MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 295-305

CYCLOTOMY AND DELTA UNITS

ANDREW J. LAZARUS

To the memory of Derrick Henry Lehmer

ABSTRACT. In this paper we examine cyclic cubic, quartic, and quintic number fields of prime conductor p containing units that bear a special relationship to the classical Gaussian periods: $\eta_j - \eta_{j+1} + c$ is a unit for periods η_j and $c \in \mathbb{Z}$.

1. INTRODUCTION

In [10], Emma Lehmer discovered that certain well-known families of cubic and quartic fields contained *translation units*, where a translation unit θ differs from a Gaussian period η by a rational integer. She then presented a family of quintic fields with the same property. Schoof and Washington [11] proved the converse of Lehmer's results for cubic fields and those quartic fields in which all units have norm $+1$.

Later D. H. and Emma Lehmer became interested in a cyclotomy where the Gaussian period η was replaced by the difference δ_j of two periods $\eta_j - \eta_{j+1}$. We will show that the fields with analogously-defined delta units are, in the cubic and quartic cases, the same as those already known. In Lehmer's quintic case the situation is more complicated because the ordering of the η's is not unique. The Lehmers observed without proof in [9] that only half of the primitive roots mod p induce an ordering of the η's which give a delta unit in the quintic field of conductor p. We investigate this phenomenon.

2. DEFINITIONS

The cyclotomic classes of degree e and prime conductor $p = ef + 1$ are

$$\mathscr{C}_j = \{g^{e\nu+j} \bmod p : \nu = 0, \dots, f-1\}, \qquad j = 0, \dots, e-1,$$

where g is any primitive root mod p. Here, $\mathscr{C}_0$ contains the eth-power residues, but the ordering of the other classes depends upon the choice of g. The Gaussian periods η are defined by

$$\eta_j = \sum_{\nu \in \mathscr{C}_j} \zeta_p^\nu, \qquad j = 0, \dots, e-1, \tag{2.1}$$

Received by the editor June 26, 1992.
1991 *Mathematics Subject Classification*. Primary 11R27, 11R16, 11R20; Secondary 11L99.
Key words and phrases. Units, cyclotomy, Gaussian periods.

where $\zeta_p = \exp(2\pi i/p)$. The Lagrange resolvent τ, sometimes called a Gauss sum, of a character χ of order e (e.g., χ is a complex-valued eth-power residue symbol) is

$$\tau(\chi) = \sum_{j=0}^{p-1} \chi(j)\zeta_p^j.$$

When χ is taken to be the character defined by $\chi(g) = \zeta_e$, the well-known fundamental relations between Gaussian periods and Lagrange resolvents are given by

$$(2.2) \qquad \tau(\chi^j) = \sum_{k=0}^{e-1} \zeta_e^{jk}\eta_k, \qquad \eta_k = e^{-1}\sum_{j=0}^{e-1} \zeta_e^{-jk}\tau(\chi^j).$$

The delta cyclotomy is defined by

$$(2.3) \qquad \delta_j = \eta_j - \eta_{j+1}.$$

Here and throughout, indices of η and δ should be understood $\bmod e$; when omitted, we mean to refer to any η or δ's. The different orderings of the η's induce different values of the δ's.

A unit θ such that $\theta = \eta + c$ for some $c \in \mathbb{Z}$ is called a *translation unit.* If $\theta = \delta + c$ for some δ defined by (2.3), then θ is a *generalized delta unit*; if $\theta = \delta \pm 1$, then θ is a *delta unit.*

3. Cubic fields

Since the conductor $p \equiv 1 \bmod 6$, we have the well-known decomposition

$$4p = L^2 + 27M^2, \qquad L \equiv 1 \bmod 3, \quad M > 0.$$

We may assume that g is chosen such that [5, Proposition 1]

$$(3.1) \qquad g^{(p-1)/3} \equiv (L+9M)/(L-9M) \mod p.$$

Theorem 1. *If K is a cyclic cubic field of prime conductor p, the following are equivalent*:

