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 χ is **quadratic** if $\chi(k)^2 = 1$ for every kin \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

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

where (D/k) is the Kronecker-Jacobi-Legendre symbol. A character χ 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 χ 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 ω^j for $0 \le j \le 2$ such that

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

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

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

⁰Copyright © 2009 by Steven R. Finch. All rights reserved.

especially in the case q = 9. The first several cubic characters are

$$\begin{split} f_7(n,5) &= \left(\frac{n}{2+3\omega}\right)_3 \Big|_{n=1,\dots,7} = \{1,\omega,\omega^2,\omega^2,\omega,1,0\}, \\ f_7(n,3) &= \left(\frac{n}{-1-3\omega}\right)_3 \Big|_{n=1,\dots,7} = \{1,\omega^2,\omega,\omega,\omega^2,1,0\}, \\ f_9(n,2)|_{n=1,\dots,9} &= \{1,\omega,0,\omega^2,\omega^2,0,\omega,1,0\}, \\ f_9(n,5)|_{n=1,\dots,9} &= \{1,\omega^2,0,\omega,\omega,0,\omega^2,1,0\}, \\ f_{13}(n,2) &= \left(\frac{n}{-4-3\omega}\right)_3 \Big|_{n=1,\dots,13} = \{1,\omega,\omega,\omega^2,1,\omega^2,\omega^2,1,\omega^2,\omega,\omega,1,0\}, \\ f_{13}(n,6) &= \left(\frac{n}{-1+3\omega}\right)_3 \Big|_{n=1,\dots,13} = \{1,\omega^2,\omega^2,\omega,1,\omega,\omega,1,\omega,\omega^2,\omega^2,1,0\}, \\ f_{19}(n,2) &= \left(\frac{n}{2-3\omega}\right)_3 \Big|_{n=1,\dots,19} = \{1,\omega,\omega,\omega^2,\omega,\omega^2,\omega,1,1,\omega^2,\omega^2,1,1,\omega^2,\omega,\omega^2,\omega,\omega,1,0\}, \\ f_{19}(n,10) &= \left(\frac{n}{5+3\omega}\right)_3 \Big|_{n=1,\dots,19} = \{1,\omega^2,\omega^2,\omega,\omega^2,\omega,1,1,\omega,\omega,1,1,\omega,\omega^2,\omega,\omega^2,\omega^2,1,0\}, \end{split}$$

A Dirichlet character χ 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]

$$\left(\frac{n}{a+bi}\right)_4$$

to be 0 if n is divisible by a + bi; otherwise it is the unique power i^j for $0 \le j \le 3$ 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:

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

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

$$\begin{split} f_5(n,2) &= \left(\frac{n}{-1-2i}\right)_4 \Big|_{n=1,\dots,5} = \{1,i,-i,-1,0\}, \\ f_5(n,3) &= \left(\frac{n}{-1+2i}\right)_4 \Big|_{n=1,\dots,5} = \{1,-i,i,-1,0\}, \\ f_{13}(n,2) &= \left(\frac{n}{3-2i}\right)_4 \Big|_{n=1,\dots,13} = \{1,i,1,-1,i,i,-i,-i,1,-1,-i,-1,0\}, \\ f_{13}(n,7) &= \left(\frac{n}{3+2i}\right)_4 \Big|_{n=1,\dots,13} = \{1,-i,1,-1,-i,-i,i,i,1,-1,-i,-1,0\}, \\ g_{15}(n,2)|_{n=1,\dots,15} &= \{1,i,0,-1,0,0,-i,-i,0,0,-1,0,i,1,0\}, \\ g_{15}(n,8)|_{n=1,\dots,15} &= \{1,-i,0,-1,0,0,i,i,0,0,-1,0,-i,1,0\}, \\ g_{16}(n,3)|_{n=1,\dots,16} &= \{1,0,i,0,-i,0,-1,0,-1,0,i,0,-i,0,1,0\}, \\ g_{16}(n,5)|_{n=1,\dots,16} &= \{1,0,i,0,i,0,1,0,-1,0,-i,0,-i,0,-1,0\}, \\ h_{16}(n,3,5,9)|_{n=1,\dots,16} &= \{1,0,i,0,i,0,1,0,-1,0,-i,0,-i,0,-1,0\}, \end{split}$$

