag{9.8}$$

*while if $\chi(-1) = -1$, then*

$$L(1, \chi) = \frac{i\pi\tau(\chi)}{q^2}\sum_{a=1}^{q-1}a\overline{\chi}(a). \tag{9.9}$$

*Proof* Since $L(1, \chi) = \sum_{n=1}^{\infty}\chi(n)/n$, by Corollary 9.8,

$$L(1, \chi) = \frac{1}{\tau(\overline{\chi})}\sum_{n=1}^{\infty}\frac{1}{n}\sum_{a=1}^{q-1}\overline{\chi}(a)e(an/q) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q-1}\overline{\chi}(a)\sum_{n=1}^{\infty}\frac{e(an/q)}{n}.$$

But $\log(1-z)^{-1} = \sum_{n=1}^{\infty}z^n/n$ for $|z| \leq 1$, $z \neq 1$, where the logarithm is the principal branch. We take $z = e(\theta)$ where $0 < \theta < 1$. Since $1 - e(\theta) = -2ie(\theta/2)\sin \pi\theta$, it follows that $\log(1 - e(\theta)) = \log(2 \sin \pi\theta) + i\pi(\theta - 1/2)$. Thus

$$L(1, \chi) = \frac{-1}{\tau(\overline{\chi})}\sum_{a=1}^{q-1}\overline{\chi}(a)(\log(2 \sin \pi a/q) + i\pi(a/q - 1/2)).$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

Since $\sum_{a=1}^{q-1} \overline{\chi}(a) = 0$, this is

$$\frac{-1}{\tau(\overline{\chi})}(S + iT)$$

where $S = \sum_{a=1}^{q-1} \overline{\chi}(a) \log(\sin \pi a/q)$ and $T = \pi/q \sum_{a=1}^{q-1} \overline{\chi}(a)a$. On replacing $a$ by $q - a$ we see that $S = \chi(-1)S$ and $T = -\chi(-1)T$. Thus if $\chi(-1) = 1$, then $T = 0$ and so

$$L(1, \chi) = \frac{-1}{\tau(\overline{\chi})} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(\sin \pi a/q).$$

Then by (9.7) we obtain (9.8). If $\chi(-1) = -1$ then $S = 0$ and so

$$L(1, \chi) = \frac{-i\pi}{\tau(\overline{\chi})q} \sum_{a=1}^{q-1} \overline{\chi}(a)a.$$

Then by (9.7) we obtain (9.9). □

We next show that $\tau(\chi)$ can be expressed in terms of $\tau(\chi^\star)$ where $\chi^\star$ is the primitive character that induces $\chi$.

**Theorem 9.10** *Let $\chi$ be a character modulo $q$ that is induced by the primitive character $\chi^\star$ modulo $d$. Then $\tau(\chi) = \mu(q/d)\chi^\star(q/d)\tau(\chi^\star)$.*

*Proof* If $(d, q/d) > 1$, then $\chi^\star(q/d) = 0$, so we begin by showing that $\tau(\chi) = 0$ in this case. Let $p$ be a prime such that $p \mid d$, $p \mid q/d$, and write $a = jq/p + k$ with $0 \le j < p$, $0 \le k < q/p$. Then

$$\tau(\chi) = \sum_{a=0}^{q-1} \chi(a)e(a/q) = \sum_{k=1}^{q/p} \sum_{j=1}^{p} \chi(jq/p + k)e(j/p + k/q).$$

But $p \mid (q/p)$, so $(jq/p + k, q) = 1$ if and only if $(jq/p + k, q/p) = 1$, which in turn is equivalent to $(k, q/p) = 1$. Also, $d \mid q/p$, so the above is

$$= \sum_{\substack{k=1 \\ (k,q/p)=1}}^{q/p} \chi^\star(k)e(k/q) \sum_{j=1}^{p} e(j/p).$$

Here the inner sum vanishes, so $\tau(\chi) = 0$ when $(d, q/d) > 1$.

Now suppose that $(d, q/d) = 1$, and let $\chi_0$ denote the principal character modulo $q/d$. Then by Theorem 9.6,

$$\tau(\chi) = \tau(\chi_0\chi^\star) = \tau(\chi_0)\tau(\chi^\star)\chi_0(d)\chi^\star(q/d).$$

By taking $n = 1$ in Theorem 4.1 we find that $\tau(\chi_0) = \mu(q/d)$. Thus we have the stated result. □

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

We now turn our attention to the more general $c_\chi(n)$. To this end we begin with an auxiliary result.

**Lemma 9.11** *Let $\chi$ be a character modulo $q$ induced by the primitive character $\chi^\star$ modulo $d$. Suppose that $r \mid q$. Then*

$$\sum_{\substack{n=1 \\ n\equiv b \pmod r}}^{q} \chi(n) = \begin{cases} \chi^\star(b)\varphi(q)/\varphi(r) & \text{if } (b,r)=1 \text{ and } d \mid r, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof* Let $S(b,r)$ denote the sum in question. If $p \mid (b,r)$ and $n \equiv b \pmod r$, then $p \mid n$, and so $(n,q) > 1$. Thus each term in $S(b,r)$ is 0. Thus we are done when $(b,r) > 1$, so we suppose that $(b,r) = 1$. Consider next the case when $d \nmid r$. Then $r$ is not a quasiperiod of $\chi$. Hence there exist $m$ and $n$ such that $(mn,q) = 1$, $m \equiv n \pmod r$, and $\chi(m) \neq \chi(n)$. Choose $c$ so that $cn \equiv m \pmod q$. Then $c \equiv 1 \pmod r$ and $\chi(c) \neq 1$. Hence $\chi(c)S(b,r) = S(b,r)$, as in the proof of Theorem 9.4, so $S(b,r) = 0$ in this case. Finally suppose that $d \mid r$. Let $\chi_0$ be the principal character modulo $q$. If $n \equiv b \pmod r$, then $\chi^\star(n) = \chi^\star(b)$. Thus

$$S(b,r) = \chi^\star(b) \sum_{\substack{n=1 \\ n\equiv b \pmod r}}^{q} \chi_0(n).$$

Write $q/r = q_1q_2$ where $q_1$ is the largest divisor of $q/r$ that is relatively prime to $r$. Then the sum on the right above is

$$\sum_{\substack{k=1 \\ (kr+b,q_1)=1}}^{q_1q_2} 1 = q_2\varphi(q_1) = \varphi(q)/\varphi(r),$$

as required. □

We are now in a position to deal with $c_\chi(n)$.

**Theorem 9.12** *Let $\chi$ be a character modulo $q$ induced by the primitive character $\chi^\star$ modulo $d$. Put $r = q/(q,n)$. Then $c_\chi(n) = 0$ if $d \nmid r$, while if $d \mid r$, then*

$$c_\chi(n) = \overline{\chi}^\star(n/(q,n))\chi^\star(r/d)\mu(r/d)\frac{\varphi(q)}{\varphi(r)}\tau(\chi^\star).$$

*Proof* If $(n,q) = 1$, then by Theorem 9.5 and Theorem 9.10 we see that

$$c_\chi(n) = \overline{\chi}(n)\tau(\chi) = \overline{\chi}^\star(n)\mu(q/d)\chi^\star(q/d)\tau(\chi^\star).$$

Since $r = q$, we have $d \mid r$, so we have the correct result. Now suppose that $(n,q) > 1$. In the definition (9.4) of $c_\chi(n)$, let $a = br + k$ with $0 \le b < q/r$,

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

$1 \le k \le r$. Then

$$c_\chi(n) = \sum_{k=1}^{r} e(kn/q) \sum_{b=1}^{q/r} \chi(br+k).$$

By Lemma 9.11 this is 0 when $d \nmid r$. Thus we may suppose that $d \mid r$. Then, by Lemma 9.11,

$$c_\chi(n) = \sum_{\substack{k=1 \\ (k,r)=1}}^{r} e(kn/q)\chi^\star(k)\varphi(q)/\varphi(r).$$

Put $m = n/(q,n)$, and let $\chi_1$ denote the character modulo $r$ induced by $\chi^\star$. Then the above is

$$= \frac{\varphi(q)}{\varphi(r)} \sum_{k=1}^{r} e(km/r)\chi_1(k).$$

Since $(m,r) = 1$, we see by the first case treated that the above is

$$\frac{\varphi(q)}{\varphi(r)} \overline{\chi}^\star(m)\mu(r/d)\chi^\star(r/d)\tau(\chi^\star),$$

which suffices. □

### 9.2.1 Exercises

1. (a) Show that

$$\frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a)\tau(\chi) = \begin{cases} e(a/q) & (a,q) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

   (b) Show that for all integers $a$,

$$e(a/q) = \sum_{\substack{d \mid q \\ d \mid a}} \frac{1}{\varphi(q/d)} \sum_{\chi \pmod{q/d}} \overline{\chi}(a/d)\tau(\chi).$$

2. Let

$$G_k(a) = \sum_{n=1}^{p} e\left(\frac{an^k}{p}\right).$$

   (a) Let $N_k(h)$ denote the number of solutions of the congruence $x^k \equiv h \pmod{p}$. Explain why

$$G_k(a) = \sum_{h=1}^{p} N_k(h) e\left(\frac{ah}{p}\right).$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(b) Let $l = (k, p-1)$. Show that if $k$ is a positive integer, then $N_k(h) = N_l(h)$ for all $h$, and hence that $G_k(a) = G_l(a)$.

(c) Suppose that $k \mid (p-1)$. Explain why

$$\sum_{a=1}^{p} |G_k(a)|^2 = p \sum_{h=1}^{p} N_k(h)^2.$$

(d) Suppose that $k \mid (p-1)$. Show that there are $(p-1)/k$ residues $h \pmod p$ for which $N_k(h) = k$, that $N_k(0) = 1$, and that $N_k(h) = 0$ for all other residue classes $\pmod p$. Hence show that the right-hand side above is $p(1 + (p-1)k)$.

(e) Let $k$ be a divisor of $p-1$. Suppose that $p \nmid a$, $p \nmid c$, and that $b \equiv ac^k \pmod p$. Show that $G_k(a) = G_k(b)$.

(f) Suppose that $k \mid (p-1)$. Show that if $p \nmid a$ then $|G_k(a)| < k\sqrt{p}$.

3. Suppose that $k \mid \varphi(q)$ and that $(h, q) = 1$.

(a) Explain why

$$\frac{1}{\varphi(q)} \sum_{\chi} \chi(x^k)\overline{\chi}(h) = \begin{cases} 1 & \text{if } x^k \equiv h \pmod q, \\ 0 & \text{otherwise.} \end{cases}$$

(b) Let $N_k(h)$ be as in Exercise 2(a). Show that

$$N_k(h) = \sum_{\substack{\chi \\ \chi^k = \chi_0}} \chi(h).$$

4. Suppose that $k \mid (p-1)$, that $N_k(h)$ is as in Exercise 2(a), and let $\chi$ be a character of order $k$, say $\chi(n) = e((\operatorname{ind} n)/k)$.

(a) Show that for all $h$,

$$N_k(h) = 1 + \sum_{j=1}^{k-1} \chi^j(h).$$

(b) Show that if $p \nmid a$, then

$$G_k(a) = \sum_{j=1}^{k-1} \overline{\chi}^j(a)\tau(\chi^j).$$

(c) Show that if $p \nmid a$, then $|G_k(a)| \le (k-1)\sqrt{p}$.

