MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 182
APRIL 1988, PAGES 535-541

Connection Between Gaussian Periods and Cyclic Units

By Emma Lehmer

Abstract. This paper finds that all known parametric families of units in real quadratic, cubic, quartic and sextic fields with prime conductor are linear combinations of Gaussian periods and exhibits these combinations. This approach is used to find new units in the real quintic field for prime conductors $p = n^4 + 5n^3 + 15n^2 + 25n + 25$.

1. Introduction. The idea that it might be of interest to explore the connection between Gaussian periods and cyclic units arose from the obvious fact that for $4p = L^2 + 27$ Shanks's "simplest cubic" [10] and the Gaussian cubic are related by a translation. Moreover, this is also the case for $p = a^2 + 16$ for Marie Gras's "simplest quartic" [2] and the cyclotomic quartic, as well as the "simplest quadratic" in [10].

Since there were no known quintic units, while the cyclotomic quintic polynomial [6] and its discriminant [7] were given by the author many years ago, it seemed worthwhile to try to discover some quintic units as linear transforms of the periods for some sequence of primes. This was accomplished for primes of the form

$$p = n^4 + 5n^3 + 15n^2 + 25n + 25.$$

Subsequently, it was shown by René Schoof and Lawrence Washington [9] that these were indeed fundamental units.

In another direction, Marie Gras [1], and later Günter Lettl [8], considered for $4p = 1 + 27M^2$ a cubic whose roots are units, but which is no longer a translation of the Gaussian cubic. However, its roots are linear combinations of the roots of the Gaussian cubic and therefore generalized Gaussian periods. A similar relation holds between the roots of Marie Gras's quartic [2] for $p = 1 + 16b^2$ and the cyclotomic quartic, except that the coefficients in the linear combination of the roots are excessively large, as we shall see in Section 4. Section 6 will be devoted to similar results for the sextic with $4p = L^2 + 27$, given by Marie Gras [3], [4]. We have not studied the case of $4p = 1 + 27M^2$, but we expect that there exists a similar relation.

2. Notation. We will use the notation of cyclotomy as follows: $p = ef + 1$ is a prime, where e is the degree of the polynomial

$$F_e(x) = \prod_{j=0}^{e-1} (x - \eta_j) \tag{2.1}$$

Received July 1, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R11, 11R16, 11R21, 11R27.

with discriminant $D(F_e)$, where the roots η_j of $F_e(x)$ for $j = 0, 1, \ldots, e-1$ are given by

$$\eta_j = \sum_{i \in C_j} \zeta_p^i \qquad (j = 0, 1, \ldots, e-1), \tag{2.2}$$

where C_j is the jth coset of eth power residues and ζ_p^ν are the primitive pth roots of unity. Kummer also considered a generalized cyclotomy in which, with integer c_i,

$$\theta_j = \sum_{i=0}^{e-1} c_i \eta_{i+j}. \tag{2.3}$$

He proved that for e a prime, all the factors of the discriminant and of the numbers represented by the polynomial whose roots are the generalized periods must be eth power residues of p. When e is composite, however, the polynomial may have exceptional factors which must divide the discriminant. In what follows we will be considering a special case of generalized periods θ_j which are units. We will show that every known cyclic unit is a generalized Gaussian period and find the actual constants c_i in (2.3).

3. The Cubic Case. The Gaussian cubic for $4p = L^2 + 27M^2$ is

$$F_3(x) = x^3 + x^2 - \frac{(p-1)}{3}x - [(L+3)p - 1]/27 \tag{3.1}$$

with discriminant $D(F_3) = p^2M^2$.

Shanks's "simplest" cubic is given by [10]

$$P_3(y) = y^3 - ty^2 - (t+3)y - 1 \tag{3.2}$$

with $D(P_3) = (t^2 + 3t + 9)^2 \equiv p^2$.