(i) $M = 1$, *so K is a simplest cubic as defined by Shanks* [12].
(ii) *K has a translation unit.*
(iii) *K has a delta unit.*
(iv) *K has a generalized delta unit.*

Proof. (i) ⇒((ii) & (iii)): Shanks showed that the polynomials

$$(3.2) \qquad Y^3 - \frac{L-3}{2}Y^2 - \frac{L+3}{2}Y - 1 = \prod_{j=0}^{2}(Y - \theta_j)$$

generate the cubic fields with $M = 1$. Emma Lehmer showed that $\eta + (L-1)/6$ is one of the units θ [10]. The Lehmers showed in [9] that if $M = 1$, then $\delta - 1$ is a unit.

(iii) ⇒ (iv): Trivial.

(ii) ⇒ (i): This is shown in [11].

(iv) $\Rightarrow$ (i): We can find the minimal polynomial $\mathrm{Irr}_{\mathbb{Q}}\,\delta$ from the definition (2.3) and the *cyclotomic numbers* of order 3. These are defined (for fixed g) by

$$(h, k) = \#\{\nu \in (\mathbb{Z}/p\mathbb{Z})^* : \nu \in \mathscr{C}_h^{(g)}, \nu + 1 \in \mathscr{C}_k^{(g)}\}.$$

There are a number of well-known general formulas satisfied by the cyclotomic numbers (see, e.g., [1, 13]), including

$$\eta_a\eta_{a+k} = \epsilon^{(k)} f + \sum_{h=0}^{e-1}(h, k)\eta_{a+h}, \tag{3.3}$$
$$\epsilon^{(k)} = \begin{cases} 1, & k = 0,\ f \text{ even, or } k = e/2,\ f \text{ odd}, \\ 0, & \text{otherwise}. \end{cases}$$

The cyclotomic numbers for $e = 3$ were determined in principle by Gauss. For g normalized by (3.1), we have [5, Proposition 1, misprint corrected]

$$\begin{aligned} (00) &= (p - 8 + L)/9, \\ (11) = (20) = (02) &= (2p - 4 - L - 9M)/18, \\ (01) = (10) = (22) &= (2p - 4 - L + 9M)/18, \\ (12) = (21) &= (p + 1 + L)/9. \end{aligned}$$

It is now a routine computation to find that

$$\mathrm{Irr}_{\mathbb{Q}}\,\delta = X^3 - pX + Mp.$$

We are therefore looking to solve

$$N_{\mathbb{Q}}^{K}(\delta + c) = c^3 - p(c + M) = \pm 1. \tag{3.4}$$

If $c = -1$, it is immediate that the only solution is $M = 1$ and a norm of -1. If $c = 1$, there are no units. First, $p = 7$ (where $M = 1$) can be checked as a special case. For $p > 7$, we have $1 - p + M < 1 + 2\sqrt{p} - p < -1$. This shows (iii) $\Rightarrow$ (i).

Generalized delta units of norm $+1$ would be, from (3.4), solutions to

$$(c - 1)(c^2 + c + 1) = p(c + M).$$

Since p is prime, it divides one of the factors on the left. If

$$dp = c^2 + c + 1, \tag{3.5}$$

then

$$d(c - 1) = c + M. \tag{3.6}$$

Isolating M, gives

$$M = cd - c - d = (c - 1)(d - 1) - 1. \tag{3.7}$$

From (3.5) and $p > 0$ we have $d > 0$. Combining this with (3.7) and $M > 0$ forces $d \geq 2$ and $c \geq 2$. When $c = 2$, hence $p = 7$ and $M = 1$, (3.6) is not satisfied. When $c = 3$, then $d = 1$, a contradiction. When $c = 4$, then $p = 7$ and $d = 3$, which gives $M = -5$, also a contradiction. Therefore, we may assume $c \geq 5$. Starting from (3.5), we have

$$dp < 2c^2 \Rightarrow L^2 + 27M^2 < \frac{8c^2}{d} \Rightarrow M < \frac{2\sqrt{2}c}{3\sqrt{3d}} < \frac{5c}{9}.$$

Plugging this back into (3.6), we have

$$d(c-1) < \frac{14c}{5} \Rightarrow d < \frac{14c}{5(c-1)} < 2$$

(since $c \geq 5$), a contradiction.