5. Suppose that $\chi_i$ is a character $(\bmod q_i)$ for $i = 1, 2$, with $(q_1, q_2) = 1$. Show that

$$c_{\chi_1\chi_2}(n) = \chi_1(q_2)\chi_2(q_1)c_{\chi_1}(n)c_{\chi_2}(n)\,.$$

6. (Apostol 1970) Let $\chi$ be a character modulo $q$ such that the identity (9.6) holds for all integers $n$. Show that $\chi$ is primitive $(\bmod q)$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

7. Let $N(q)$ denote the number of pairs $x, y$ of residue classes (mod $q$) such that $y^2 \equiv x^3 + 7 \pmod q$.
   (a) Show that $N(q)$ is a multiplicative function of $q$, that $N(2) = 2$, $N(3) = 3$, $N(7) = 7$, and that $N(p) = p$ when $p \equiv 2 \pmod 3$.
   (b) Suppose that $p \equiv 1 \pmod 3$. Let $\chi_1(n)$ be a cubic character modulo $p$, and let $\chi_2(n) = \left(\frac{n}{p}\right)$ be the quadratic character modulo $p$. Show that
$$\begin{aligned} N(p) &= \frac{1}{p}\sum_{a=1}^{p} e(7a/p)\left(\sum_{h=1}^{p}\big(1+\chi_1(h)+\chi_1^2(h)\big)e(ah/p)\right) \\ &\quad\times\left(\sum_{k=1}^{p}(1+\chi_2(k))e(-ak/p)\right) \\ &= p + \frac{2}{p}\Re\big(\tau(\chi_1)\tau(\chi_2)\tau\big(\chi_1^2\chi_2\big)\chi_1\chi_2(-7)\big), \end{aligned}$$
   and deduce that $|N(p) - p| \le 2\sqrt{p}$.
   (c) Deduce that $N(p) > 0$ for all $p$.
   (d) Show that $N(2^k) = 2^{k-1}$ for $k \ge 2$, that $N(3^k) = 2 \cdot 3^{k-1}$ for $k \ge 2$, that $N(7^k) = 6 \cdot 7^{k-1}$ for $k \ge 2$, and that $N(p^k) = N(p)p^{k-1}$ for all other primes.
   (e) Conclude that the congruence $y^2 \equiv x^3 + 7 \pmod q$ has solutions for every positive integer $q$.
   (f) Suppose that $x$ and $y$ are integers such that $y^2 = x^3 + 7$. Show that $2 \mid y$, $x \equiv 1 \pmod 4$, and that $x > 0$. Note that $y^2 + 1 = (x+2)(x^2 - 2x + 4)$, so that $y^2 + 1$ is composed of primes $\equiv 1 \pmod 4$, and yet $x + 2 \equiv 3 \pmod 4$. Deduce that this equation has no solution in integers.
8. (Mordell 1933) Explain why the number $N$ of solutions of the congruence $c_1 x_1^{k_1} + \cdots + c_m x_m^{k_m} \equiv c \pmod p$ is
$$N = \frac{1}{p}\sum_{a=1}^{p} e(-ac/p)\prod_{j=1}^{m} G_{k_j}(ac_j)$$
   where $G_k$ is defined as in Exercise 2.
   (b) Suppose that $c = 0$ but that $p$ does not divide any of the numbers $c_j$. Show that $|N - p^{m-1}| \le Cp^{m/2}$ where $C = \prod_{j=1}^{m}((k_j, p-1) - 1)$.
   (c) Suppose that $c \not\equiv 0 \pmod p$ and that for all $j$, $c_j \not\equiv 0 \pmod p$. Show that $|N - p^{m-1}| \le Cp^{(m-1)/2}$ where $C$ is defined as above.
9. (Mattics 1984) Suppose that $h$ has order $(p-1)/k$ modulo $p$. Show that
$$\left|\sum_{m=1}^{p-1} e\left(\frac{h^m}{p}\right)\right| \le 1 + (k-1)\sqrt{p}.$$
10. Let $\chi_1$ and $\chi_2$ be primitive characters (mod $q$).

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(a) Show that if $(a, q) = 1$, then

$$\sum_{n=1}^{q} \chi_1(n)\chi_2(a-n) = \chi_1\chi_2(a)q\frac{\tau(\overline{\chi}_1\overline{\chi}_2)}{\tau(\overline{\chi}_1)\tau(\overline{\chi}_2)}.$$

(b) Show that if $\chi_1\chi_2$ is primitive, then

$$\sum_{n=1}^{q} \chi_1(n)\chi_2(a-n) = \chi_1\chi_2(a)\frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)} \tag{9.10}$$

for all $a$.

When $a = 1$, the sum (9.10) is known as the *Jacobi sum* $J(\chi_1, \chi_2)$. In the same way that the Gauss sum is analogous to the gamma function, the Jacobi sum (and its evaluation in terms of Gauss sums) is analogous to the beta function

$$B(\alpha, \beta) = \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\,dx = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}.$$

11. Let $C$ be the smallest field that contains the field $\mathbb{Q}$ of rational numbers and is closed under square roots. Thus $C$ is the set of complex numbers that are constructible by ruler-and-compass. We show that if $p$ is of the form $p = 2^k + 1$, then $\zeta = e(1/p) \in C$, which is to say that a regular $p$-gon can be constructed.
    (a) Let $p$ be any prime, and $\chi$ any non-principal character modulo $p$. Explain why

$$\tau(\chi)^2 \sum_{n=1}^{p} \overline{\chi}(n)\overline{\chi}(1-n) = p\tau(\chi^2).$$

    (b) From now on assume that $p$ is of the form $p = 2^k + 1$. Explain why $\chi^{2^k} = \chi_0$ for any character modulo $p$, and deduce that $\chi(n) \in C$ for all $\chi$ and all integers $n$.
    (c) Deduce that if $\tau(\chi^2) \in C$, then $\tau(\chi) \in C$.
    (d) Suppose that $\chi$ has order $2^r$. Show successively that the numbers

$$-1 = \tau(\chi^{2^r}),\ \tau(\chi^{2^{r-1}}), \ldots, \tau(\chi^2),\ \tau(\chi)$$

lie in $C$.
    (e) Explain why $\sum_\chi \tau(\chi) = (p-1)\zeta$.
    (f) (Gauss) If $p = 2^k + 1$, then $\zeta \in C$.
12. Let $\chi$ be a character modulo $p$ and put $J(\chi) = \sum_{n=1}^{p} \chi(n)\chi(1-n)$.
    (a) Show that if $\chi^2 \neq \chi_0$, then $|J(\chi)| = \sqrt{p}$.
    (b) Suppose that $p \equiv 1 \pmod 4$. Show that there is a quartic character $\chi$ modulo $p$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(c) Show that if $\chi$ is a quartic character, then $J(\chi)$ is a Gaussian integer. That is, $J(\chi) = a + ib$ where $a$ and $b$ are rational integers.

(d) Deduce that $a^2 + b^2 = p$.

13. (a) Write

$$|\tau(\chi)|^2 = \sum_{m=1}^{q} \chi(m)e(m/q) \sum_{n=1}^{q} \overline{\chi}(n)e(-n/q),$$

and in the second sum replace $n$ by $mn$ where $(m, q) = 1$, to see that the above is

$$= \sum_{n=1}^{q} \overline{\chi}(n)c_q(n-1).$$

(b) Use Theorem 4.1 to show that the above is

$$= \sum_{d|q} d\mu(q/d) \sum_{\substack{n=1 \\ n\equiv 1 \pmod d}}^{q} \overline{\chi}(n).$$

(c) Use Theorem 9.4 to show that if $\chi$ is primitive, then $|\tau(\chi)| = \sqrt{q}$.

## 9.3 Quadratic characters

A character is *quadratic* if it has order 2 in the group of characters modulo $q$. That is, the character takes on only the values $-1$, 0, and 1, with at least one $-1$. Similarly, a character is *real* if all its values are real. Hence a real character is either the principal character or a quadratic character. The Legendre symbol $\left(\frac{n}{p}\right)_L$ is a primitive quadratic character modulo p, and further quadratic characters arise from the Jacobi and Kronecker symbols. We now determine all quadratic characters modulo $q$. If $\chi$ is a character modulo $q$ induced by the primitive character $\chi^\star$ modulo $d$, $d \mid q$, then $\chi$ is quadratic if and only if $\chi^\star$ is quadratic. Hence it suffices to determine the primitive quadratic characters.

Suppose that $\chi$ is a character modulo $q$, that $q = q_1q_2$, $(q_1, q_2) = 1$, $\chi = \chi_1\chi_2$ as in Lemma 9.3. By the Chinese Remainder Theorem we see that $\chi$ is a real character if and only if both $\chi_1$ and $\chi_2$ are real characters. Hence by Lemma 9.3, $\chi$ is a primitive quadratic character if and only if $\chi_1$ and $\chi_2$ are. Thus it suffices to determine the primitive quadratic characters modulo a prime power.

In Section 5.2 we saw that a character $\chi$ modulo $p$ may be written in the form $\chi(n) = e(k \text{ ind } n/(p-1))$. Such a character is primitive provided that it is non-principal, which is to say that $k \not\equiv 0 \pmod{p-1}$. Similarly, $\chi$ is quadratic if and only if the least denominator of the fraction $k/(p-1)$ is 2. If

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

$p = 2$ then this is impossible, but for $p > 2$ this is equivalent to the condition $k \equiv (p-1)/2 \pmod{p-1}$. Thus there is no quadratic character modulo 2, but for each odd prime $p$ there is a unique quadratic character, given by the Legendre symbol.

Now suppose that $p$ is an odd prime and that $q = p^m$ with $m > 1$. We have seen that a character $\chi$ modulo such a $q$ is of the form $\chi(n) = e(k \operatorname{ind} n/\varphi(q))$, and that $\chi$ is primitive if and only if $p \nmid k$. This character is quadratic only when $k \equiv \varphi(q)/2 \pmod{\varphi(q)}$, so there is a unique quadratic character modulo $q$, but it is not primitive because $p \mid k$ for this $k$. That is, the only quadratic character modulo $p^m$ is induced by the primitive quadratic character modulo $p$.

Finally, suppose that $q = 2^m$. For the modulus 2 there is only the principal character, but for $q = 4$ we have a primitive quadratic character

$$\chi_1(n) = \begin{cases} (-1)^{(n-1)/2} & (n \text{ odd}), \\ 0 & (n \text{ even}). \end{cases}$$

For $m > 2$ we write $\chi((-1)^\mu 5^\nu) = e(j\mu/2 + k\nu/2^{m-2})$, and we see that this character is real if and only if $2^{m-3} \mid k$. However, the character is primitive if and only if $k$ is odd, so primitive quadratic characters arise only when $m = 3$, and for this modulus we have two different characters (corresponding to $j = 0$, $j = 1$). Let $\chi_2((-1)^\mu 5^\nu) = e(\nu/2)$. That is, $\chi_2(n) = (-1)^{(n^2-1)/8}$. Then the characters modulo 8 are $\chi_0$, $\chi_1$, $\chi_2$, and $\chi_1\chi_2$, of which the latter two are primitive.

We next show that the primitive quadratic characters arise precisely from the Kronecker symbol $\left(\frac{d}{n}\right)_K$. We say that $d$ is a *quadratic discriminant* if either

(a) $d \equiv 1 \pmod 4$ and $d$ is square-free
or
(b) $4 \mid d$, $d/4 \equiv 2$ or $3 \pmod 4$, and $d/4$ is square-free.

For each quadratic discriminant $d$ we define the Kronecker symbol $\left(\frac{d}{n}\right)_K$ by the following relations:

(i) $\left(\frac{d}{p}\right)_K = 0$ when $p \mid d$;

(ii) $\left(\frac{d}{2}\right)_K = \begin{cases} 1 & \text{when } d \equiv 1 \pmod 8, \\ -1 & \text{when } d \equiv 5 \pmod 8; \end{cases}$

(iii) $\left(\frac{d}{p}\right)_K = \left(\frac{d}{p}\right)_L$, the Legendre symbol, when $p > 2$;

(iv) $\left(\frac{d}{-1}\right)_K = \begin{cases} 1 & \text{when } d > 0, \\ -1 & \text{when } d < 0; \end{cases}$

(v) $\left(\frac{d}{n}\right)_K$ is a totally multiplicative function of $n$.

It is not immediately apparent that this definition of the Kronecker symbol gives rise to a character, but we now show that this is the case.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

**Theorem 9.13** *Let $d$ be a quadratic discriminant. Then $\chi_d(n) = \left(\frac{d}{n}\right)_K$ is a primitive quadratic character modulo $|d|$, and every primitive quadratic character is given uniquely in this way.*

*Proof* It is easy to see that $\left(\frac{-4}{n}\right)_K$ is the primitive quadratic character modulo 4. Similarly, $\left(\frac{8}{n}\right)_K$ and $\left(\frac{-8}{n}\right)_K$ are the primitive quadratic characters modulo 8.

Suppose that $p$ is a prime, $p \equiv 1 \pmod 4$. We show that $\left(\frac{p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ for all $n$. To see this, note that if $q$ is an odd prime, then by (iii) and quadratic reciprocity, $\left(\frac{p}{q}\right)_K = \left(\frac{p}{q}\right)_L = \left(\frac{q}{p}\right)_L$. Also, $\left(\frac{p}{2}\right)_K = (-1)^{(p^2-1)/8} = \left(\frac{2}{p}\right)_L$, and $\left(\frac{p}{-1}\right)_K = 1 = \left(\frac{-1}{p}\right)_L$. Since these two functions agree on all primes, and also on $-1$, and both are totally multiplicative, it follows that $\left(\frac{p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ for all integers $n$.

Suppose that $p$ is a prime, $p \equiv 3 \pmod 4$. We show that $\left(\frac{-p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ for all $n$. To see this, note that if $q$ is an odd prime, then by (iii) and quadratic reciprocity, $\left(\frac{-p}{q}\right)_K = \left(\frac{-p}{q}\right)_L = \left(\frac{q}{p}\right)_L$. Also, $\left(\frac{-p}{2}\right)_K = (-1)^{((-p)^2-1)/8} = (-1)^{(p^2-1)/8} = \left(\frac{2}{p}\right)_L$, and $\left(\frac{-p}{-1}\right)_K = -1 = \left(\frac{-1}{p}\right)_L$. Since these two functions agree on all primes, and also on $-1$, and both are totally multiplicative, it follows that $\left(\frac{-p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ for all integers $n$.

