Cubic and Quartic Characters

Steven Finch

June 5, 2009

In this essay, we revisit Dirichlet characters [1], but focusing here on non-real cases (that is, of order exceeding 2).

Let $\mathbb{Z}_n^*$ denote the group (under multiplication modulo $n$) of integers relatively prime to $n$, and let $\mathbb{C}^*$ denote the group (under ordinary multiplication) of nonzero complex numbers. We wish to examine homomorphisms $\chi : \mathbb{Z}_n^* \to \mathbb{C}^*$ satisfying certain requirements. A Dirichlet character $\chi$ is quadratic if $\chi(k)^2 = 1$ for every $k$ in $\mathbb{Z}_n^*$. It is well-known that, if $\chi \neq 1$ is a primitive quadratic character modulo $n$, then $D = \chi(-1)n$ is a fundamental discriminant and

$$\chi(k) = \left(\frac{D}{k}\right) \text{ for all } k \in \mathbb{Z}_n^*$$

where $(D/k)$ is the Kronecker-Jacobi-Legendre symbol. A character $\chi$ is real if and only if it is quadratic. By the correspondence with $(D/.)$, quadratic characters can be said to be completely understood.

A Dirichlet character $\chi$ is cubic if $\chi(k)^3 = 1$ for every $k$ in $\mathbb{Z}_n^*$. Let $\omega = (-1 + i\sqrt{3})/2$ where $i$ is the imaginary unit. Let $a + b\omega$ be a prime in the ring $\mathbb{Z}[[\omega]]$ of Eisenstein-Jacobi integers with norm $a^2 - ab + b^2 \neq 3$. For any positive integer $n$ in $\mathbb{Z}$, define the cubic residue symbol [2, 3]

$$\left(\frac{n}{a + b\omega}\right)_3$$

to be 0 if $n$ is divisible by $a + b\omega$; otherwise it is the unique power $\omega^j$ for $0 \leq j \leq 2$ such that

$$n(a^2 - ab + b^2 - 1)/3 \equiv \omega^j \mod(a + b\omega).$$

The only prime divisor of 9 is $1 - \omega$, which has norm 3. Hence we will need an alternative way of representing characters:

$$f_q(n, k) = \begin{cases} \omega^e & \text{if } n \equiv k^e \mod q \\ 0 & \text{otherwise} \end{cases}$$

Copyright © 2009 by Steven R. Finch. All rights reserved.
especially in the case $q = 9$. The first several cubic characters are

$$f_7(n, 5) = \left(\frac{n}{2+3\omega}\right)_3|_{n=1,\ldots,7} = \{1, \omega, \omega^2, \omega, 1, 0\},$$

$$f_7(n, 3) = \left(\frac{n}{-1-3\omega}\right)_3|_{n=1,\ldots,7} = \{1, \omega^2, \omega, \omega^2, 1, 0\},$$

$$f_9(n, 2)|_{n=1,\ldots,9} = \{1, \omega, 0, \omega^2, \omega^2, 0, \omega, 1, 0\},$$

$$f_9(n, 5)|_{n=1,\ldots,9} = \{1, \omega^2, 0, \omega, \omega, 0, \omega^2, 1, 0\},$$

$$f_{13}(n, 2) = \left(\frac{n}{4-3\omega}\right)_3|_{n=1,\ldots,13} = \{1, \omega, \omega^2, 1, \omega^2, 1, \omega^2, \omega, 1, 0\},$$

$$f_{13}(n, 6) = \left(\frac{n}{-1+3\omega}\right)_3|_{n=1,\ldots,13} = \{1, \omega^2, \omega, 1, \omega, 1, \omega, \omega^2, 1, 0\},$$

$$f_{19}(n, 2) = \left(\frac{n}{2-3\omega}\right)_3|_{n=1,\ldots,19} = \{1, \omega, \omega^2, \omega, \omega^2, 1, 1, \omega^2, \omega^2, 1, \omega^2, \omega^2, \omega, 1, 0\},$$

$$f_{19}(n, 10) = \left(\frac{n}{5+3\omega}\right)_3|_{n=1,\ldots,19} = \{1, \omega^2, \omega^2, \omega, \omega^2, 1, 1, \omega, 1, 1, \omega^2, \omega^2, \omega^2, 1, 0\},$$

$$f_{31}(n, 3) = \left(\frac{n}{5+6\omega}\right)_3|_{n=1,\ldots,31}$$

$$= \{1, 1, \omega, 1, \omega^2, \omega, 1, \omega^2, \omega^2, \omega, \omega^2, \omega, 1, 1, \omega, \omega^2, \omega^2, \omega^2, \omega, 1, \omega, 1, 1, 0\},$$