Now suppose

$$dp = c - 1, \tag{3.8}$$

so

$$M = d(c^2 + c + 1) - c. \tag{3.9}$$

If $c = 1$, we would have from (3.8) that $d = 0$ and then from (3.9), $M = -1$, impossible. Moreover, $\operatorname{sgn} d = \operatorname{sgn} c$ by (3.8). When both are negative,

$$M < d(c^2 + c + 1) + dc = d(c+1)^2 \leq 0,$$

a contradiction. For $c > 1$, we must have that $c \geq 8$, since $p \geq 7$. Now

$$p \leq dp < c \Rightarrow M^2 < \frac{4c}{27} \Rightarrow M < \sqrt{c}.$$

Combining this with (3.9) gives the inequality $c^2 + 1 < \sqrt{c}$, which never holds. Hence, there are no generalized delta units of norm $+1$.

For the norm -1 case we are looking for solutions to

$$(c+1)(c^2 - c + 1) = p(c + M).$$

Proceeding similarly to the positive-norm case, we first consider the possibility that $dp = c^2 - c + 1$ and $M = cd - c + d = (c+1)(d-1) + 1$. As before, $d > 0$. If $d = 1$, we see that $M = 1$ is a solution to (3.4), regardless of c. From now on, assume $d > 1$. If $c \leq 2$, then either $p < 7$ or $M < 0$, which are impossible. Assume $c \geq 3$. Then

$$dp < 2c^2 \Rightarrow M < \frac{2\sqrt{2}c}{3\sqrt{3d}} \Rightarrow d(c+1) < \frac{14c}{5} \Rightarrow d < \frac{14c}{9(c+1)} < 2,$$

contradicting the assumption $d \geq 2$.

The remaining case is $dp = c + 1$. We have $M = d(c^2 - c + 1) - c$. If $c = -1$, then $d = 0$ and $M = 1$, a solution to (3.4). If $c < -1$, then $d < 0$. Now

$$M = d(c^2 - c + 1) - c < d(c^2 - c + 1) + dc < d(c^2 + 1) < 0,$$

a contradiction. It remains to check only $c \geq 0$. Immediately we get $d > 0$. But then, as with $dp = c - 1$, we quickly get a contradiction:

$$p < dp < 2c \Rightarrow M < \sqrt{c} \Rightarrow c^2 - c + 1 < c + \sqrt{c},$$

and since $c \geq 6$, this, too, is impossible. □

We found all solutions to (3.4) during the proof of the theorem and summarize this result.

Corollary 3.1. *All generalized delta units have norm* -1. *If* $M \neq 1$, *there are no generalized delta units. If* $M = 1$, *then* $\delta - 1$ *is a unit. If, in addition, there exists* $c \in \mathbb{Z}$ *such that* $p = c^2 - c + 1$, *then* $\delta + c$ *and* $\delta - (c - 1)$ *are also units.*

Shanks [12] showed that when $M = 1$, the group generated by -1 and any two of the units θ_j in (3.2) is the full unit group, and that Galois action on the units θ is given by the map $\theta \to -(\theta + 1)^{-1}$. Since η_0 is invariant under choice of g, we fix θ_0.

Proposition 3.2. *The ordering of the* η *induced by* $\theta_0 = \eta_0 - (L + 1)/6$ *and Shanks's map* $\theta_{j+1} = -(\theta_j + 1)^{-1}$ *coincides with the ordering obtained by* (2.1) *and* (3.1).