Suppose next that $d_1$ and $d_2$ are quadratic discriminants with $(d_1, d_2) = 1$. Put $d = d_1 d_2$. Supposing that $\left(\frac{d_i}{n}\right)_K$ is a primitive quadratic character modulo $|d_i|$ for $i = 1, 2$, we shall show that $\left(\frac{d}{n}\right)_K$ is a primitive quadratic character modulo $|d|$. If $q$ is an odd prime, then by (iii), $\left(\frac{d}{q}\right)_K = \left(\frac{d}{q}\right)_L = \left(\frac{d_1}{q}\right)_L \left(\frac{d_2}{q}\right)_L = \left(\frac{d_1}{q}\right)_K \left(\frac{d_2}{q}\right)_K$. Also, by (ii) we see that $\left(\frac{d}{2}\right)_K = \left(\frac{d_1}{2}\right)_K \left(\frac{d_2}{2}\right)_K$, and by (iv) that $\left(\frac{d}{-1}\right)_K = \left(\frac{d_1}{-1}\right)_K \left(\frac{d_2}{-1}\right)_K$. Since $\left(\frac{d}{n}\right)_K = \left(\frac{d_1}{n}\right)_K \left(\frac{d_2}{n}\right)_K$ when $n$ is a prime or $n = -1$, and since both sides are totally multiplicative functions, it follows that this identity holds for all integers $n$. Hence by Lemma 9.3, $\left(\frac{d}{n}\right)_K$ is a primitive character modulo $|d|$.

This allows us to account for all primitive quadratic characters, so the proof is complete. □

Since the Kronecker symbol and Legendre symbol agree whenever both are defined, we may omit the subscripts. The same remark applies to the Jacobi symbol $\left(\frac{n}{q}\right)_J$, which for odd positive $q = p_1 p_2 \cdots p_r$ is defined to be $\left(\frac{n}{q}\right)_J = \prod_{i=1}^r \left(\frac{n}{p_i}\right)_L$. Sometimes we let $\chi_d(n)$ denote the character $\left(\frac{d}{n}\right)$.

A character $\chi$ modulo $q$ is an even function, $\chi(-n) = \chi(n)$, if $\chi(-1) = 1$; for the primitive quadratic character $\chi_d$ this occurs if $d > 0$. In the case of the Legendre symbol, if $p \equiv 1 \pmod 4$, then $\left(\frac{n}{p}\right)_L = \chi_p(n)$ is even. Similarly, $\chi$ is odd, $\chi(-n) = -\chi(n)$, if $\chi(-1) = -1$. For $\chi_d$ this occurs when $d < 0$. For the Legendre symbol, if $p \equiv 3 \pmod 4$, then $\left(\frac{n}{p}\right)_L = \chi_{-p}(n)$ is odd.

We have taken the quadratic reciprocity law for the Legendre symbol for granted, since it is treated in a variety of ways in elementary texts. In Exercise 9.3.6 below we outline a proof of quadratic reciprocity that is unusual that

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

it applies directly to the Jacobi symbol, without first being restricted to the Legendre symbol. For future purposes it is convenient to formulate quadratic reciprocity also for the Kronecker symbol.

**Theorem 9.14** *Suppose that $d_1$ and $d_2$ are relatively prime quadratic discriminants. Then*

$$\left(\frac{d_1}{d_2}\right)\left(\frac{d_2}{d_1}\right) = \varepsilon(d_1, d_2) \tag{9.11}$$

*where $\varepsilon(d_1, d_2) = 1$ if $d_1 > 0$ or $d_2 > 0$, and $\varepsilon(d_1, d_2) = -1$ if $d_1 < 0$ and $d_2 < 0$.*

For odd $n$ let $m^2$ be the largest square dividing $n$. Then there is a unique choice of sign and a unique quadratic discriminant $d_2$ such that $n = \pm m^2 d_2$, and then if $(n, d_1) = 1$ the above can be applied to express $\left(\frac{d_1}{n}\right)$ in terms of $\left(\frac{d_2}{d_1}\right)$. If $n$ is even, then $4n = m^2 d_2$ for unique $m$ and quadratic discriminant $d_2$, so if $(n, d_1) = 1$ we can again express $\left(\frac{d_1}{n}\right)$ in terms of $\left(\frac{d_2}{d_1}\right)$.

*Proof* Suppose that $d_1 = p \equiv 1 \pmod 4$. Then

$$\left(\frac{p}{d_2}\right)_K = \left(\frac{d_2}{p}\right)_L = \left(\frac{d_2}{p}\right)_K,$$

so (9.11) holds in this case. Next suppose that $d_1 = -p$ where $p \equiv 3 \pmod 4$. Then

$$\left(\frac{-p}{d_2}\right)_K = \left(\frac{d_2}{p}\right)_L = \left(\frac{d_2}{-1}\right)_K \left(\frac{d_2}{-p}\right)_K,$$

so (9.11) holds in this case also. Next consider the case $d_1 = -4$. Then $d_2$ is odd, and hence $d_2 \equiv 1 \pmod 4$, so that $\left(\frac{-4}{d_2}\right)_K = \left(\frac{-4}{1}\right)_K = 1$, while $\left(\frac{d_2}{-4}\right)_K = \left(\frac{d_2}{-1}\right)_K$, and (9.11) again holds. If $d_1 = 8$ then $d_2$ is odd and $\left(\frac{8}{d_2}\right)_K = (-1)^{(d_2^2-1)/8} = \left(\frac{d_2}{8}\right)_K$, so (9.11) holds. Similarly, if $d_2$ is odd, then $\left(\frac{-8}{d_2}\right)_K = \left(\frac{-4}{d_2}\right)_K \left(\frac{8}{d_2}\right)_K = \left(\frac{8}{d_2}\right)_K = \left(\frac{8}{d_2}\right)_K = \left(\frac{d_2}{-1}\right)_K \left(\frac{d_2}{-8}\right)_K$, so again (9.11) holds.

Now let $d_1$, $d_2$ and $d$ be pairwise coprime quadratic discriminants. Then

$$\left(\frac{d_1 d_2}{d}\right)_K = \left(\frac{d_1}{d}\right)_K \left(\frac{d_2}{d}\right)_K.$$

Suppose that (9.11) holds for the pair $d_1, d$, and also for the pair $d_2, d$. Then the above is

$$= \varepsilon(d_1, d)\left(\frac{d}{d_1}\right)_K \varepsilon(d_2, d)\left(\frac{d}{d_2}\right)_K$$
$$= \varepsilon(d_1, d)\varepsilon(d_2, d)\left(\frac{d}{d_1 d_2}\right)_K.$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

But $\varepsilon(d_1, d)\varepsilon(d_2, d) = \varepsilon(d_1 d_2, d)$, so it follows that (9.11) holds also for the pair $d_1 d_2, d$. Since all quadratic discriminants can be constructed as the product of smaller quadratic discriminants, or by appealing to the special cases already considered, it follows now that (9.11) holds for all quadratic discriminants. □

Let $\chi$ be a character modulo $q$. By means of Theorems 9.7 and 9.10 we can describe $|\tau(\chi)|$. By Theorem 9.5 we may also relate the argument of $\tau(\chi)$ to that of $\tau(\overline{\chi})$, but otherwise there is little in general that we can say about the argument of $\tau(\chi)$. However, in the special case of quadratic characters, a striking phenomenon arises, which was first noted and established by Gauss. Suppose that $\chi_d$ is a primitive quadratic character. Then $\overline{\chi}_d = \chi_d$, so by multiplying both sides of (9.7) by $\tau(\chi_d)$, and using Theorem 9.7, we see that $\tau(\chi_d)^2 = \chi_d(-1)|d| = d$. Thus $\tau(\chi_d) = \pm\sqrt{d}$ if $d > 0$ and $\tau(\chi_d) = \pm i\sqrt{-d}$ if $d < 0$. We show below that in both cases it is always the positive sign that occurs. We begin with the following fundamental result.

**Theorem 9.15** *Let*

$$S(a, q) = \sum_{n=1}^{q} e\left(\frac{an^2}{2q}\right).$$

*If $a$ and $q$ are positive integers and at least one of them is even, then*

$$S(a, q) = \overline{S(q, a)}e(1/8)\sqrt{q/a}.$$

*Proof* We apply the Poisson summation formula, in the form of Theorem D.3, to the function $f(x) = e(ax^2/(2q))$ for $1/2 < x < q + 1/2$, with $f(x) = 0$ otherwise. Thus

$$S(a, q) = \sum_n f(n) = \lim_{K\to\infty} \sum_{k=-K}^{K} \widehat{f}(k)$$

where

$$\widehat{f}(k) = \int_{1/2}^{q+1/2} e(ax^2/(2q) - kx)\, dx.$$

We complete the square by writing

$$\frac{ax^2}{2q} - kx = \frac{a}{2q}(x - kq/a)^2 - \frac{k^2 q}{2a},$$

and make the change of variable $u = (x - kq/a)/q$, to see that

$$\widehat{f}(k) = qe(-k^2 q/(2a)) \int_{1/(2q)-k/a}^{1/(2q)+1-k/a} e(aqu^2/2)\, du.$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

By integrating by parts we see that

$$\widehat{f}(k) \ll_{a,q} 1/(|k|+1).$$

Since at least one of $a$ and $q$ is even, if $k \equiv r \pmod a$ then $qk^2 \equiv qr^2 \pmod{2a}$. Thus if we write $k = am + r$, then

$$\sum_{k=-K}^{K} \widehat{f}(k) = q\left(\sum_{r=1}^{a} e\left(\frac{-qr^2}{2a}\right)\right)\left(\sum_{m=-K/a}^{K/a} \int_{1/(2q)-m-r/a}^{1/(2q)+1-m-r/a} e(aqu^2/2)\,du\right) + O_{q,a}(1/K).$$

Here the integrals may be combined to form one integral, which, as $K$ tends to infinity tends to $I(aq/2)$ where $I(c) = \int_{-\infty}^{\infty} e(cu^2)\,du$. This is a conditionally convergent improper Riemann integral, but it is not necessary to evaluate this symmetrically as $\lim_{U\to\infty} \int_{-U}^{U}$, since $\int_U^{\infty} e(cu^2)\,du \ll 1/U$, by integration by parts. Thus we have shown that

$$S(a,q) = q\overline{S(q,a)}I(aq/2).$$

We take $a = 2$ and $q = 1$, and note that $S(2,1) = 1$ and $S(1,2) = 1+i$. Hence $I(1) = 1/(1-i) = e(1/8)/\sqrt{2}$. By a linear change of variables it is clear that if $c > 0$ then $I(c) = I(1)/\sqrt{c}$. On combining this information in the above, we obtain the stated identity. □

By taking $a = 2$ we immediately obtain

**Corollary 9.16** (Gauss) *For any positive integer $q$,*

$$\sum_{n=1}^{q} e(n^2/q) = q^{1/2}\frac{1+i^{-q}}{1+i^{-1}} = \begin{cases} q^{1/2} & \text{if } q \equiv 1 \pmod 4, \\ 0 & \text{if } q \equiv 2 \pmod 4, \\ iq^{1/2} & \text{if } q \equiv 3 \pmod 4, \\ (1+i)q^{1/2} & \text{if } q \equiv 0 \pmod 4. \end{cases}$$

This in turn enables us to reach our goal.

**Theorem 9.17** *Let $\chi_d(n) = \left(\frac{d}{n}\right)$ be a primitive quadratic character. If $d > 0$, then $\tau(\chi_d) = \sqrt{d}$. If $d < 0$ then $\tau(\chi_d) = i\sqrt{-d}$.*

In the special case of the Legendre symbol, if we write $\tau_p = \sum_{n=1}^{p} \left(\frac{n}{p}\right)e(n/p)$, then this asserts that $\tau_p = \sqrt{p}$ for $p \equiv 1 \pmod 4$, while $\tau_p = i\sqrt{p}$ for $p \equiv 3 \pmod 4$.

*Proof* As in some of the preceding proofs, we establish the identities when the modulus is an odd prime or power of 2, and then write $d = d_1 d_2$ to extend to the general primitive quadratic character.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

Let

$$G(a,q)=\sum_{x=1}^{q} e\left(\frac{ax^2}{q}\right). \tag{9.12}$$

If $p$ is an odd prime, then the number of solutions of the congruence $x^2 \equiv n \pmod p$ is $1+\left(\frac{n}{p}\right)_L$, so $G(a,p)=\sum_{n=1}^{p}\left(1+\left(\frac{n}{p}\right)\right)e(an/p)$. Thus if $p \nmid a$, then

$$G(a,p)=\sum_{n=1}^{p}\left(\frac{n}{p}\right)e(an/p). \tag{9.13}$$

Suppose that $p \equiv 1 \pmod 4$. Then from the above we see that $\tau(\chi_p)=G(1,p)$, and then by taking $q=p$ in Corollary 9.16 it follows that $G(1,p)=\sqrt{p}$ in this case.

Now suppose that $p \equiv 3 \pmod 4$. Then from the above we see that $\tau(\chi_{-p})=G(1,p)$, and then by taking $q=p$ in Corollary 9.16 it follows that $G(1,p)=i\sqrt{p}$ in this case.

Clearly $\tau(\chi_{-4})=e(1/4)-e(3/4)=2i, \tau(\chi_8)=e(1/8)-e(3/8)-e(5/8)+e(7/8)=\sqrt{8}$, and $\tau(\chi_{-8})=e(1/8)+e(3/8)-e(5/8)-e(7/8)=i\sqrt{8}$. Thus we have the stated result when $d$ is a power of 2.