$$f_{31}(n, 11) = \left(\frac{n}{-1-6\omega}\right)_3|_{n=1,\ldots,31}$$

$$= \{1, 1, \omega, 1, \omega^2, \omega, 1, \omega, \omega^2, \omega, \omega^2, \omega^2, 1, 1, \omega^2, \omega^2, \omega, \omega^2, \omega^2, \omega, 1, 1, 1, 0\},$$

$$f_{37}(n, 2) = \left(\frac{n}{-4+3\omega}\right)_3|_{n=1,\ldots,37}$$

$$= \{1, \omega, \omega^2, \omega^2, \omega^2, 1, \omega^2, 1, \omega, 1, \omega, \omega^2, \omega^2, \omega, \omega^2, \omega^2, \omega, 1, 1, 0\},$$

$$f_{37}(n, 5) = \left(\frac{n}{-7-3\omega}\right)_3|_{n=1,\ldots,37}$$

$$= \{1, \omega^2, \omega, \omega, \omega, 1, \omega, 1, \omega^2, 1, 1, \omega^2, \omega, 1, \omega^2, \omega^2, \omega, \omega^2, \omega^2, \omega, 1, 1, 0\}. $$
A Dirichlet character $\chi$ is **quartic (biquadratic)** if $\chi(k)^4 = 1$ for every $k$ in $\mathbb{Z}^*_n$. Let $a + bi$ be a prime in the ring $\mathbb{Z}[i]$ of Gaussian integers with norm $a^2 + b^2 \neq 2$. For any positive integer $n$ in $\mathbb{Z}$, define the quartic (biquadratic) residue symbol $[2, 3]
 n \pmod{a + bi}$
to be 0 if $n$ is divisible by $a + bi$; otherwise it is the unique power $i^j$ for $0 \leq j \leq 3$ such that

$$n^{(a^2+b^2-1)/4} \equiv i^j \mod(a + bi).$$

The only prime divisor of 16 is $1 + i$, which has norm 2. We will again need alternative ways of representing characters:

$$f_q(n, k) = \begin{cases} 0 & \text{if } n \equiv k^e \mod q, \\ i^e & \text{otherwise,} \end{cases}$$

$$g_q(n, k) = \begin{cases} 0 & \text{if } n \equiv k^e \mod q \text{ or } q - n \equiv k^e \mod q, \\ i^e & \text{otherwise}, \end{cases}$$

$$h_q(n, k, \ell, m) = \begin{cases} 0 & \text{if } q - n \equiv m^e \mod q, \\ (-1)^{e+1} & \text{if } n \equiv k^e \mod q \text{ or } n \equiv \ell^e \mod q, \end{cases}$$

especially in the cases $q = 15, 16, 20$ and 35. The first several non-real quartic characters are

$$f_5(n, 2) = \left(\frac{n}{1-2i}\right)_4^{n=1,\ldots,5} = \{1, i, -i, -1, 0\},$$

$$f_5(n, 3) = \left(\frac{n}{1+2i}\right)_4^{n=1,\ldots,5} = \{1, -i, i, -1, 0\},$$

$$f_{13}(n, 2) = \left(\frac{n}{3+2i}\right)_4^{n=1,\ldots,13} = \{1, i, 1, -1, i, -i, -i, 1, -1, -i, -1, 0\},$$

$$f_{13}(n, 7) = \left(\frac{n}{3+2i}\right)_4^{n=1,\ldots,13} = \{1, -i, 1, -1, -i, i, i, 1, -1, i, -1, 0\},$$

$$g_{15}(n, 2)|_{n=1,\ldots,15} = \{1, i, 0, -1, 0, 0, -i, -i, 0, 0, -1, 0, i, 1, 0\},$$

$$g_{15}(n, 8)|_{n=1,\ldots,15} = \{1, -i, 0, -1, 0, 0, i, 0, 0, -1, 0, -i, 1, 0\},$$

$$g_{16}(n, 3)|_{n=1,\ldots,16} = \{1, 0, i, 0, -i, 0, -1, 0, -1, 0, -i, 0, i, 0, 1, 0\},$$

$$g_{16}(n, 5)|_{n=1,\ldots,16} = \{1, 0, -i, 0, i, 0, -1, 0, -1, 0, i, 0, -i, 0, 1, 0\},$$

$$h_{16}(n, 3, 5, 9)|_{n=1,\ldots,16} = \{1, 0, i, 0, i, 0, 1, 0, -1, 0, -i, 0, -i, 0, -1, 0\}.$$
We mention that $[4]$