Proof. We find that

$$\begin{aligned}(\eta_1 &+ (L-1)/6)(\eta_0 + (L+5)/6)\\ &= \tfrac{1}{36}(36\,\eta_0\eta_1 + 6\,\eta_1 L + 30\,\eta_1 + 6\,L\eta_0 + L^2 + 4\,L - 6\,\eta_0 - 5)\\ &= \tfrac{1}{36}(4\,\eta_0 p + 10\,\eta_0 - 2\,\eta_0 L + 4\,\eta_1 p - 26\,\eta_1 - 2\,\eta_1 L + 4\,\eta_2 p + 4\,\eta_2 + 4\,\eta_2 L)\\ &= -1,\end{aligned}$$

expanding $\eta_0\eta_1$ by (3.3) and substituting in $\eta_2 = -1 - \eta_0 - \eta_1$ and $p = (L^2 + 27)/4$. Therefore, $\theta_1 = -(\theta_0 + 1)^{-1}$. Applying Galois action to both sides proves the general case. □

Hasse [4] wrote elements of cyclic cubic fields as $[x, y]$, where

$$[x, y] = x - y\tau(\chi) - \overline{y\tau(\chi)} \in K,$$

$$x \in \mathbb{Z},\quad y \in \mathbb{Q}[\zeta_3],\quad \chi(\cdot) = \left(\frac{\cdot}{(L + 3\sqrt{-3}M)/2}\right)_3.$$

He normalized Galois action so that $[x, y] \to [x, \zeta_3 y]$. (Warning: Hasse used $L \equiv -1 \bmod 3$.)

Proposition 3.3. *Shanks's map is the inverse of Galois action as normalized by Hasse.*

Proof. It is evident from the relations (2.2) that Hasse's map takes

$$\eta_0 = (1 + \tau(\chi) + \tau(\bar{\chi}))/3 \to (1 + \zeta_3\tau(\chi) + \zeta_3^2\tau(\bar{\chi}))/3 = \eta_2,$$

whereas the previous proposition shows that Shanks's map increments the index of η. □

Delta units and the choice of g. Fix, for the moment, the choice of g. In general, redefining the periods using a generator $g' \in \mathscr{C}_j^{(g)}$ yields $\eta'_\nu = \eta_{\nu j}$. If $g' \in \mathscr{C}_{-1}^{(g)}$, then $\delta'_\nu = -\delta_{e-\nu}$. Therefore, in looking for delta units, $\mathscr{C}_j^{(g)}$ and $\mathscr{C}_{-j}^{(g)}$ can be paired, so $\phi(e)/2$ essentially distinct delta polynomials must be considered. Therefore, when $e < 5$, the existence of delta units does not depend on the choice of g. For cubic fields, choosing a primitive root from the other class of cubic nonresidues $\mathscr{C}_2$ changes the signs of δ, c, and the norm of the delta units.

4. Quartic fields

Because we are interested in both cyclotomy and units, we will consider only the real fields, where $p \equiv 1 \bmod 8$. (The unit groups of the imaginary quartic fields are generated, up to torsion, by quadratic units.) Here we will use the normalization

$$p = a^2 + b^2, \qquad b \equiv 0 \bmod 4, \ b > 0, \ a \equiv 1 \bmod 4,$$

and a primitive root g is chosen (per [7]) with

$$g^{(p-1)/4} \equiv a/b \mod p. \tag{4.1}$$

Theorem 2. *If K is a real cyclic quartic field of prime conductor p, the following are equivalent:*

(i) *$b = 4$, so K is a simplest quartic field as defined by Gras* [3].
(ii) *K has a translation unit of norm $+1$.*
(iii) *K has a delta unit.*
(iv) *K has a generalized delta unit of norm $+1$.*

Proof. (i)$\Rightarrow$((ii) & (iii)): Emma Lehmer showed that if $b = 4$, then $-\eta + (a-1)/4$ is a root of the Gras quartic polynomial [3]

$$Y^4 - aY^3 - 6Y^2 + aY + 1, \tag{4.2}$$

so it is a unit of norm $+1$ [10, equation (4.5), corrected]. The Lehmers later showed that if $b = 4$, then either $\delta + 1$ or $\delta - 1$ is a unit [9], without determining which sign held for a particular g.