Next suppose that $d=d_1d_2$ where $d_1$ and $d_2$ are quadratic discriminants and $(d_1,d_2)=1$. Then by Theorem 9.6, $\tau(\chi_d)=\tau(\chi_{d1})\tau(\chi_{d2})\chi_{d1}(|d_2|)\chi_{d_2}(|d_1|)$. By considering the possible combinations of signs of $d_1$ and of $d_2$ we find that $\chi_{d_1}(|d_2|)\chi_{d_2}(|d_1|)=\chi_{d_1}(d_2)\chi_{d_2}(d_1)$ in all cases. This product is $\varepsilon(d_1,d_2)$ in the notation of Theorem 9.14. That is,

$$\tau(\chi_d)=\varepsilon(d_1,d_2)\tau(\chi_{d_1})\tau(\chi_{d_2}).$$

Thus if $\tau(\chi_{d_1})$ and $\tau(\chi_{d_2})$ have the asserted values, then so also does $\tau(\chi_d)$. Since every primitive quadratic character can be constructed this way, the proof is complete. □

### 9.3.1 Exercises

1. (a) Show that if $p>2$ and $p \nmid b$, then

$$\sum_{n=1}^{p}\left(\frac{n}{p}\right)\left(\frac{n+b}{p}\right)=-1.$$

(b) Suppose that $p>2$ and that $p \nmid d$. Explain why

$$\sum_{x=1}^{p}\left(\frac{x^2-d}{p}\right)=\sum_{n=1}^{p}\left(1+\left(\frac{n}{p}\right)\right)\left(\frac{n-d}{p}\right),$$

and deduce that this sum is $-1$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(c) Put $d = b^2 - 4ac$, and suppose that $p > 2$, $p \nmid d$. Show that

$$\sum_{x=1}^{p} \left( \frac{ax^2 + bx + c}{p} \right) = \left( \frac{a}{p} \right).$$

2. Let $p$ be a prime, $p \equiv 1 \pmod 4$, and let $\mathcal{N}$ be a set of $Z$ residue classes modulo $p$.
   (a) Explain why

$$\sum_{m \in \mathcal{N}} \sum_{n \in \mathcal{N}} \left( \frac{m-n}{p} \right) = \frac{1}{\sqrt{p}} \sum_{a=1}^{p} \left( \frac{a}{p} \right) \Big| \sum_{n \in \mathcal{N}} e(an/p) \Big|^2.$$

   (b) Suppose that $\left(\frac{m-n}{p}\right) = 1$ whenever $m \in \mathcal{N}$, $n \in \mathcal{N}$, and $m \neq n$. Show that $Z \leq \sqrt{p}$.
3. Put $f_{\boldsymbol{a}}(r) = r^2 + a_1 r + a_0$ where $\boldsymbol{a} = (a_0, a_1)$. Show that if $r_1, r_2, r_3$ are distinct modulo $p$, then

$$\sum_{a_0=1}^{p} \sum_{a_1=1}^{p} \left( \frac{f_{\boldsymbol{a}}(r_1)}{p} \right) \left( \frac{f_{\boldsymbol{a}}(r_2)}{p} \right) \left( \frac{f_{\boldsymbol{a}}(r_3)}{p} \right) = p.$$

4. We used Corollary 9.16 to determine the sign of $\tau(\chi_{\pm p})$, and then used quadratic reciprocity to determine the sign of $\tau(\chi_d)$ for the general quadratic discriminant $d$. We now show that quadratic reciprocity for the Legendre symbol can be derived from Theorem 9.15 (mainly Corollary 9.16). Let $G(a, q) = \sum_{n=1}^{q} e(an^2/q)$.
   (a) Suppose that $p$ is an odd prime. Explain why

$$G(a, p) = \left( \frac{a}{p} \right)_L \sum_{n=1}^{p} \left( \frac{n}{p} \right) e(n/p)$$

   when $(a, p) = 1$.
   (b) Suppose that $(q_1, q_2) = 1$. By writing $n$ modulo $q_1 q_2$ in the form $n = n_1 q_2 + n_2 q_1$, show that $G(a, q_1 q_2) = G(aq_2, q_1) G(aq_1, q_2)$.
   (c) Let $p$ and $q$ denote odd primes. Show that

$$G(1, pq) = \left( \frac{p}{q} \right)_L \left( \frac{q}{p} \right)_L G(1, p) G(1, q),$$

   and use Corollary 9.16 to show that

$$\left( \frac{p}{q} \right)_L \left( \frac{q}{p} \right)_L = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

   (d) By taking $a = -1$ in (a), and using Corollary 9.16, show that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
   (e) By taking $a = 4$ in Theorem 9.15, show that $\left(\frac{2}{p}\right)_L = (-1)^{(p^2-1)/8}$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(f) Suppose that $p$ is an odd prime, and $k$ is an integer, $k \geq 2$. Show that $G(a, p^k) = pG(a, p^{k-2})$.

5. Let $\mathcal{L}_1$ denote the contour $z = u$, $-\infty < u < \infty$ in the complex plane, let $\mathcal{L}_2$ denote the contour $z = (1+i)u$, $-\infty < u < \infty$, and let $I(c) = \int_{-\infty}^{\infty} e(cu^2)\,du$, as in the proof of Theorem 9.15.
   (a) Note that $I(c) = \int_{\mathcal{L}_1} e^{2\pi i c z^2}\,dz$.
   (b) Explain why $\int_{\mathcal{L}_1} e^{2\pi i c z^2}\,dz = \int_{\mathcal{L}_2} e^{2\pi i c z^2}\,dz$.
   (c) Show that

$$\int_{\mathcal{L}_2} e^{2\pi i c z^2}\,dz = (1+i)\int_{-\infty}^{\infty} e^{-4\pi c u^2}\,du = \frac{1+i}{2\sqrt{\pi c}}\int_{-\infty}^{\infty} e^{-v^2}\,dv = \frac{1+i}{2\sqrt{c}}.$$

   (d) Thus give a proof, independent of that found in the proof of Theorem 9.15, that

$$\int_{-\infty}^{\infty} e(cu^2)\,du = \frac{1}{(1-i)\sqrt{c}}.$$

6. Quadratic reciprocity à la Conway (1997, pp. 127–133). If $(a, n) = 1$ and $n$ is an odd positive integer, then we define the *Zolotarev symbol* (not a standard term) $\left(\frac{a}{n}\right)_Z$ to be 1 if the map $x \mapsto ax$ is an even permutation of a complete residue system modulo $n$, and $\left(\frac{a}{n}\right)_Z = -1$ if it is odd.
   (a) Compute the decomposition of the permutation $x \mapsto 7x \pmod{15}$ into disjoint cycles, and thus show that $\left(\frac{7}{15}\right)_Z = -1$.
   (b) Suppose that $p$ is an odd prime and that $a$ has order $h$ modulo $p$. Show that the map $x \mapsto ax \pmod p$ consists of one 1-cycle (0) and $(p-1)/h$ $h$-cycles. Deduce that $\left(\frac{a}{p}\right)_Z = (-1)^{(p-1)/h}$.
   (c) Continue in the same notation, and show that $(p-1)/h$ is even if and only if $a^{(p-1)/2} \equiv 1 \pmod p$. Deduce that $\left(\frac{a}{p}\right)_Z = \left(\frac{a}{p}\right)_L$.
   (d) If $n$ is odd and positive, then the permutation $x \mapsto -x \pmod n$ consists of one 1-cycle and $(n-1)/2$ 2-cycles of the form $(x\ -x)$. Hence deduce that $\left(\frac{-1}{n}\right)_Z = (-1)^{(n-1)/2}$.
   (e) If $(ab, n) = 1$, then the map $x \mapsto abx \pmod n$ is the composition of the map $x \mapsto ax \pmod n$ and the map $x \mapsto bx \pmod n$. Deduce that $\left(\frac{ab}{n}\right)_Z = \left(\frac{a}{n}\right)_Z\left(\frac{b}{n}\right)_Z$.
   (f) Let $p$ be a prime, $p > 2$, and let $g$ be a primitive root of $p$. By (b) with $h = p-1$, deduce that $\left(\frac{g}{p}\right)_Z = -1$. Then by (e) deduce that $\left(\frac{g^k}{p}\right)_Z = (-1)^k$, and hence give a second proof of (c).
   (g) Suppose that $n$ is odd and positive, and that $(a, n) = 1$. Let

$$\mathcal{P} = \{1, 2, \ldots, (n-1)/2\}, \qquad \mathcal{N} = \{-1, -2, \ldots, -(n-1)/2\}.$$

   Let $K$ be the number of $k \in \mathcal{P}$ such that $ak \in \mathcal{N} \pmod n$. Put $\varepsilon_k = 1$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

if $k$ and $ak$ lie in the same subset, otherwise put $\varepsilon_k = -1$. Note that $\varepsilon_k = \varepsilon_{-k}$. Let $\pi^+$ be the permutation that leaves $\mathcal{N}$ fixed and maps $\mathcal{P}$ to itself by the formula $k \mapsto \varepsilon_k ak \pmod n$. Let $\pi^-$ be the map that leaves $\mathcal{P}$ fixed and maps $\mathcal{N}$ to itself by the formula $k \mapsto \varepsilon_k ak \pmod n$. Finally let $\pi^*$ be the product of those transpositions $(ak\ -ak)$ for which $k \in \mathcal{P}$ and $ak \in \mathcal{N}$. Show that the map $x \mapsto ax \pmod n$ is the permutation $\pi^*\pi^+\pi^-$. Let $\sigma$ be the 'sign change permutation' $x \mapsto -x \pmod n$. Show that $\pi^- = \sigma\pi^+\sigma$. That is, $\pi^+$ and $\pi^-$ are conjugate permutations. They are the same apart from the fact that they operate on different sets. Thus they have the same cycle structure, and hence the same parity. Deduce that $\left(\frac{a}{n}\right)_Z = (-1)^K$.

(h) Suppose that $n$ is odd and positive, that $(a, n) = 1$, and that $a > 0$. Show that $\left(\frac{a}{n}\right)_Z = (-1)^K$ where $K$ is the number of integers lying in the intervals $((r - \frac{1}{2})\frac{n}{a}, \frac{rn}{a})$ for $r = 1, 2, \ldots [a/2]$.

(i) Show that if $a > 0$, $(2a, n) = 1$, $m \equiv n \pmod{4a}$, then $\left(\frac{a}{m}\right)_Z = \left(\frac{a}{n}\right)_Z$.

(j) Show that if $n$ is odd and positive, then $\left(\frac{2}{n}\right)_Z = (-1)^{(p^2-1)/8}$.

(k) Suppose that $m$ and $n$ are odd and positive, and that $m \equiv -n \pmod 4$, say $m + n = 4a$. Justify the following manipulations:

$$\left(\frac{m}{n}\right)_Z = \left(\frac{4a}{n}\right)_Z = \left(\frac{a}{n}\right)_Z = \left(\frac{a}{m}\right)_Z = \left(\frac{4a}{m}\right)_Z = \left(\frac{n}{m}\right)_Z.$$

(l) Suppose that $m$ and $n$ are odd and positive, and that $m \equiv n \pmod 4$, say $m > n$ and $m - n = 4a$. Justify the following manipulations:

$$\left(\frac{m}{n}\right)_Z = \left(\frac{4a}{n}\right)_Z = \left(\frac{a}{n}\right)_Z = \left(\frac{a}{m}\right)_Z = \left(\frac{4a}{m}\right)_Z$$
$$= \left(\frac{-n}{m}\right)_Z = \left(\frac{n}{m}\right)_Z (-1)^{(m-1)/2}.$$

(m) Suppose that $a$ is odd and positive and that $(2a, mn) = 1$. Show that

$$\left(\frac{a}{mn}\right)_Z = \left(\frac{mn}{a}\right)_Z (-1)^{\frac{a-1}{2}\frac{mn-1}{2}} = \left(\frac{m}{a}\right)_Z \left(\frac{n}{a}\right)_Z (-1)^{\frac{a-1}{2}\frac{mn-1}{2}}$$
$$= \left(\frac{a}{m}\right)_Z \left(\frac{a}{n}\right)_Z (-1)^{\frac{a-1}{2}\frac{mn-1}{2} + \frac{a-1}{2}\frac{m-1}{2} + \frac{a-1}{2}\frac{n-1}{2}}.$$

Show that this last exponent is even, so that $\left(\frac{a}{mn}\right)_Z = \left(\frac{a}{m}\right)_Z \left(\frac{a}{n}\right)_Z$ in this case.

(n) Suppose that $a$ is odd and negative and that $(a, mn) = 1$. Use (m) to show that the identity $\left(\frac{a}{mn}\right)_Z = \left(\frac{a}{m}\right)_Z \left(\frac{a}{n}\right)_Z$ holds in this case also. Thus this holds for all odd $a$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(o) Suppose that $a$ is even and that $(a, mn) = 1$. Justify the following manipulations:

$$\left(\frac{a}{mn}\right)_Z = \left(\frac{-a}{mn}\right)_Z (-1)^{\frac{mn-1}{2}} = \left(\frac{mn-a}{mn}\right)_Z (-1)^{\frac{mn-1}{2}}$$
$$= \left(\frac{mn-a}{m}\right)_Z \left(\frac{mn-a}{n}\right)_Z (-1)^{\frac{mn-1}{2}}$$
$$= \left(\frac{-a}{m}\right)_Z \left(\frac{-a}{n}\right)_Z (-1)^{\frac{mn-1}{2}} = \left(\frac{a}{m}\right)_Z \left(\frac{a}{n}\right)_Z (-1)^{\frac{mn-1}{2}+\frac{m-1}{2}+\frac{n-1}{2}}.$$

Show that this last exponent is even, and thus deduce that

$$\left(\frac{a}{mn}\right)_Z = \left(\frac{a}{m}\right)_Z \left(\frac{a}{n}\right)_Z$$

holds in all cases.