\begin{align*}
h_{16}(n, 11, 13, 9)|_{n=1, \ldots, 16} &= \{1, 0, -i, 0, -i, 0, 1, 0, -1, 0, i, 0, i, 0, -1, 0\}, \\
f_{17}(n, 3) &= \left(\frac{n}{1+4i}\right)_4|_{n=1, \ldots, 17} = \{1, -1, -i, 1, -i, -i, -1, -1, -1, -i, i, 1, i, -1, 1, 0\}, \\
f_{17}(n, 6) &= \left(\frac{n}{1+4i}\right)_4|_{n=1, \ldots, 17} = \{1, -1, -i, 1, -i, i, -1, i, i, -i, 1, -i, 1, -1, 1, 0\}, \\
g_{20}(n, 3)|_{n=1, \ldots, 20} &= \{1, 0, i, 0, 0, 0, -i, 0, -1, 0, -1, 0, 0, 0, 0, i, 0, 1, 0\}, \\
g_{20}(n, 7)|_{n=1, \ldots, 20} &= \{1, 0, -i, 0, 0, 0, i, 0, -1, 0, -1, 0, i, 0, 0, -i, 0, 1, 0\}, \\
f_{29}(n, 2) &= \left(\frac{n}{5-2i}\right)_4|_{n=1, \ldots, 29} = \{1, i, i, -1, -1, -1, -1, -i, -i, -1, i, -1, i, i, -i, 1, \\
&\qquad i, -1, 1, 1, 1, -i, -i, -1, 0\}, \\
f_{29}(n, 8) &= \left(\frac{n}{-5+2i}\right)_4|_{n=1, \ldots, 29} = \{1, -i, -i, -1, -1, 1, -1, -i, -i, -1, i, 1, -i, i, -i, 1, \\
&\qquad -i, -1, 1, 1, 1, i, i, -1, 0\}, \\
g_{35}(n, 2)|_{n=1, \ldots, 35} &= \{1, i, i, -1, 0, -1, 0, -i, -1, 0, 1, -i, 0, 0, 1, -i, -1, 0, \\
&\qquad 0, i, -i, 1, 0, -1, -i, 0, -1, 0, -1, i, i, 1, 0\}, \\
g_{35}(n, 18)|_{n=1, \ldots, 35} &= \{1, -i, -i, -1, 0, -1, 0, i, -1, 0, 1, i, i, 0, 1, i, 1, 0, \\
&\qquad 0, -i, i, 1, 0, -1, i, 0, -1, 0, -1, -i, i, 1, 0\}, \\
f_{37}(n, 2) &= \left(\frac{n}{1+6i}\right)_4|_{n=1, \ldots, 37} = \{1, i, -1, -1, -i, -i, 1, -1, 1, -1, -i, i, 1, -i, i, -i, i, \\
&\qquad -1, -i, -i, -1, 1, -1, -1, i, i, 1, 1, -i, -1, 0\}, \\
f_{37}(n, 5) &= \left(\frac{n}{1-6i}\right)_4|_{n=1, \ldots, 37} = \{1, -i, -1, -1, i, i, 1, 1, 1, -1, 1, -i, i, -i, i, -i, i, \\
&\qquad -1, i, i, -i, -1, 1, -1, -i, -1, -i, i, 1, 1, -i, -1, 0\}. \\
\end{align*}

We mention that $[4]$ \# Dirichlet characters of order $\ell$ and modulus $n$ $=$ \# solutions $x$ in $\mathbb{Z}_n^*$ of the equation $x^\ell = 1$
and thus, by Möbius inversion,

\[
\begin{align*}
\text{\# primitive quadratic Dirichlet characters of modulus } & \leq N \sim \frac{6}{\pi^2} N, \\
\text{\# primitive cubic Dirichlet characters of modulus } & \leq N \sim A N, \\
\text{\# primitive quartic Dirichlet characters of modulus } & \leq N \sim B N \ln(N),
\end{align*}
\]
as \(N \to \infty\), where \([5, 6, 7]\)

\[
A = \frac{11\sqrt{3}}{18\pi} \prod_{p \equiv 1 \mod 3} \left(1 - \frac{2}{p(p+1)}\right) = 0.3170565167..., \\
B = \frac{7}{\pi} \frac{1}{16K^2} \prod_{p \equiv 1 \mod 4} \left(1 - \frac{5p - 3}{p^2(p+1)}\right) = 0.1908767211...
\]

and \(K\) is the Landau-Ramanujan constant \([8]\). No one appears to have examined \(B\) before.