(iii)$\Rightarrow$((iv) & (i)): Since Hasse's [4] normalization for quartic fields agrees with ours, we will use it to obtain $\mathrm{Irr}_{\mathbb{Q}}\,\delta$. The symbol $[x_0, x_1, y_0, y_1]$ will represent the element of K given by

$$[x_0, x_1, y_0, y_1] = \tfrac{1}{4}(x_0 - x_1\sqrt{p} + (y_0 + iy_1)\tau(\chi) + (y_0 - iy_1)\overline{\tau(\chi)}),$$

where χ is the quartic character belonging to K, viz., the quartic residue symbol $\left(\frac{\cdot}{a+bi}\right)_4$. (Condition (4.1) is equivalent to $\chi(g) = i$ [7].) A general formula for the minimal polynomial of any element written in this way appears in [8] (or see Gras [3]). From (2.2),

$$\delta_0 = \eta_0 - \eta_1 = [-1, -1, 1, 0] - [-1, 1, 0, -1] = [0, -2, 1, 1].$$

The minimal polynomial formula now gives

$$\mathrm{Irr}_{\mathbb{Q}}\,\delta = Y^4 - p(Y + b')^2, \qquad b' = b/4,$$

whence

$$N_{\mathbb{Q}}^{K}(\delta + c) = c^4 - p(b' - c)^2. \tag{4.3}$$

Immediately we have $c = 1 \Rightarrow b = 4$ and norm $+1$; $c = -1$ is impossible.

(ii)$\Rightarrow$ (i): Proven in [11].

(iv) $\Rightarrow$ (i): From (4.3), units of norm $+1$ will be solutions to

$$c^4 - 1 = (c+1)(c-1)(c^2+1) = p(b'-c)^2. \tag{4.4}$$

There are no primes $\equiv 1 \bmod 8$ dividing the left side for $c = \pm 2, \pm 3$, and when $c = \pm 4$, the prime $p = 17$ divides the left side, but $p = 17$ implies $b' = 1$ and (4.4) is not satisfied. The cases $c = \pm 1$ have been handled above, so we may assume $|c| \geq 5$.

Supposing, first, that $dp = c+1$, we have $b' = c \pm \sqrt{d(c-1)(c^2+1)}$. The minus root gives $b' < 0$, impossible. The plus root gives $b' > |c|^{3/2} + c > |c|^{3/2}/4$. Then $b > |c|^{3/2}$, so $p > |c|^3$. Since $(b'-c)^2 > \frac{124}{125}|c|^3$, we are reduced to the inequality $c^4 > \frac{124}{125}c^6$, which is never true for $|c| \geq 5$. The case $dp = c-1$ is virtually identical. The case $dp = c^2+1$ is similar. Here, $b' = c \pm \sqrt{d(c^2-1)}$. Since $b' \in \mathbb{Z}$ and $c \neq \pm 1$, we cannot have $d = 1$, so the minus root is impossible. Then

$$b' > \frac{\sqrt{24}(\sqrt{2}-1)}{5}|c| > \frac{2|c|}{5} \Rightarrow p > \frac{64}{25}c^2 \Rightarrow c^4 - 1 = p(b'-c)^2 > 3c^4,$$

which again has no solution. □

We have also proved *en passant*:

Corollary 4.1. *A generalized delta unit of norm* $+1$ *is a delta unit with* $c = 1$. *If* $\theta = \delta \pm 1$ *is a delta unit, then* $b = 4$, *the plus sign holds, and* $N_{\mathbb{Q}}^{K}\theta = 1$.