(p) Suppose that $(a, m) = 1$ and that $m$ is odd, composite, and square-free. Show that the permutation $x \mapsto ax \pmod m$ of reduced residues modulo $m$ is always even. (Hence it is essential that we used complete residue systems in the above.)

7. Let $p$ be a prime number, $p > 2$. (a) Show that

$$\prod_{k=1}^{p-1} (1 - e(k/p))^{\left(\frac{k}{p}\right)} = \exp(-\tau(\chi_p) L(1, \chi_p))$$

where $\chi_p(n) = \left(\frac{k}{p}\right)$.
Let $\mathcal{R} = \left\{r : 0 < r < p, \left(\frac{r}{p}\right) = 1\right\}, \mathcal{N} = \left\{n : 0 < n < p, \left(\frac{n}{p}\right) = -1\right\}$, and set

$$Q = \frac{\prod_{n\in\mathcal{N}} \sin \pi n/p}{\prod_{r\in\mathcal{R}} \sin \pi r/p}.$$

(b) Show that if $p \equiv 3 \pmod 4$, then $Q = 1$.
(c) Show that if $p \equiv 1 \pmod 4$, then $Q = \exp(\sqrt{p}\, L(1, \chi_p))$.

8. (Chowla & Mordell 1961) Continue with the notation of the preceding problem, let $c$ be chosen, $0 < c < p$, so that $\left(\frac{c}{p}\right) = -1$, and put

$$f(z) = \prod_{r\in\mathcal{R}} \frac{1 - z^{cr}}{1 - z^r} - 1.$$

(a) Show that if $L(1, \chi_p) = 0$, then $f(e(1/p)) = 0$.
(b) Explain why $f$ is a polynomial with integral coefficients.
(c) Show that if $L(1, \chi_p) = 0$, then there exists a polynomial $g \in \mathbb{Z}[z]$ such that $f(z) = g(z)(1 + z + \cdots + z^{p-1})$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(d) By taking $z = 1$ in the above, show that it would follow that $c^{(p-1)/2} \equiv 1 \pmod{p}$.
(e) Explain why $c^{(p-1)/2} \equiv -1 \pmod{p}$; deduce that $L(1, \chi_p) \neq 0$.

## 9.4 Incomplete character sums

Let $\chi$ be a character modulo $q$. We call the sum $\sum_{n=M+1}^{M+N} \chi(n)$ *incomplete* if $N < q$. Such a sum trivially has absolute value at most $N$. We now use our knowledge of Gauss sums to show that if $\chi$ is non-principal, then this sum is $o(N)$ provided that $N$ is not too small compared with $q$. Suppose first that $\chi$ is a primitive character modulo $q$ with $q > 1$. Then by Corollary 9.8,

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

Here the inner sum is a geometric series. We note that

$$\begin{aligned} \sum_{n=M+1}^{M+N} e(n\alpha) &= \frac{e((M+N+1)\alpha) - e((M+1)\alpha)}{e(\alpha) - 1} \\ &= e((2M+N+1)\alpha/2) \frac{\sin \pi N\alpha}{\sin \pi \alpha} \end{aligned} \tag{9.14}$$

if $\alpha$ is not an integer. (If $\alpha \in \mathbb{Z}$, then the sum is $N$.) On combining this with the above, we see that

$$\sum_{n=M+1}^{M+N} \chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) e\left(\frac{a(2M+N+1)}{2q}\right) \frac{\sin \pi aN/q}{\sin \pi a/q}. \tag{9.15}$$

By Theorem 9.7 and the triangle inequality the right-hand side has absolute value

$$< \frac{1}{\sqrt{q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q-1} \frac{1}{\sin \pi a/q}.$$

Here the second half of the range of summation contributes the same amount as the first. Hence it suffices to multiply by 2 and sum over $1 \leq a \leq q/2$. However, if $q$ is odd, then $q/2$ is not an integer and hence the sum is actually over the range $1 \leq a \leq (q-1)/2$, while if $q$ is even, then $4 \mid q$ (since if $q \equiv 2 \pmod 4$, then there is no primitive character modulo $q$), and hence $(q/2, q) > 1$, and so it suffices to sum over $1 \leq a \leq q/2 - 1$ in this case. Hence in either case the

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

expression above is

$$\leq \frac{2}{\sqrt{q}} \sum_{a=1}^{(q-1)/2} \frac{1}{\sin \pi a/q}.$$

The function $f(\alpha) = \sin \pi\alpha$ is concave downward in the interval $[0, 1/2]$, and hence it lies above the chord through the points $(0, 0), (1/2, 1)$. That is, $\sin \pi\alpha \geq 2\alpha$ for $0 \leq \alpha \leq 1/2$. Thus the above is

$$\leq \sqrt{q} \sum_{a=1}^{(q-1)/2} \frac{1}{a} < \sqrt{q} \sum_{a=1}^{(q-1)/2} \log \frac{1 + \frac{1}{2a}}{1 - \frac{1}{2a}} = \sqrt{q} \sum_{a=1}^{(q-1)/2} \log \frac{2a+1}{2a-1} = \sqrt{q} \log q.$$

That is,

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < \sqrt{q} \log q \tag{9.16}$$

when $\chi$ is primitive. We now extend this to imprimitive non-principal characters. Suppose that $\chi$ is induced by $\chi^\star$ modulo $d$. Let $r$ be the product of those primes that divide $q$ but not $d$. Then

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

By the case already treated, we know that the inner sum above has absolute value not exceeding $d^{1/2} \log d$, and hence the given sum has absolute value not more than $2^{\omega(r)} d^{1/2} \log d$. But $2^{\omega(r)} \leq d(r) \ll r^{1/2} \leq (q/d)^{1/2}$, so we have proved

**Theorem 9.18** (The Pólya–Vinogradov inequality) *Let $\chi$ be a non-principal character modulo $q$. Then for any integers $M$ and $N$ with $N > 0$,*

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

In (9.16) we saw that the implicit constant can be taken to be 1 when $\chi$ is primitive. With a little more care it can be seen that the implicit constant

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

can be taken to be 1 for all non-principal characters. The above estimate is important in many contexts, but we confine ourselves to two applications at this point.

**Corollary 9.19** *Let $\chi$ be a non-principal character modulo $p$, and let $n_\chi$ be the least positive integer $n$ such that $\chi(n) \neq 1$. Then $n_\chi \ll_\varepsilon p^{\frac{1}{2\sqrt{e}}+\varepsilon}$.*

*Proof* Suppose that $\chi(n) = 1$ for all $n \leq y$. Then $\chi(n) = 1$ whenever $n$ is composed entirely of primes $q \leq y$. Hence, in the notation of Section 7.1, if $y \leq x < y^2$, then

$$\sum_{n\leq x} \chi(n) = \psi(x, y) + \sum_{y<q\leq x} \chi(q)[x/q]$$

where $q$ denotes a prime. Thus

$$\left|\sum_{n\leq x} \chi(n)\right| \geq \psi(x, y) - \sum_{y<q\leq x} [x/q] = [x] - 2\sum_{y<q\leq x} [x/q]$$
$$= x\left(1 - 2\log\frac{\log x}{\log y}\right) + O\left(\frac{x}{\log x}\right).$$

If $x = p^{1/2}(\log p)^2$, then the sum on the left is $o(x)$, while if $y > x^{1/\sqrt{e}+\varepsilon}$, then the lower bound on the right is $\gg \varepsilon x$. Thus $n_\chi \ll_\varepsilon x^{1/\sqrt{e}+\varepsilon}$. □

**Corollary 9.20** *The number of primitive roots modulo $p$ in the interval $[M + 1, M + N]$ is*

$$\frac{\varphi(p-1)}{p}N + O\big(p^{1/2+\varepsilon}\big).$$

Since the number of primitive roots in an interval of length $p$ is exactly $\varphi(p - 1)$, the above asserts that primitive roots are roughly uniformly distributed into subintervals of length $N$ provided that $N > p^{1/2+\varepsilon}$.

*Proof* Let $q_1, q_2, \ldots, q_r$ be the distinct prime factors of $p - 1$, and put $q = \prod_{i=1}^{r} q_i$. Then $n$ is a primitive root modulo $p$ if and only if $(\operatorname{ind} n, q) = 1$. For $1 \leq i \leq r$ put

$$\chi_i(n) = e\left(\frac{\operatorname{ind} n}{q_i}\right).$$

Then

$$\frac{1}{q_i}\sum_{a=1}^{q_i} \chi_i(n)^a = \begin{cases} 1 & \text{if } q_i \mid \operatorname{ind} n, \\ 0 & \text{otherwise.} \end{cases}$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

Thus

$$\prod_{i=1}^{r}\left(\chi_0(n)-\frac{1}{q_i}\sum_{a_i=1}^{q_i}\chi_i(n)^{a_i}\right)=\begin{cases}1 & \text{if } n \text{ is a primitive root (mod } p),\\ 0 & \text{otherwise.}\end{cases}$$

The left-hand side above is

$$\prod_{i=1}^{r}\left((1-1/q_i)\chi_0(n)-\frac{1}{q_i}\sum_{a_i=1}^{q_i-1}\chi_i^{a_i}(n)\right)=\sum_{d\mid q}\frac{\varphi(q/d)}{q/d}\,\frac{\mu(d)}{d}\sum_{\substack{\chi\\ \operatorname{ord}\chi=d}}\chi(n).$$

Thus the number of primitive roots in the interval $[M+1, M+N]$ is

$$\frac{1}{q}\sum_{d\mid q}\varphi(q/d)\mu(d)\sum_{\substack{\chi\\ \operatorname{ord}\chi=d}}\sum_{n=M+1}^{M+N}\chi(n). \tag{9.17}$$

The only character of order $d=1$ is the principal character $\chi_0$, which gives us the main term

$$\frac{\varphi(q)}{q}((1-1/p)N+O(1))=\frac{\varphi(p-1)}{p}N+O(1).$$

A character of order $d>1$ is non-principal, and for such characters the innermost sum in (9.17) is $\ll p^{1/2}\log p$. Since there are $\varphi(d)$ such characters, the contribution in (9.17) of $d>1$ is

$$\ll\frac{\varphi(q)}{q}p^{1/2}\log p\sum_{d\mid(p-1)}|\mu(d)|\ll 2^{\omega(p-1)}p^{1/2}\log p\ll p^{1/2+\varepsilon}.$$

This gives the stated result. □

Suppose that $\chi$ is a non-principal character modulo $q$. Further insights into the Pólya–Vinogradov inequality may be gained by considering the sum $f_\chi(\alpha)=\sum_{0<n\le q\alpha}\chi(n)$ as a function of the real variable $\alpha$, for $0\le\alpha\le 1$. We extend the domain of $f_\chi(\alpha)$ by periodicity, and compute its Fourier coefficients:

$$\widehat{f}_\chi(k)=\int_0^1 f_\chi(\alpha)e(-k\alpha)\,d\alpha=\sum_{n=1}^{q}\chi(n)\int_{n/q}^{1}e(-k\alpha)\,d\alpha.$$

The nature of this integral depends on whether $k=0$ or not. In the former case we find that

$$\widehat{f}_\chi(0)=\sum_{n=1}^{q}\chi(n)\left(1-\frac{n}{q}\right)=\frac{-1}{q}\sum_{n=1}^{q}n\chi(n),$$

while for $k\neq 0$ we have

$$\widehat{f}_\chi(k)=\sum_{n=1}^{q}\chi(n)\frac{1-e(-kn/q)}{-2\pi ik}=\frac{1}{2\pi ik}\sum_{n=1}^{q}\chi(n)e(-kn/q)=\frac{c_\chi(-k)}{2\pi ik}.$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

It is convenient to restrict to primitive characters, since then $c_\chi(-k) = \overline{\chi}(-k)\tau(\chi)$ by Theorem 9.5. Since $f_\chi(\alpha)$ is a function of bounded variation it follows that

$$f_\chi(\alpha) = \frac{-1}{q}\sum_{n=1}^{q} n\chi(n) + \frac{\tau(\chi)}{2\pi i}\sum_{k\neq 0}\frac{\overline{\chi}(-k)}{k}e(k\alpha) \tag{9.18}$$

at points of continuity of $f_\chi$, with the understanding that the sum is calculated as the limit of the symmetric partial sums $\sum_{-K}^{K}$. If $\chi(-1) = 1$, then $f_\chi(\alpha)$ is an odd function and the contributions of $k$ and of $-k$ can be combined to form a sine series. If $\chi(-1) = -1$, then $f_\chi(\alpha)$ is an even function, and the two terms merge to form a cosine series. In this case it is interesting to note that if we take $\alpha = 0$ then we obtain another proof of (9.9). Among other possible values of $\alpha$ that might be considered, the possibility $\alpha = 1/2$ is particularly striking. If $\chi(-1) = 1$ then $f_\chi(1/2) = 0$ by symmetry, so in continuing we suppose that $\chi(-1) = -1$. Note that if $q$ is odd then $1/2$ is not of the form $n/q$, and hence $f_\chi(\alpha)$ is continuous at $1/2$. On the other hand, there is no primitive character modulo 2 and hence if $q$ is even then $4 \mid q$. In this case we can solve the equation $n/q = 1/2$ by taking $n = q/2$, but then $q/2$ is even, so that $(q/2, q) > 1$, and hence $\chi(q/2) = 0$. Hence $f_\chi(\alpha)$ is continuous at $1/2$ in all cases, and we deduce that

$$\sum_{0<n\leq q/2}\chi(n) = \frac{-1}{q}\sum_{n=1}^{q} n\chi(n) - \frac{\tau(\chi)}{\pi i}\sum_{k=1}^{\infty}\frac{\overline{\chi}(k)}{k}(-1)^k.$$

As we already discovered by taking $\alpha = 0$, the first term on the right is $\tau(\chi)L(1, \overline{\chi})/(\pi i)$. But

$$\sum_{k=1}^{\infty}\frac{\chi(k)(-1)^k}{k^s} = (2^{1-s}\chi(2) - 1)L(s, \chi)$$

for any character $\chi$ and any $s$ with positive real part, so we have proved

**Theorem 9.21** *Let $\chi$ be a primitive character modulo $q$ such that $\chi(-1) = -1$. Then*

$$\sum_{1\leq n\leq q/2}\chi(n) = (2 - \chi(2))\frac{\tau(\chi)}{\pi i}L(1, \overline{\chi}).$$

In the special case that $\chi$ is a quadratic character we know the exact value of the Gauss sum, and hence we can say more.