Now define the **Dirichlet L-series associated to** \(\chi \neq 1\):

\[
L_\chi(z) = \sum_{n=1}^{\infty} \chi(n)n^{-z} = \prod_p (1 - \chi(p)p^{-z})^{-1}, \quad \text{Re}(z) > 1
\]

which can be made into an entire function. Special values are more complicated for cubic/quartic characters than for quadratic characters \([1]\). For example, if \(\chi = (\cdot/(2 + 3\omega))_3\), then

\[
L_\chi(1) = 7^{-2/3}(-2 - 3\omega)^{1/3} \left(\omega^2 \ln(y_1) + \omega \ln(y_2) + \ln(y_3)\right)
\]

where \(y_1 < y_2 < y_3\) are the (real) zeroes of \(y^3 - 7y^2 + 14y - 7\); if \(\chi = f_9(\cdot, 2)\), then

\[
L_\chi(1) = -\frac{7}{3\omega^{1/3}} \left(\omega^2 \ln \left(\sin \left(\frac{\pi}{18}\right)\right) + \omega \ln \left(\cos \left(\frac{\pi}{18}\right)\right) + \ln \left(\sin \left(\frac{\pi}{9}\right)\right)\right).
\]

As more examples, if \(\chi = (\cdot/(-1 - 2i))_4\), then

\[
L_\chi(1) = 2^{1/2}5^{-5/4}(3 + 4i)^{1/4}\pi;
\]

if \(\chi = g_{16}(\cdot, 3)\), then

\[
L_\chi(1) = -\frac{1}{2}i^{1/4} \left(i \ln \left(\cot \left(\frac{3\pi}{16}\right)\right) + \ln \left(\tan \left(\frac{\pi}{16}\right)\right)\right);
\]
if $\chi = h_{16}(\cdot, 3, 5, 9)$, then
\[ L_\chi(1) = 8^{-1/2}i^{1/4} \pi. \]
See a general treatment of quartic cases in [9].

The elaborate formulas for moments of $L_\chi(1/2)$ over primitive quadratic characters $\chi$ do not yet appear to have precise analogs for primitive cubic characters. Baier & Young [10] proved that
\[ \sum_{q \leq Q} \sum_{\chi} |L_\chi(1/2)|^2 = O(Q^{6/5+\varepsilon}) \]
as $Q \to \infty$, for any $\varepsilon > 0$, where the big-$O$ constant depends on $\varepsilon$. The inner summation is over all primitive cubic characters modulo $q$. As a consequence, $L_\chi(1/2) \neq 0$ for infinitely many such $\chi$.

0.1. Cubic Twists. Given an elliptic curve $E$ over $\mathbb{Q}$ with L-series
\[ L_E(z) = \sum_{n=1}^{\infty} c_n n^{-z}, \]
the L-series obtained via twisting $L_E(z)$ by a cubic character $\chi$ is
\[ L_{E,\chi}(z) = \sum_{n=1}^{\infty} \chi(n) c_n n^{-z}. \]
Of course, while each $c_n \in \mathbb{Z}$, the coefficients $\chi(n)c_n \in \mathbb{Z}[\omega]$ need not be real. This generalizes the sense of quadratic twists discussed in [11]; we refer to a paper of David, Fearnley & Kisilevsky [6] for more information on such L-series.

There is a different sense of cubic twists that interests us – it is important for the study of the family of elliptic curves $F_d$ given by $x^3 + y^3 = d$ – and features the cubic residue symbol $(d/\cdot)_3$ in an intriguing way. We mentioned the problem of evaluating $L_{F_d}(1)$ for cube-free $d > 2$ in [11] but did not give details. By definition [12],
\[ L_{F_d}(z) = \sum_{a, b \in \mathbb{Z}} (a + b\omega^2) \left( \frac{d}{a + b\omega} \right)_3 (a^2 - ab + b^2)^{-z} \]
\[ = \sum_{a, b \in \mathbb{Z}} (a + b\omega) \left( \frac{d}{a + b\omega^2} \right)_3 (a^2 - ab + b^2)^{-z} \]
\[ = \prod_{p \equiv 2 \mod 3} (1 + p^{1-2z})^{-1} \cdot \prod_{p \equiv 1 \mod 3} (1 - c_p p^{-z} + p^{1-2z})^{-1} \]
Cubic and Quartic Characters

where

\[ c_p = (h + k\omega^2) \left( \frac{d}{h + k\omega} \right)_3 + (h + k\omega) \left( \frac{d}{h + k\omega^2} \right)_3 \]

and \( p = (h + k\omega)(h + k\omega^2) \), \( h \equiv 1 \mod 3 \), \( k \equiv 0 \mod 3 \). To extend to composite indices, use the usual recurrence \( c_{p^j} = c_{p^{j-1}} c_p - p c_{p^{j-2}} \) for \( j \geq 2 \), \( c_1 = 1 \) and \( c_{mn} = c_m c_n \) for coprime integers \( m, n \).