Gras showed that Galois action on the roots θ of (4.2) is given by $\theta_{j+1} = (\theta_j - 1)/(\theta_j + 1)$.

Proposition 4.2. *The ordering of the* η *induced by* $\theta_0 = -\eta_0 + (a-1)/4$ *and Gras's map* $\theta_{j+1} = (\theta_j - 1)/(\theta_j + 1)$ *coincides with the ordering obtained by* (2.1) *and* (4.1). *Gras's map is the inverse of Galois action as normalized by Hasse.*

Proof. The identity $\theta_1(\theta_0 + 1) = \theta_0 - 1$, which suffices to prove the first statement, was verified using the rule for multiplication in Hasse's basis [4, §8(1)]. Hasse normalized Galois action so that $[x_0, x_1, y_0, y_1] \to [x_0, -x_1, -y_1, y_0]$, and the proof of the second statement is analogous to Proposition 3.3. □

Remarks. (1) Choosing a generator from the other class of nonresidues $\mathscr{C}_3$ changes the sign of all δ, hence c.

(2) The only known example of a translation unit of norm -1 is $\eta - 2$ in the field of conductor 401 [11]. This field does not contain a generalized delta unit. The only generalized delta unit of norm -1 which we have found is $\delta + 2$ in the field of conductor 17, which also contains delta units; no others can exist for $c^4 + 1$ squarefree.

5. Quintic fields

Dickson showed [2] that the conductor $p \equiv 1 \bmod 5$ may be decomposed as

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2,$$

subject to

$$xw = v^2 - 4uv - u^2, \qquad x \equiv 1 \bmod 5.$$

If (x, u, v, w) is one solution to this system, the others are $(x, -v, u, -w)$, $(x, v, -u, -w)$, and $(x, -u, -v, w)$. If g is a primitive root $\bmod p$, Katre and Rajwade proved in [6] that (x, u, v, w) can be defined unambiguously, given g, by the additional condition

$$g^{(p-1)/5} \equiv (a - 10b)/(a + 10b) \bmod p, \qquad a = x^2 - 125w^2, \quad b = 2xu - xv - 25vw. \tag{5.1}$$

Conversely, if a choice of (x, u, v, w) is fixed, primitive roots g in only one of the four classes of quintic nonresidues in $\mathbb{Z}/p\mathbb{Z}$ will satisfy (5.1). The cyclotomic numbers for such g are given by

$$\begin{aligned} (00) &= (p - 14 + 3x)/25, \\ (01) = (10) = (44) &= (4p - 16 - 3x + 50v + 25w)/100, \\ (02) = (20) = (33) &= (4p - 16 - 3x + 50u - 25w)/100, \\ (03) = (30) = (22) &= (4p - 16 - 3x - 50u - 25w)/100, \\ (04) = (40) = (11) &= (4p - 16 - 3x - 50v + 25w)/100, \\ (12) = (21) = (34) = (43) = (14) = (41) &= (2p + 2 + x - 25w)/50, \\ (13) = (31) = (23) = (32) = (24) = (42) &= (2p + 2 + x + 25w)/50. \end{aligned} \tag{5.2}$$

If we set $\delta_j = \eta_j - \eta_{j+1}$, we have, by direct computation,

$$\begin{aligned} \operatorname{Irr}_{\mathbb{Q}} \delta = \Delta(Y) = Y^5 - Y^3 p + Y^2 vp & \\ + \frac{p\left((3u + v)(u - v) + 5w^2\right) Y}{4} & \\ + \frac{p(u(u - v)^2 + (3u - 4v)w^2)}{4} & . \end{aligned} \tag{5.3}$$