**Corollary 9.22** *If $d$ is a quadratic discriminant with $d < 0$, then*

$$\sum_{1\leq n\leq |d|/2}\left(\frac{d}{n}\right) > 0.$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511874314.011 Published online by Cambridge University Press

On taking $\alpha = (M+N)/q$ and then $\alpha = M/q$, and differencing, we see that

$$\sum_{n=M+1}^{M+N} \chi(n) = \frac{\tau(\chi)}{2\pi i} \sum_{k\neq 0} \frac{\overline{\chi}(-k)}{k} e(kM/q)(e(kN/q) - 1) + O(1).$$

Since $e(kN/q) - 1 \sim 2\pi i kN/q$ when $|k|$ is small compared with $N/q$, for rough heuristics we think of the above as being approximately

$$\frac{\tau(\chi)N}{q} \sum_{0<|k|\leq N/q} \overline{\chi}(-k) e(kM/q).$$

Here a sum over an interval of length $N$ reflects – approximately – to form a sum over an interval of length $N/q$. Further examples of this sort of phenomenon will emerge when we consider approximate functional equations of $\zeta(s)$ and of $L(s, \chi)$.

The Fourier expansion (9.18) is also useful in deriving quantitative estimates. We know not only that $\mathrm{Var}_{[0,1]} f_\chi = \varphi(q)$, but (by Theorems 2.10 and 3.1) also that this variation is reasonably well distributed in subintervals, in the sense that $\mathrm{Var}_{[\alpha,\beta]} f_\chi \ll \varphi(q)(\beta - \alpha)$ when $\beta - \alpha > q^{-1+\varepsilon}$. We apply Theorem D.2 to $f_\chi(\alpha)$, and divide the range of integration $(0, 1)$ into $K$ intervals of length $1/K$, throughout each of which the integrand has a constant order of magnitude. Thus we see that

$$f_\chi(\alpha) = \frac{-1}{q} \sum_{n=1}^{q} n\chi(n) + \frac{\tau(\chi)}{2\pi i} \sum_{0<|k|\leq K} \frac{\overline{\chi}(-k)}{k} e(k\alpha) + O\left(\frac{\varphi(q)}{K} \log 2K\right) \tag{9.19}$$

for $K \leq q^{1-\varepsilon}$. This can be used to obtain sharper constants in the Pólya–Vinogradov inequality; see Exercise 9.4.9.

We can also show that the estimate provided by the Pólya–Vinogradov inequality is in general not far from the truth.

**Theorem 9.23** *Suppose that $\chi$ is a non-principal character modulo $q$. Then*

$$\max_{M,N} \left| \sum_{n=M+1}^{M+N} \chi(n) \right| \geq \frac{|\tau(\chi)|}{\pi}.$$

*Proof* Clearly

$$\left| \sum_{M=1}^{q} e(M/q) \sum_{n=M+1}^{M+N} \chi(n) \right| \leq \sum_{M=1}^{q} \left| \sum_{n=M+1}^{M+N} \chi(n) \right| \leq q \max_{M} \left| \sum_{n=M+1}^{M+N} \chi(n) \right|.$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511874314.011 Published online by Cambridge University Press

Here the sum on the left is

$$\sum_{n=1}^{N}\sum_{M=1}^{q} e(M/q)\chi(M+n) = \sum_{n=1}^{N} e(-n/q)\sum_{M=1}^{q}\chi(M)e(M/q).$$

By (9.14) this is

$$e\left(\frac{-(N+1)}{2q}\right)\frac{\sin \pi N/q}{\sin \pi/q}\tau(\chi).$$

If $q$ is even, then we may take $N = q/2$, and then the quotient of sines is $= 1/(\sin \pi/q) \geq q/\pi$, while if $q$ is odd, then we may take $N = (q-1)/2$, in which case the quotient of sines is

$$\frac{\cos \frac{\pi}{2q}}{\sin \frac{\pi}{q}} = \frac{1}{2\sin \frac{\pi}{2q}} \geq \frac{q}{\pi}.$$

The stated lower bound now follows by combining these estimates. □

If $\chi$ is primitive modulo $q$, then the lower bound of Theorem 9.23 is $\sqrt{q}/\pi$. Further lower bounds of this nature can be derived by using Parseval's identity (4.4) for the finite Fourier transform; see Exercise 9.4.8. In addition to the lower bound above, which applies to all characters, for a sparse subset of characters we can obtain a better lower bound.

**Theorem 9.24** (Paley) *There is a positive constant $c$ such that*

$$\max_{M,N}\sum_{n=M+1}^{M+N}\left(\frac{d}{n}\right) > c\sqrt{d}\log\log d$$

*for infinitely many positive quadratic discriminants $d$.*

*Proof* Let $\chi$ be a primitive character modulo $q$ such that $\chi(-1) = 1$. By taking $M = k-h-1$ and $N = 2h+1$ in (9.15) we see that

$$\sum_{n=k-h}^{k+h}\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q}\overline{\chi}(a)e(ak/q)\frac{\sin \pi a(2h+1)/q}{\sin \pi a/q}.$$

Let $h$ be the integer closest to $q/3$. Then the sine in the numerator is approximately $\sin 2\pi a/3$ when $a$ is small. We shall choose $\chi$ so that $\chi(a) = \left(\frac{a}{3}\right)_L$ when $a$ is small. Thus these two factors are strongly correlated. We would take $k = 0$ except for the need to dampen the effects of the larger values of $a$. To this end

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

we sum over $k$, for $-K \le k \le K$ and divide by $2K+1$. Thus by (9.14),

$$\frac{1}{2K+1}\sum_{k=-K}^{K}\sum_{n=k-h}^{k+h}\chi(n)$$
$$= \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q}\overline{\chi}(a)\frac{\sin\pi a(2h+1)/q}{\sin\pi a/q}\,\frac{\sin\pi(2K+1)a/q}{(2K+1)\sin\pi a/q}. \qquad (9.20)$$

Here the last factor is approximately 1 if $\|a/q\| \le 1/K$, and decreases as $\|a/q\|$ becomes larger. Thus, despite its complicated appearance, the expression above is effectively

$$\frac{2q}{\pi\tau(\overline{\chi})}\sum_{a=1}^{A}\frac{\overline{\chi}(a)\sin 2\pi a/3}{a}$$

where $A = q/K$. To make this precise we observe that

$$\sin\pi(2h+1)a/q = \sin 2\pi a/3 + O(\|a/q\|)$$

and that

$$\frac{\sin\pi(2K+1)a/q}{(2K+1)\sin\pi a/q} = \begin{cases} 1+O(K^2\|a/q\|^2) & (\|a/q\| \le 1/K), \\ O\big(K^{-1}\|a/q\|^{-1}\big) & (\|a/q\| > 1/K). \end{cases}$$

Thus the right-hand side of (9.20) is

$$= \frac{2}{\tau(\overline{\chi})}\sum_{a=1}^{q/K}\overline{\chi}(a)\left(\frac{1}{\pi a/q}+O\left(\frac{a}{q}\right)\right)\left(\sin 2\pi a/3 + O\left(\frac{a}{q}\right)\right)$$
$$\times\left(1+O\left(\frac{K^2a^2}{q^2}\right)\right)+O\left(\frac{1}{\sqrt{q}}\sum_{q/K<a\le q/2}\frac{q^2}{Ka^2}\right)$$
$$= \frac{2q}{\pi\tau(\overline{\chi})}\sum_{a=1}^{q/K}\frac{\overline{\chi}(a)\sin 2\pi a/3}{a}+O(\sqrt{q}). \qquad (9.21)$$

Now let $y$ be a large parameter, and suppose that

$$q \equiv 5 \pmod 8,$$
$$\left(\frac{q}{p}\right)_L = \left(\frac{p}{3}\right)_L \qquad (3 < p \le y). \qquad (9.22)$$

Thus by the Chinese Remainder Theorem, $q$ is restricted to certain residue classes modulo $Q = 8\prod_{3<p\le y}p$. Now let $q$ be the least positive number that satisfies these constraints. Then $q$ is square-free, and hence $q$ is a quadratic discriminant, so we may take $\chi(n) = \left(\frac{q}{n}\right)_K$. Also, $q < Q$. By the Prime Number Theorem in the form of (6.13) we see that $\log Q = (1+o(1))y$. Let $K$ be the

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

least integer such that $K > q/y$. Then by (9.22), $\chi(a) = \left(\frac{a}{3}\right)_L$ for $1 \le a \le q/K$, $(a, 3) = 1$. Thus $\sum_{1\le a\le u} \chi(a) \sin 2\pi a/3 = u/\sqrt{3} + O(1)$, so the main term in (9.21) is

$$\frac{2\sqrt{q}}{\pi\sqrt{3}}(\log y + O(1)) \ge \left(\frac{2}{\pi\sqrt{3}} + o(1)\right)\sqrt{q}\log\log q.$$

This completes the proof. □

In the two preceding theorems we have seen that the character sum can be large when $N$ is comparable to $q$. For shorter sums we would expect the sum to be smaller, and indeed one would conjecture that if $\chi$ is a non-principal character modulo $q$, then

$$\sum_{n=M+1}^{M+N} \chi(n) \ll_\varepsilon N^{1/2}q^\varepsilon \tag{9.23}$$

for any $\varepsilon > 0$. Although our present knowledge falls far short of this, we now show that some improvement of the Pólya–Vinogradov inequality is possible, at least in some situations. Our approach depends on the Riemann hypothesis for curves over a finite field, in the form of the following character sum estimate, which we derive from the exposition of Schmidt (1976).

**Lemma 9.25** (Weil) *Suppose that $d|(p-1)$ with $d > 1$ and that $\chi$ is a character modulo $p$ of order $d$. Suppose further that $e_j \ge 1$ $(1 \le j \le k)$, that $d \nmid e_j$ for some $j$ with $1 \le j \le k$ and that the $c_1, c_2, \dots, c_k$ are distinct modulo $p$. Then*

$$\left|\sum_{n=1}^{p} \chi\left((n+c_1)^{e_1}(n+c_2)^{e_2}\cdots(n+c_k)^{e_k}\right)\right| \le (k-1)p^{1/2}.$$

*Proof* Let $f(x) = (x+c_1)^{e_1}(x+c_2)^{e_2}\cdots(x+c_k)^{e_k}$. Then, by Lemma 4B of Schmidt (1976), $f(x)$ cannot satisfy $f(x) \equiv g(x)^d \pmod p$ identically where $g$ is a polynomial with integer coefficients. The lemma then follows from Theorem 2$C'$ *ibidem*. □

**Lemma 9.26** *Suppose that $\chi$ is a non-principal character modulo $p$ and let*

$$S_{h,r} = \sum_{n=1}^{p}\left|\sum_{m=1}^{h}\chi(m+n)\right|^{2r}.$$

*Then $S_{h,r} \ll r^{2r}\left(h^r p + h^{2r}p^{1/2}\right)$ for positive integers $r$.*

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

*Proof* Clearly we may suppose that $h \le p$. Let $d$ denote the order of $\chi$. Then $d > 1$ and

$$S_{h,r} = \sum_{m_1,\dots,m_{2r}} \sum_{n=1}^{p} \chi((n+m_1)\cdots(n+m_r)(n+m_{r+1})^{d-1}\cdots(n+m_{2r})^{d-1}).$$

For a given $2r$–tuple $m_1,\dots,m_{2r}$ let $c_1 < c_2 < \cdots < c_k$ be the distinct values of the $m_j$, and let $a_l$ and $b_l$ denote the number of occurrences of $c_l$ amongst the $m_1,\dots,m_r$ and $m_{r+1},\dots,m_{2r}$ respectively. Let $e_l = a_l + (d-1)b_l$. Then $(n+m_1)\cdots(n+m_r)(n+m_{r+1})^{d-1}\cdots(n+m_{2r})^{d-1} = (n+c_1)^{e_1}\cdots(n+c_k)^{e_k}$. Note that $e_1+\cdots+e_k = r + r(d-1) = rd$. If there is an $l$ such that $d \nmid e_l$, then by Lemma 9.25 the sum over $n$ is bounded by $(k-1)p^{\frac{1}{2}}$, and so the total contribution to $S_{h,r}$ from such $2r$–tuples is

$$\le 2rh^{2r}p^{\frac{1}{2}}.$$

On the other hand, if $d|e_l$ for every $l$, then $kd \le e_1 + \cdots e_k = rd$ and so $k \le r$. The number of choices of $m_1,\dots,m_{2r}$ with $m_l \in \{c_1,\dots,c_k\}$ is at most $k^{2r}$ and the number of choices for $c_1,\dots,c_k$ is $\binom{h}{k}$. Thus the total contribution to $S_{h,r}$ from these terms is bounded by

$$\sum_{k\le r} k^{2r}\binom{h}{k}p \ll r^{2r}h^r p.$$

□

Our main result takes the following form.