For \( d = 1 \) and \( p \equiv 1 \mod 3 \), it is known that \( c_p = \gamma_p \), where \( \gamma_p \) is the unique integer \( \alpha \equiv 2 \mod 3 \) such that \( \alpha^2 + 3\beta^2 = 4p \) for some integer \( \beta \equiv 0 \mod 3 \). Now, for \( d > 1 \) and \( p \equiv 1 \mod 3 \), \( p \nmid d \), it can be shown that \( c_p \) is the unique integer \( \alpha \equiv 2 \mod 3 \) such that three conditions:

- \( \alpha^2 + 3\beta^2 = 4p \) for some integer \( \beta \)
- \( \alpha \equiv d^{(p-1)/3}\gamma_p \mod p \)
- \( |\alpha| < 2\sqrt{p} \)

are simultaneously satisfied [13].

Sextic twists are required to study Bachet’s equation \( y^2 = x^3 + n \) for arbitrary \( n \) (the Fermat cubic problem is a special case with \( n = -432d^2 \) and \( d \) cube-free). Such residue symbols are beyond us. Here is a formula for L-series coefficients \( c_p \) in this more general setting: when \( p = 3 \), \( p|n \) or \( p \equiv 2 \mod 3 \), we have \( c_p = 0 \); otherwise [14]

\[ c_p = \left( \frac{n}{p} \right) \cdot \begin{cases} 2a - b & \text{if } (4n)^{(p-1)/3} \equiv 1 \mod p, \\ -a - b & \text{if } (4n)^{(p-1)/3}b \equiv -a \mod p, \\ 2b - a & \text{if } (4n)^{(p-1)/3}a \equiv -b \mod p \end{cases} \]

where \( p = a^2 - ab + b^2 \) with \( a \equiv 1 \mod 3 \), \( b \equiv 0 \mod 3 \) and \( (\cdot/\cdot) \) is the Kronecker-Jacobi-Legendre symbol. The sequence of integers for which \( y^2 = x^3 + n \) has zero rank [15]:

\[ ..., -12, -10, -9, -8, -6, -5, -3, -1, 1, 4, 6, 7, 13, 14, 16, 20, ... \]

deserves close attention!

0.2. Quartic Twists. Quartic twists are required to study \( y^2 = x^3 - nx \) for arbitrary \( n \) (the congruent number problem is a special case with \( n = d^2 \) and \( d \)
Cubic and Quartic Characters

square-free [11]). Analogous to the expression for $L_{d,q}(z)$,

$$L_{En}(z) = \sum_{a,b \in \mathbb{Z} \atop a \equiv 1 \text{ mod } 4 \atop b \equiv 0 \text{ mod } 2} (a - bi) \left( \frac{-n}{a + bi} \right) 4 (a^2 + b^2)^{-z}$$

$$= \sum_{a,b \in \mathbb{Z} \atop a \equiv 1 \text{ mod } 4 \atop b \equiv 0 \text{ mod } 2} (a + bi) \left( \frac{-n}{a - bi} \right) 4 (a^2 + b^2)^{-z}.$$  

Here also is the corresponding formula for L-series coefficients $c_p$: when $p = 2$, $p|n$ or $p \equiv 3 \text{ mod } 4$, we have $c_p = 0$; otherwise [14]

$$c_p = 2 \left( \frac{2}{p} \right) \cdot \begin{cases} -a & \text{if } n^{(p-1)/4} \equiv 1 \text{ mod } p, \\ a & \text{if } n^{(p-1)/4} \equiv -1 \text{ mod } p, \\ -b & \text{if } n^{(p-1)/4}b \equiv -a \text{ mod } p, \\ b & \text{if } n^{(p-1)/4}b \equiv a \text{ mod } p \end{cases}$$

where $p = a^2 + b^2$ with $a \equiv 3 \text{ mod } 4$, $b \equiv 0 \text{ mod } 2$. Again, the sequence of integers for which $y^2 = x^3 - nx$ has zero rank [15]:

..., −12, −11, −10, −7, −6, −4, −2, −1, 3, 4, 8, 9, 11, 13, 18, ...

is worthy of deeper study.

References


[9] K. Hardy and K. S. Williams, Evaluation of the infinite series $\sum_{n=1}^{\infty} \left( \frac{a}{n} \right)_4 n^{-1}$, *Proc. Amer. Math. Soc.* 109 (1990) 597–603; MR1019275 (90k:11114).