In the quintic case, defining the periods η' with $g' \in \mathscr{C}_2^{(g)}$ effects the substitution $(x, u, v, w) \to (x, -v, u, -w)$. Hence, the minimal polynomial of $\delta'_j = \eta'_j - \eta'_{j+1} = \eta_{2j} - \eta_{2(j+1)}$ is given by

$$\begin{aligned} \Delta'(Y) = Y^5 - Y^3 p + Y^2 up & \\ + \frac{p\left((3v - u)(v + u) + 5w^2\right) Y}{4} & \\ - \frac{p(v(v + u)^2 + (3v + 4u) w^2)}{4} & . \end{aligned} \tag{5.4}$$

The quintic analogue to a simplest field was given by Emma Lehmer in [10]. For $n \in \mathbb{Z}$ set

$$u = n + 1, \qquad v = n + 2, \qquad w = \left(\frac{n}{5}\right)_2,$$

from which it follows that $x = -\left(\frac{n}{5}\right)_2(4n^2 + 10n + 5)$ and

$$p = n^4 + 5n^3 + 15n^2 + 25n + 25. \tag{5.5}$$

Lehmer showed that

$$\theta = w\eta - (w - n^2)/5 \tag{5.6}$$

is a translation unit up to sign.

The normalization (5.1) of g reduces to

$$\begin{gathered} g^{(p-1)/5} \equiv (a - 10b)/(a + 10b) \bmod p, \\ a = 4(4n^4 + 30n^2 + 25), \quad b = -2\left(\frac{n}{5}\right)_2 (2n^3 + 20n + 25). \end{gathered} \tag{5.7}$$

Theorem 3. *Suppose p is of type* (5.5) *and g is chosen such that* (5.7) *holds. Then $\delta - 1$ is a unit. If $p \neq 11$,*

(i) *$\delta - 1$ is the only generalized delta unit, and*
(ii) *$\delta' + c$ is never a unit.*

Proof. For such p, $\Delta(Y)$ reduces to

$$\begin{aligned} &Y^5 - pY^3 + p(n+2)Y^2 - pnY - p \\ &\quad = 1 + (Y-1)(Y^4 + Y^3 - (p-1)Y^2 + [p(n+1)+1]Y + p + 1). \end{aligned}$$

Clearly, $\delta - 1$ is a unit of norm -1. The equations $N_{\mathbb{Q}}^K(\delta - c) \pm 1 = \Delta(c) \pm 1 = 0$ may be considered as quintic polynomials in c. The lack of integer solutions to the unit equations may be proved by locating their irrational solutions between consecutive integers. If $n \geq 1$, then $\Delta(c) + 1$ has a root in each open interval $(\hat{c}, \hat{c} + 1)$ for

$$\hat{c} \in \{-n^2 - 3n - 6, -1, 0, n + 1, n^2 + 2n + 3\}.$$

In each case, $\operatorname{sgn}(\Delta(\hat{c}) + 1) \neq \operatorname{sgn}(\Delta(\hat{c} + 1) + 1)$. This accounts for all five roots, so there are no generalized delta units when $n \geq 1$. The polynomial $\Delta(c) - 1$ has an exact root at $c = 1$ instead of an irrational root in $(0, 1)$; otherwise, its four irrational roots are located in the same intervals. Similar results hold for $n < -3$. The case $n = -3$ yields no solutions for c, which leaves only $p = 11$. Hence (i). For the proof of (ii), replace Δ by Δ' and proceed in the same way. □

Corollary 5.1. *Take x, u, v, w, p, a, and b as above and define the periods with an arbitrary primitive root g. If $p = 11$, all g define an ordering such that $\Delta(Y)$ has delta units. Otherwise, $\Delta(Y)$ has delta units if and only if g satisfies*

$$g^{(p-1)/5} \equiv \left(\frac{a - 10b}{a + 10b}\right)^{\pm 1} \quad \bmod p.$$