**Theorem 9.27** (Burgess) *For any odd prime $p$ and any positive integer $r$ we have*

$$\sum_{n=M+1}^{M+N} \chi(n) \ll rN^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\alpha_r}$$

*where $\alpha_r = 1$ when $r = 1$ or $2$ and $\alpha_r = \frac{1}{2r}$ otherwise.*

Suppose that $\delta > 1/4$. If $N > p^{\delta}$, then the bound above is $o(N)$ if $r$ is chosen suitably large in terms of $\delta$. Thus any interval of length $N$ contains both quadratic residues and quadratic non-residues. In addition the reasoning used to derive Corollary 9.19 applies here, so we see that the least positive quadratic non-residue modulo $p$ is $\ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.

*Proof* When $r = 1$ or $N > p^{5/8}$ the bound is weaker than the Pólya–Vinogradov Inequality (Theorem 9.18), and when $r > 2$ and $N > p^{1/2}$ the stated bound is weaker than the case $r = 2$. Also, when $N \le p^{\frac{r+1}{4r}}$ the bound is

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

worse than trivial. Hence we may suppose that

$$p > p_0, \quad r \geq 2, \quad \text{and} \quad p^{\frac{r+1}{4r}} < N \leq \begin{cases} p^{5/8} & \text{when } r = 2, \\ p^{1/2} & \text{when } r > 2. \end{cases} \tag{9.24}$$

Let $S(M, N)$ denote the sum in question. Then

$$S(M, N) = \sum_{n=M+1}^{M+N} \chi(n + ab) + S(M, ab) - S(M + N, ab).$$

Let

$$\mathcal{M}(y) = \max_{\substack{M,N \\ N \leq y}} |S(M, N)|.$$

Then

$$S(M, N) = \sum_{n=M+1}^{M+N} \chi(n + ab) + 2\theta\mathcal{M}(ab)$$

where $|\theta| \leq 1$. We sum this over $a \in [1, A]$ and $b \in [1, B]$. Thus

$$ABS(M, N) = \sum_{n,a,b} \chi(n + ab) + 2AB\theta_1\mathcal{M}(AB).$$

We suppose that

$$A < p \tag{9.25}$$

and then define $\nu(\ell)$ to be the number of pairs $a, n$ with $a \in [1, A]$, $n \in [M + 1, M + N]$ and $n \equiv a\ell \pmod p$. Thus

$$\left|\sum_{n,a,b} \chi(n + ab)\right| = \left|\sum_{\ell=1}^{p} \sum_{\substack{n,a \\ n \equiv a\ell \pmod p}} \chi(a) \sum_{b} \chi(\ell + b)\right|$$
$$\leq \sum_{\ell=1}^{p} \nu(\ell) \left|\sum_{b} \chi(\ell + b)\right|.$$

By Hölder's inequality,

$$\left(\sum_{\ell=1}^{p} \nu(\ell) \left|\sum_{b} \chi(\ell + b)\right|\right)^{2r} \leq \left(\sum_{\ell=1}^{p} \nu(\ell)^{\frac{2r}{2r-1}}\right)^{2r-1} \sum_{\ell=1}^{p} \left|\sum_{b} \chi(\ell + b)\right|^{2r}$$

and

$$\left(\sum_{\ell=1}^{p} \nu(\ell)^{\frac{2r}{2r-1}}\right)^{2r-1} \leq \left(\sum_{\ell=1}^{p} \nu(\ell)\right)^{2r-2} \sum_{\ell=1}^{p} \nu(\ell)^2.$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

Clearly

$$\sum_{\ell=1}^{p} \nu(\ell) = AN.$$

We show below that if

$$AN < \frac{1}{2}p, \quad 1 \le A \le N, \tag{9.26}$$

then

$$\sum_{\ell=1}^{p} \nu(\ell)^2 \ll AN \log p. \tag{9.27}$$

Assuming this, we take $A = \left[\frac{1}{10}Np^{-1/(2r)}\right]$, $B = \left[p^{1/(2r)}\right]$. Then (9.24) gives (9.25) and (9.26). Thus from Lemma 9.26 with $h = B$ we see that

$$\sum_{n,a,b} \chi(n+ab) \ll rN^{2-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}}.$$

Hence there is an absolute constant $C$ such that

$$|S(M,N)| \le CrN^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}} + 2\mathcal{M}(N/10). \tag{9.28}$$

Choose $M_1$, $N_1$ with $N_1 \le N$ so that $|S(M_1,N_1)| = \mathcal{M}(N)$. If (9.24) fails because $N_1 \le p^{\frac{r+1}{4r}}$, then (9.28) with $M = M_1$, $N = N_1$ is trivial. Thus we have

$$\mathcal{M}(N) \le N^{1-\frac{1}{r}}\lambda + 2\mathcal{M}(N/10) \tag{9.29}$$

where

$$\lambda = Crp^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}}.$$

Moreover (9.29) is also trivial when $N \le p^{\frac{r+1}{4r}}$. We apply (9.29) repeatedly with $N$ replaced by $[N/10]$, $\left[[N/10]/10\right]$, and so on. Thus

$$\mathcal{M}(N) \le N^{1-\frac{1}{r}}\lambda \sum_{k=0}^{K} 2^k 10^{-k(1-\frac{1}{r})} + 2^{K+1}\mathcal{M}(10^{-K-1}N).$$

The trivial bound $\mathcal{M}(10^{-K-1}N) \ll 10^{-K}N$ with a judicious choice of $K$ suffices to give

$$\mathcal{M}(N) \ll N^{1-\frac{1}{r}}\lambda$$

which completes the proof, apart from the need to establish (9.27) with (9.26). Clearly

$$\sum_{\ell} \nu(\ell)^2$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

is the number of choices of $a, n, a', n', \ell$ with $a, a' \in [1, A]$, $n, n' \in [1, N]$, $M + n \equiv a\ell \pmod p$, $M + n' \equiv a'\ell \pmod p$. Since $1 \le a, a' \le A < p$, by elimination of $l$ we see that this is the number of solutions of $(a - a')M \equiv a'n - an' \pmod p$ with $a, n, a', n'$ as before. Given any such pair $a, a'$, choose $k$ so that $k \equiv (a - a')M \pmod p$ and $|k| < p/2$. We have $1 \le a'n, an' \le AN \le \frac{1}{10}N^2 p^{-\frac{1}{2r}} < p/2$ in all cases. Thus $a'n - an' = k$. Given any one pair $n = n_0$, $n' = n'_0$ satisfying this equation we have, in general, $n = n_0 + \frac{a}{(a,a')}h$, $n' = n'_0 + \frac{a'}{(a,a')}h$. Moreover $|h| \le \frac{N(a,a')}{\max\{a,a'\}}$. Therefore the total number of possible pairs $n$,$n'$ is at most $1 + \frac{2N(a,a')}{\max\{a,a'\}}$. Hence

$$\begin{aligned}\sum_{\ell} \nu(\ell)^2 &\ll A^2 + \sum_{1\le a\le a'\le A} \frac{N(a,a')}{a'} \\ &\ll A^2 + \sum_{d\le A} \sum_{1\le b\le b'\le A/d} \frac{N}{b'} \\ &\ll A^2 + AN \log 2A.\end{aligned}$$

and so we have (9.27). □

### 9.4.1 Exercises

1. Let $\chi$ be a non-principal character modulo $q$, and suppose that $(a, q) = 1$. Choose $\overline{a}$ so that $a\overline{a} \equiv 1 \pmod q$.
   (a) Explain why
   $$\overline{\chi}(a) \sum_{n=M+1}^{M+N} \chi(an + b) = \sum_{n=M+\overline{a}b+1}^{M+\overline{a}b+N} \chi(n).$$
   (b) Show that
   $$\sum_{n=M+1}^{M+N} \chi(an + b) \ll \sqrt{q} \log q.$$
2. With reference to the proof of Theorem 9.21, show that $2^{\omega(r)} \le c\sqrt{r}$ for all positive integers $r$ where $c = 4/\sqrt{6}$, and that equality holds only when $r = 6$.
3. Show that if $\chi$ is a character modulo $q$ with $\chi(-1) = -1$, then
   $$\sum_{n=1}^{q} n^2 \chi(n) = q \sum_{n=1}^{q} n\chi(n).$$

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

4. (a) Let $c_n$ and $f(n)$ have period $q$. Show that

$$\sum_{n=1}^{q} c_n f(n) = \sum_{n=1}^{q} c_n \frac{1}{q} \sum_{k=1}^{q} \widehat{f}(k) e(kn/q) = \frac{1}{q} \sum_{k=1}^{q} \widehat{f}(k)\widehat{c}(-k).$$

(b) Suppose that $1 \le N \le q$ and set $f(n) = 1$ for $M+1 \le n \le M+N$, and $f(n) = 0$ for other residues (mod $q$). Show that $\widehat{f}(0) = N$ and by (9.14) or otherwise that

$$\widehat{f}(k) = e(-(2M+N+1)k/q) \frac{\sin \pi k N/q}{\sin \pi k/q}$$

for $k \not\equiv 0 \pmod q$.

(c) By subtracting $\widehat{c}(0)N/q$ from both sides and applying the triangle inequality, show that

$$\left| \sum_{n=M+1}^{M+N} c_n - \frac{N}{q} \sum_{n=1}^{q} c_n \right| \le \frac{1}{q} \sum_{k=1}^{q-1} \frac{|\widehat{c}(k)|}{\sin \pi k/q}$$

5. (a) Suppose that a function $f$ is concave upwards. Explain why

$$f(x) \le \frac{1}{2\delta} \int_{x-\delta}^{x+\delta} f(u)\, du$$

for $\delta > 0$.

(b) Take $f(u) = \csc \pi u$, $x = k/q$, and $\delta = 1/(2q)$, and sum over $k$ to see that

$$\sum_{k=1}^{q-1} \frac{1}{\sin \pi k/q} < q \int_{1/(2q)}^{1-1/(2q)} \frac{1}{\sin \pi u}\, du.$$

(c) Note that $\csc v$ has the antiderivative $\log(\csc v - \cot v)$, and hence deduce that the integral above is

$$= \frac{q}{\pi} \log \frac{1 + \cos \frac{\pi}{2q}}{1 - \cos \frac{\pi}{2q}}.$$

(d) By means of the inequalities $1 - \theta^2/2 \le \cos\theta \le 1$ deduce that the above is

$$< \frac{q}{\pi} \log \frac{16q^2}{\pi^2} = \frac{2q}{\pi} \log \frac{4q}{\pi}.$$

(e) Note that this is $< q \log q$ if $q > \exp((\log 4/\pi)/(1-2/\pi)) = 1.944\ldots$.

6. Let $c_n$ be a sequence with period $q$ and finite Fourier transform $\widehat{c}(k)$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

(a) Show that

$$\sum_{M=1}^{q}\left|\sum_{n=M+1}^{M+N}c_n-\frac{N}{q}\sum_{n=1}^{q}c_n\right|^2=\frac{1}{q}\sum_{k=1}^{q-1}|\widehat{c}(k)|^2\frac{\sin^2\pi Nk/q}{\sin^2\pi k/q}$$

for $1\le N\le q$.

(b) Suppose that $c_n=1$ for $0<n<q$ and that $c_0=0$. Show that $\widehat{c}(0)=q-1$ and that $\widehat{c}(k)=-1$ for $0<k<q$. Deduce that

$$\sum_{k=1}^{q-1}\frac{\sin^2\pi Nk/q}{\sin^2\pi k/q}=(q-N)N$$

for $0\le N\le q$.

(c) Take $q=2N$ and write $k=2n-1$ to deduce that

$$\sum_{n=1}^{N}\frac{1}{\left(N\sin\pi\frac{2n-1}{2N}\right)^2}=1.$$

Let $N$ tend to infinity to show that $\sum_{n=1}^{\infty}(2n-1)^{-2}=\pi^2/8$, and hence that $\zeta(2)=\pi^2/6$.

7. (a) Show that if $\chi$ is a primitive character modulo $q$, $q>1$, then

$$\sum_{M=1}^{q}\left|\sum_{n=M+1}^{M+N}\chi(n)\right|^2\le Nq$$

for $1\le N\le q$.

(b) Show that if $\chi\ne\chi_0\pmod p$, then

$$\sum_{M=1}^{p}\left|\sum_{n=M+1}^{M+N}\chi(n)\right|^2=N(p-N)$$

for $1\le N\le p$.