If $M = 1$, then $t = (L-3)/2$, $D(F_3) = D(P_3)$, and as we have said in the introduction, $P_3(y)$ is a linear transform of $F_3(x)$, namely

$$P_3(y) = F_3\left(y - \frac{L-1}{6}\right),$$

so that

$$\theta_i = \eta_i + \frac{L-1}{6}.$$

If $L = 1$, then (3.1) becomes simply

$$F_3(x) = x^3 + x^2 - \frac{9M^2 - 1}{4}x - M^2, \qquad D(F_3) = p^2M^2, \tag{3.3}$$

while $t = 3(9M-1)/2$ in (3.2) with $D(P_3) = 27^2p^2$ [8].

Hence, P_3 can no longer be a linear transform of F_3. However, the equation whose roots are $\delta_i = 3(\eta_i - \eta_{i+1})$, namely

$$G_3(z) = z^3 - 9pz - 27pM \qquad \text{with } D(G_3) = 27^2p^2, \tag{3.4}$$

is a linear transform of $P_3(y)$. In fact,

$$P_3(y) = G_3\left(y - \frac{9M-1}{2}\right),$$

and hence in this case,

$$\theta_i = 3(\eta_i - \eta_{i+1}) + \frac{9M-1}{2}. \tag{3.5}$$

Therefore, all the prime factors of numbers represented by

$$P_3(y) = y^3 - \frac{3}{2}(9M-1)y^2 - \frac{3}{2}(9M+1)y - 1 \tag{3.6}$$

are cubic residues of p, except 3 in case $3 \nmid M$. For example, for $p = 331$, $M = 7$, $P_3(1) = 3^3 \cdot 7$, $P_3(2) = -557$, $P_3(3) = -7 \cdot 157$, $P_3(4) = -3^3 \cdot 67$, $P_3(5) = -7 \cdot 383$.

4. The Quartic Case. The Gaussian quartic for $p = a^2 + 16b^2$ with $a \equiv 1 \pmod 4$ is

$$F_4(x) = x^4 + x^3 - \frac{3(p-1)}{8}x^2 - \frac{3p - 2pa - 1}{16}x + \frac{(p-1)^2 - 4p(a-1)^2}{256} \tag{4.1}$$

with $D(F_4) = 4b^6p^3$, while Marie Gras's quartic [2] is

$$P_4(y) = y^4 - ty^3 - ry^2 + ty + 1. \tag{4.2}$$

She also defines

$$z^2 = (t^2 - 4r - 8)/p \quad \text{and} \quad x^2 + y^2 = (t^2 - 2r + 4)/p. \tag{4.3}$$

As in the cubic case, there are two cases according as $a = 1$ or $b = 1$. In both these cases, the field is totally real. The simplest case is when $b = 1$, so that $p = a^2 + 16$ and $t = a$ and $r = 6$ in (4.2), which becomes

$$P_4(y) = y^4 - ay^3 - 6y^2 + ay + 1, \qquad D(P_4) = D(F_4) = 4p^3. \tag{4.4}$$

It is not hard to verify that

$$P_4(y) = F_4\left(y - \frac{a-1}{4}\right), \tag{4.5}$$

so that in this case,

$$\theta_i = \eta_i + \frac{a-1}{4}.$$

If $a = 1$, then $p = 1 + 16b^2$, and (4.1) reduces to

$$F_4(x) = x^4 + x^3 - 6b^2x^2 - b^2x + b^4, \tag{4.6}$$

while (4.2) has values of t and r that are surprisingly large. They are given by Marie Gras [2] for $p < 10000$. Since there are only five values of $p < 10000$ for which $a = 1$, we reprint the values of t from her tabie together with the values of z derived from her values of r from (4.3) as follows:

p	t	z
257	382352	23504
401	80	10
577	123975327936	5159943648
1297	1194681	33159
1601	575066704688492400	14372175520538672