$$\begin{split} h_{16}(n,11,13,9)\big|_{n=1,\dots,16} &= \{1,0,-i,0,-i,0,1,0,-1,0,i,0,i,0,-1,0\},\\ f_{17}(n,3) &= \left. \left(\frac{n}{1-4i}\right)_4 \right|_{n=1,\dots,17} = \{1,-1,i,1,i,-i,-i,-1,-1,-i,-i,i,1,i,-1,1,0\},\\ f_{17}(n,6) &= \left. \left(\frac{n}{1+4i}\right)_4 \right|_{n=1,\dots,17} = \{1,-1,-i,1,-i,i,i,-1,-1,i,i,-i,1,-i,-1,1,0\},\\ g_{20}(n,3)\big|_{n=1,\dots,20} &= \{1,0,i,0,0,0,-i,0,-1,0,-1,0,-i,0,0,0,i,0,1,0\},\\ g_{20}(n,7)\big|_{n=1,\dots,20} &= \{1,0,-i,0,0,0,i,0,-1,0,-1,0,i,0,0,0,-i,0,1,0\}, \end{split}$$

$$g_{35}(n,2)|_{n=1,\dots,35} = \{1, i, i, -1, 0, -1, 0, -i, -1, 0, 1, -i, i, 0, 0, 1, -i, -i, 1, 0, 0, i, -i, 1, 0, -1, -i, 0, -1, 0, -1, i, i, 1, 0\},\$$

$$g_{35}(n,18)|_{n=1,\dots,35} = \{1,-i,-i,-1,0,-1,0,i,-1,0,1,i,-i,0,0,1,i,i,1,0,0,-i,i,1,0,-1,i,0,-1,-i,-i,1,0\},$$

$$\begin{aligned} f_{37}(n,5) &= \left. \left(\frac{n}{-1-6i} \right)_4 \right|_{n=1,\dots,37} \\ &= \left. \{ 1,-i,-1,-1,i,i,1,1,-1,1,i,-i,-i,1,i,-i,i,-i,-i,-i,-i,-i,-i,1,1,i,-1,0 \}. \end{aligned}$$

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,

primitive quadratic Dirichlet characters of modulus
$$\leq N \sim \frac{6}{\pi^2} N$$
,

- # primitive cubic Dirichlet characters of modulus $\leq N \sim A N$,
- # primitive quartic Dirichlet characters of modulus $\leq N \sim B N \ln(N)$,

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** $\chi \neq 1$:

$$L_{\chi}(z) = \sum_{n=1}^{\infty} \chi(n) n^{-z} = \prod_{p} \left(1 - \chi(p) p^{-z} \right)^{-1}, \quad \text{Re}(z) > 1$$

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

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

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 χ do not yet appear to have precise analogs for primitive cubic characters. Baier & Young [10] proved that

$$\sum_{q \le Q} \sum_{\chi} |L_{\chi}(1/2)|^2 = O\left(Q^{6/5+\varepsilon}\right)$$

as $Q \to \infty$, for any $\varepsilon > 0$, where the big-O constant depends on ε . The inner summation is over all primitive cubic characters modulo q. As a consequence, $L_{\chi}(1/2) \neq 0$ for infinitely many such χ .