8. Let $f_\chi(\alpha)=\sum_{0<n\le q\alpha}\chi(n)$. Show that if $\chi$ is a primitive character modulo $q$, then

$$\int_0^1|f_\chi(\alpha)-a_\chi|^2\,d\alpha=\frac{q}{12}\prod_{p\mid q}\left(1-\frac{1}{p^2}\right)$$

where $a_\chi=0$ if $\chi(-1)=1$, and

$$a_\chi=\frac{-1}{q}\sum_{n=1}^{q}n\chi(n)=-iL(1,\overline{\chi})\tau(\chi)/\pi$$

if $\chi(-1)=-1$.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

9. (a) Show that

$$\sum_{d|q} \frac{\log p}{p-1} \ll \log\log 3q.$$

(b) Recall Exercise 2.1.16, and show that

$$\sum_{\substack{k\le K\\(k,q)=1}} \frac{1}{k} = \frac{\varphi(q)}{q}\log K + O\left(\frac{\varphi(q)}{q}\log\log q\right) + O\left(\frac{2^{\omega(q)}}{K}\right)$$

for $1 \le K \le q$.

(c) Suppose that $\chi$ is a primitive character modulo $q$, $q > 1$. Use Theorem D.2 to show that

$$\sum_{n=M+1}^{M+N} \chi(n) = \frac{\tau(\chi)}{2\pi i}\sum_{0<|k|\le K} \frac{\overline{\chi}(-k)}{k} e(kM/q)(e(kN/q)-1) + O\left(\frac{\varphi(q)}{K}\log 2K\right)$$

when $K < q^{1-\varepsilon}$.

(d) By taking $K = q^{1/2}\log q$ show that if $\chi$ is a primitive character modulo $q$, $q > 1$, then

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| \le \frac{\varphi(q)}{\pi q} q^{1/2}\log q + O\big(q^{1/2}\log\log 3q\big).$$

10. (Bernstein 1914a,b) Let $\chi$ be a primitive character (mod $q$), with $q > 1$. Show that

$$\sum_{|n|\le q} (1-|n|/q)\chi(n)e(n\alpha) \ll \sqrt{q}$$

uniformly in $\alpha$.

## 9.5 Notes

Section 9.2. That the sum in (9.6) vanishes when $(n, q) > 1$ was proved by de la Vallée Poussin (1896), in a complicated way. We follow the simpler argument that Schur showed Landau (1908, pp. 430–431).

The evaluation of the sum $c_\chi$ is found in Hasse (1964, pp. 449–450). Our derivation follows that of Montgomery & Vaughan (1975). A different proof has been given by Joris (1977).

Section 9.3. Let $\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ be the Dedekind zeta function of the algebraic number field $K$. Here the sum is over all ideals $\mathfrak{a}$ in the ring $\mathcal{O}_K$ of integers in $K$. In case $K$ is a quadratic extension of $\mathbb{Q}$, then the discriminant

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511874314.011 Published online by Cambridge University Press

$d$ of $K$ is a quadratic discriminant, $K = \mathbb{Q}(\sqrt{d})$, and $\zeta_K(s) = \zeta(s)L(s, \chi_d)$. In other words, the number of ideals of norm $n$ is $\sum_{k|n} \chi_d(k)$.

Section 9.4. Concerning the constant that can be taken in Theorem 9.18, see Landau (1918), Cochrane (1987), Hildebrand (1988a,b), and Granville & Soundararajan (2005). Granville & Soundararajan (2005) also show that in the case of a cubic character, the sum in Theorem 9.18 is $\ll \sqrt{q}(\log q)^\theta$ where $\theta$ is an absolute constant, $\theta < 1$.

On the assumption of the Generalized Riemann Hypothesis for all Dirichlet characters, Montgomery & Vaughan (1977) have shown that

$$\sum_{n=M+1}^{M+N} \chi(n) \ll q^{1/2} \log\log q.$$

See Granville & Soundararajan (2005) for a much simpler proof. Paley's lower bound, Theorem 9.24 above, shows that the above is essentially best-possible. Nevertheless, it is known that one can do better a good deal of the time. In fact in Montgomery & Vaughan (1979) it is shown that for each $\theta \in (0, 1)$ there is a $c(\theta) > 0$ such that if $P > P_0(\theta)$, then for at least $\theta\pi(P)$ primes $p \le P$ we have

$$\max_N \left| \sum_{n=1}^{N} \left(\frac{n}{p}\right) \right| \le c(\theta) p^{1/2},$$

and if $q > P_0(\theta)$, then for at least $\theta\varphi(q)$ of the non-principal characters modulo $q$ we have

$$\max_N \left| \sum_{n=1}^{N} \chi(n) \right| \le c(\theta) q^{1/2}.$$

Walfisz (1942) and Chowla (1947) showed that there exist infinitely many primitive quadratic characters $\chi$ for which $L(1, \chi) \gtrsim e^{C_0} \log\log q$. In view of Theorem 9.21, this provides an alternative approach for proving estimates similar to Paley's Theorem 9.24. For recent developments concerning large $L(1, \chi)$, see Vaughan (1996), Montgomery & Vaughan (1999), and Granville & Soundararajan (2003).

Lemma 9.25 is a consequence of Weil's proof of the Riemann Hypothesis for curves over finite fields, and originally depended on considerable machinery from algebraic geometry. Later Stepanov used constructs from transcendence theory to estimate complete character sums, and subsequently Bombieri used Stepanov's ideas to give a proof of Weil's theorem that depends only on the Riemann–Roch theorem. Schmidt (1976) gives an exposition of this more elementary approach that even avoids the Riemann–Roch theorem. Friedlander & Iwaniec (1992) showed that the Pólya–Vinogradov inequality can be sharpened, in the direction of Burgess' estimates, without using Weil's estimates. The

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

proof of Theorem 9.27 above is developed from one of Iwaniec appearing in Friedlander (1987), with a further wrinkle from Friedlander & Iwaniec (1993).

Burgess first (1957) treated the Legendre symbol and then (1962a, b) generalized his method to deal with arbitrary Dirichlet characters having cube-free conductor. Burgess' extension to composite moduli involves an extra new idea that does not extend well when the conductor is divisible by higher powers of primes. For some progress in this direction see Burgess (1986).

## 9.6 References


Apostol, T. M. (1970). Euler's $\varphi$-function and separable Gauss sums, *Proc. Amer. Math. Soc*. **24**, 482–485.

Baker, R. C. & Montgomery, H. L. (1990). Oscillations of quadratic $L$-functions, *Analytic Number Theory* (Urbana, 1989), Prog. Math. 85. Boston: Birkhäuser, pp. 23–40.

Bernstein, S. N. (1914a). Sur la convergence absolue des séries trigonométriques, *C. R. Acad, Sci. Paris* **158**, 1661–1663.

(1914b). Ob absoliutnoi skhodimosti trigonometricheskikh riadov, *Soobsch. Khar'k. matem. ob-va* (2) **14**, 145–152; 200–201.

Burgess, D. A. (1957). The distribution of quadratic residues and non-residues, *Mathematika* **4**, 106–112.

(1962a). On character sums and primitive roots, *Proc. London Math. Soc.* (3) **12**, 179–192.

(1962b). On character sums and $L$-series, *Proc. London Math. Soc.* (3) **12**, 193–206.

(1986). The character sum estimate with $r = 3$, *J. London Math. Soc.* (2) **33**, 219–226.

Chowla, S. (1947). On the class-number of the corpus $P(\sqrt{-k})$, *Proc. Nat. Inst. Sci. India* **13**, 197–200.

Chowla, S. & Mordell, L. J. (1961). Note on the nonvanishing of $L(1)$, *Proc. Amer. Math. Soc.* **12**, 283–284.

Cochrane, T. (1987). On a trigonometric inequality of Vinogradov, *J. Number Theory* **27**, 9–16.

Conway, J. H. (1997). *The Sensuous Quadratic Form*, Carus monograph 26. Washington: Math. Assoc. Amer.

Friedlander, J. B. (1987). Primes in arithmetic progressions and related topics, *Analytic Number Theory and Diophantine Problems* (Stillwater, 1984), Prog. Math. 70, Boston: Birkhäuser, pp. 125–134.

Friedlander, J. B. & Iwaniec, H. (1992). A mean-value theorem for character sums, *Michigan Math. J.* **39**, 153–159.

(1993). Estimates for character sums, *Proc. Amer. Math. Soc.* **119**, 365–372.

(1994). A note on character sums, *The Rademacher legacy to mathematics* (University Park, 1992), Contemp. Math. 166, Providence: Amer. Math. Soc., pp. 295–299.

Fujii, A., Gallagher, P. X., & Montgomery, H. L. (1976). Some hybrid bounds for character sums and Dirichlet $L$-series, *Topics in Number Theory* (Proc. Colloq.


Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

Debrecen, 1974), Colloq. Math. Soc. Janos Bolyai 13. Amsterdam: North-Holland, pp. 41–57.

Granville, A. & Soundararajan, K. (2003). The distribution of values of $L(1, \chi_d)$, *Geom. Funct. Anal*. **13**, 992–1028; *Errata* **14** (2004), 245–246.

(2006). *Large character sums: pretentious characters and the Pólya-Vinogradov inequality*, to appear, 24 pp.

Hasse, H. (1964). *Vorlesungen über Zahlentheorie*, Second Edition, Grundl. Math. Wiss. 59. Berlin: Springer-Verlag.

Hildebrand, A. (1988a). On the constant in the Pólya–Vinogradov inequality, *Canad. Math. Bull*. **31**, 347–352.

(1988b). Large values of character sums, *J. Number Theory* **29**, 271–296.

Joris, H. (1977). On the evaluation of Gaussian sums for non-primitive characters, *Enseignement Math*. (2) **23**, 13–18.

Landau, E. (1908). Nouvelle démonstration pour la formule de Riemann sur le nombre des nombres premiers inférieurs à une limite donnée, et démonstration d'une formule plus générale pour le cas des nombres premiers d'une progression arithmétique, *Ann. École Norm. Sup.* (3) **25** 399–448; *Collected Works*, Vol. 4. Essen: Thales Verlag, 1986, pp. 87–130.

(1918). Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen, *Nachr. Akad. Wiss.* Göttingen, 79–97; *Collected Works*, Vol. 7. Essen: Thales Verlag, 1986, pp. 114–132.

Martin, G. (2006). Inequities in the Shanks–Rényi prime number race, 32 pp., to appear.

Mattics, L. E. (1984). Advanced problem 6461, *Amer. Math. Monthly* **91**, 371.

Montgomery, H. L. (1976). Distribution questions concerning a character sum, *Topics in Number Theory* (Proc. Colloq. Debrecen, 1974), Colloq. Math. Soc. Janos Bolyai 13. Amsterdam: North-Holland, pp. 195–203.

(1980). An exponential polynomial formed with the Legendre symbol, *Acta Arith*. **37**, 375–380.

Montgomery, H. L. & Vaughan, R. C. (1975). The exceptional set in Goldbach's problem, *Acta Arith*. **27**, 353–370.

(1977). Exponential sums with multiplicative coefficients, *Invent. Math*. **43**, 69–82.

(1979). Mean values of character sums, *Canad. J. Math*. **31**, 476–487.

(1999). Extreme values of Dirichlet $L$-functions at 1, *Number Theory in Progress*, Vol. 2 (Zakopane–Kościelisko, 1997). Berlin: de Gruyter, pp. 1039–1052.

Mordell, L. J. (1933). The number of solutions of some congruences in two variables, *Math. Z*. **37**, 193–209.

Paley, R. E. A. C. (1932). A theorem of characters, *J. London Math. Soc*. **7**, 28–32.

Pólya, G. (1918). Über die Verteilung der quadratischen Reste und Nichtreste, *Nachr. Akad. Wiss. Göttingen*, 21–29.

Schmidt, W. M. (1976). *Equations over finite fields. An elementary approach*, Lecture Notes Math. 536, Berlin: Springer-Verlag.

Schur, I. (1918). Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste, *Nachr. Akad. Wiss. Göttingen*, 30–36.

de la Vallée Poussin, C. J. (1896). Recherches analytiques sur la théorie des nombres premiers, I–III, *Ann. Soc. Sci. Bruxelles* **20**, 183–256, 281–362, 363–397.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press

Vaughan, R. C. (1996). Small values of Dirichlet *L*-functions at 1, *Analytic Number Theory*. (Allerton Park, 1995), Vol. 2, Prog. Math. 139, Boston: Birkhäuser, pp. 755–766.

Vinogradov, I. M. (1918). Sur la distribution des résidus et des nonrésidus des puissances, *J. Soc. Phys. Math. Univ. Permi*, 18–28.

(1919). Über die Verteilung der quadratischen Reste und Nichtreste, *J. Soc. Phys. Math. Univ. Permi*, 1–14.

Vorhauer, U. M. A. (2006). *A note on comparative prime number theory*, to appear.

Walfisz, A. (1942). On the class-number of binary quadratic forms, *Trudy Tbliss. Mat. Inst*. **11**, 57–71.

Cambridge Books Online © Cambridge University Press, 2010
https://doi.org/10.1017/CBO9780511814014 Published online by Cambridge University Press