These are the g in two (*i.e., half*) *of the four nonresidue classes.*

Proof. This is immediate from the theorem and (5.1). □

The field of conductor 11 is a special case. It is of type (5.5) with either $n = -2$ or $n = -1$. (One can show that 11 is the only integer represented nonuniquely by the polynomial (5.5).) The period polynomial for $p = 11$ is

$$Y^5 + Y^4 - 4Y^3 - 3Y^2 + 3Y + 1,$$

so the periods η are themselves units. Also $\eta \pm 1$ and $\eta + 2$ are Galois-conjugate units (but not conjugate to η). Choosing to use $n = -2$, we have from (5.3) and (5.4) that $\delta - 1$, $\delta + 2$, $\delta - 3$, $\delta' \pm 1$, and $\delta' + 2$ are all units, no two conjugate.

The converse of Theorem 3 is false. In the field of conductor 211 using $(x, u, v, w) = (1, 1, 2, -5)$, $\delta - 1$ is a unit of norm -1. There is a generalized delta unit $\delta - 3$ for $p = 61$ and $(x, u, v, w) = (1, 1, 4, -1)$.

Schoof and Washington showed that Galois action on the quintic translation units (5.6) can be given by

$$\theta \to \frac{(n+2) + n\theta - \theta^2}{1 + (n+2)\theta}. \tag{5.8}$$

When g satisfies (5.7), then (5.6) induces an ordering of the θ_j. The method of Proposition 3.2 can be used to show that with this ordering the image of θ_0 under (5.8) is θ_2 when $w = 1$, and θ_3 when $w = -1$. In [11], the map (5.8) was derived from (5.6) and the canonical ordering of the η_j, but we have changed the normalization of (x, u, v, w) from [10] and [11]. The normalizations (3.1), (4.1), and (5.1) all follow naturally from Jacobi sums; they insure that the character defined by $\chi(g) = \zeta_e$ coincides with the particular eth-power residue symbol modulo p belonging to the field K [5]. Using Lehmer's u and v with normalized g makes the units translates of δ' instead of δ. Changing u and v seemed the lesser evil.

Remark. We were unable to find any infinite family of quintic fields with generalized delta units containing either $p = 61$ or $p = 211$. Furthermore, we were unable to make any progress on the conjecture of Schoof and Washington in [11] that all quintic fields with translation units are of Emma Lehmer's form (5.5).

Bibliography

1. Paul Bachmann, *Die Lehre von der Kreisteilung*, Teubner, Leipzig and Berlin, 1927.

→ Leonard E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.

3. Marie-Nicole Gras, *Table numérique du nombre de classes et des unités des extensions cycliques de degré 4 de* $\mathbb{Q}$, Publ. Math. Fasc. 2, Fac. Sci. Besançon, 1977/1978.

4. Helmut Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Math. Abhandlungen, vol. 3, Walter deGruyter, Berlin, 1975, pp. 285–379; originally published 1950.

5. S. A. Katre and A. R. Rajwade, *Complete solution of the cyclotomic problem in* F_q *for any prime modulus* l, $q = p^\alpha$, $p \equiv 1 \pmod{l}$, Acta Arith. **45** (1985), 183–199.

6. ———, *Unique determination of cyclotomic numbers of order five*, Manuscripta Math. **53** (1985), 65–75.

7. ———, *Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum*, Math. Scand. **60** (1987), 52–62.

8. Andrew J. Lazarus, *Gaussian periods and units in certain cyclic fields*, Proc. Amer. Math. Soc. **115** (1992), 961–968.

9. D. H. Lehmer and Emma Lehmer, *The Lehmer project*, Math. Comp. **61** (1993), 313–317.

10. Emma Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541.

11. René Schoof and Lawrence C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556.

12. Daniel Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

13. Thomas Storer, *Cyclotomy and difference sets*, Markham, Chicago, 1967.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, DAVIS, CALIFORNIA 95616
Current address: 2745 Elmwood Avenue, Berkeley, California 94705