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 χ 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],

$$L_{F_d}(z) = \sum_{\substack{a,b\in\mathbb{Z}\\a\equiv 1 \mod 3\\b\equiv 0 \mod 3}} (a+b\omega^2) \left(\frac{d}{a+b\omega}\right)_3 (a^2-ab+b^2)^{-z}$$

$$= \sum_{\substack{a,b\in\mathbb{Z}\\a\equiv 1 \mod 3\\b\equiv 0 \mod 3}} (a+b\omega) \left(\frac{d}{a+b\omega^2}\right)_3 (a^2-ab+b^2)^{-z}$$

$$= \prod_{p\equiv 2 \mod 3} (1+p^{1-2z})^{-1} \cdot \prod_{p\equiv 1 \mod 3} (1-c_pp^{-z}+p^{1-2z})^{-1}$$

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 $j \ge 2$, $c_1 = 1$ 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 γ_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 β

•
$$\alpha \equiv d^{(p-1)/3} \gamma_p \mod p$$

•
$$|\alpha| < 2\sqrt{p}$$

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]:

$$\dots, -12, -10, -9, -8, -6, -5, -3, -1, 1, 4, 6, 7, 13, 14, 16, 20, \dots$$

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

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

$$L_{E_n}(z) = \sum_{\substack{a,b\in\mathbb{Z}\\a\equiv 1 \mod 4\\b\equiv 0 \mod 2}} (a-bi) \left(\frac{-n}{a+bi}\right)_4 (a^2+b^2)^{-z}$$
$$= \sum_{\substack{a,b\in\mathbb{Z}\\a\equiv 1 \mod 4\\b\equiv 0 \mod 2}} (a+bi) \left(\frac{-n}{a-bi}\right)_4 (a^2+b^2)^{-z}.$$

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

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

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

$$\dots, -12, -11, -10, -7, -6, -4, -2, -1, 1, 3, 4, 8, 9, 11, 13, 18, \dots$$

is worthy of deeper study.

As a quintic follow-on to [5, 7], we merely mention [16].

References

- [1] S. R. Finch, Quadratic Dirichlet L-series, unpublished note (2005).
- T. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, 1976, pp. 55–62, 138–139, 229; MR0434929 (55 #7892).
- [3] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1998, pp. 234–251; MR1625181 (99d:11092).
- [4] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A060594, A114643, A060839, A160498, A073103 and A160499.
- [5] S. Finch and P. Sebah, Squares and cubes modulo n, arXiv:math/0604465.
- [6] C. David, J. Fearnley and H. Kisilevsky, On the vanishing of twisted L-functions of elliptic curves, *Experiment. Math.* 13 (2004) 185–198; MR2068892 (2005e:11082).

- [7] S. Finch, Quartic and octic characters modulo n, arXiv:0907.4894.
- [8] S. R. Finch, Landau-Ramanujan constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 98–104.
- [9] K. Hardy and K. S. Williams, Evaluation of the infinite series $\sum_{\substack{n=1\\(n/p)=1}}^{\infty} \left(\frac{n}{p}\right)_4 n^{-1}$, *Proc. Amer. Math. Soc.* 109 (1990) 597–603; MR1019275 (90k:11114).
- [10] S. Baier and M. P. Young, Mean values with cubic characters, J. Number Theory 130 (2010) 879–903; arXiv:0804.2233; MR2600408.
- [11] S. R. Finch, Elliptic curves over \mathbb{Q} , unpublished note (2005).
- [12] N. M. Stephens, The diophantine equation $X^2 + Y^2 = DZ^2$ and the conjectures of Birch and Swinnerton-Dyer, J. Reine Angew. Math. 231 (1968) 121–162; MR0229651 (37 #5225).
- [13] D. Zagier and G. Kramarz, Numerical investigations related to the *L*-series of certain elliptic curves, *J. Indian Math. Soc.* 52 (1987) 51–69; MR0989230 (90d:11072).
- [14] H. Cohen, Number Theory. v. 1, Tools and Diophantine Equations, Springer-Verlag, 2007, pp. 566–570; MR2312337 (2008e:11001).
- [15] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A002150, A002151, A002156 and A002158.
- [16] S. Finch and P. Sebah, Residue of a mod 5 Euler product, arXiv:0912.3677.