The discriminant $D(P_4)$ is

$$D(P_4) = \frac{p^3z^4}{16}\left[\left(\frac{t^2+16}{p} + z^2\right)^2 p - 4t^2z^2\right], \tag{4.7}$$

where the expression in square brackets appears to be a square. For example, for $p = 257$, $D(P_4) = 257^3 \cdot 2^{20} \cdot 13^2 \cdot 113^2 \cdot 1621^2 \cdot 10141^2$. We note that all the odd prime factors are quadratic, but not quartic residues of 257, and therefore they are all exceptional. For $p = 401$ we have $D(P_4) = 2^4 5^4 \cdot 401^3 \cdot 421^2$, and 2 and 421 are both quartic residues of 401.

The roots θ_i of (4.2) are negative reciprocals in pairs. Therefore, we can order the θ's so that

$$\theta_0\theta_2 = \theta_1\theta_3 = -1. \tag{4.8}$$

Marie Gras [2] gives two fundamental relations in terms of x, y, z defined in (4.3) for cyclic quartic fields, which in our case can be written:

$$t^2 + pz^2 + 16 = 2p(x^2 + y^2), \qquad -tz = (x^2 - y^2) - 8bxy. \tag{4.9}$$

We next let

$$\theta_i = c_0\eta_i + c_1\eta_{i+1} + c_2\eta_{i+2} + c_3\eta_{i+3} \qquad (i = 0, 1, 2, 3). \tag{4.10}$$

Then (4.8) implies

$$c_0c_2 + c_1c_3 = 2(b^2t^2 - 1)/p. \tag{4.11}$$

Using this and the fact that $\sum_{i=0}^{3} c_i = -t$ and $\sum_{i=0}^{3}(-1)^i c_i = -z$, and that

$$\sum_{i=0}^{3} c_i^2 = [p(t^2 + 2z^2) + t^2 + 16]/4p,$$

we find that (4.9) is satisfied with $c_0 - c_2 = x$ and $c_1 - c_3 = y$, so that

$$\begin{aligned} 2c_0 &= x + (z - t)/2, & 2c_1 &= y - (z + t)/2, \\ 2c_2 &= -x + (z - t)/2, & 2c_3 &= -y - (z + t)/2. \end{aligned} \tag{4.12}$$

The c's given below were actually computed by D. H. Lehmer as a solution of the system (4.10), using his multiprecision package to get the roots of the two equations and then solving the system for the c's.

p	257	401	577	1297	1601
$-c_0$	81543	14	30421906939	318850	152504156397432653
$-c_1$	110033	21	27917477683	278821	135156198948853027
$-c_2$	97881	21	34145728853	295070	142215283707082883
$-c_3$	92895	24	31490214461	301940	145191065635123837

These values of c_i were subsequently checked by (4.2).

5. The Quintic Case. As was mentioned in the introduction, no quintic units were known, but the Gaussian quintic was given in [6] in terms of the Dickson form in four variables (x, u, v, w), which represents

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2 \tag{5.1}$$

with the side conditions

$$xw = v^2 - u^2 - 4uv, \qquad x \equiv 1 \pmod 5. \tag{5.2}$$

After some experimentation it was decided to consider the special case in which x, u, v, w were expressed in terms of a single variable n as follows (where $(\frac{n}{5})$ is the Legendre symbol):

$$v = -(n+1), \quad u = 2+n, \quad w = -\left(\frac{n}{5}\right), \tag{5.3}$$

so that $u + v = 1$ and x is given by (5.2) as

$$x = -\left(\frac{n}{5}\right)(4n^2 + 10n + 5), \tag{5.4}$$

so that, using (5.1), we have

$$x^2 = 16p - 100n^2 - 300n - 375. \tag{5.5}$$

Hence, p is given by the quartic

$$p = n^4 + 5n^3 + 15n^2 + 25n + 25. \tag{5.6}$$

We can now write the polynomial $F_5(t)$ given in [6] in terms of n as follows:

$$\begin{aligned} F_5(t) = {} & t^5 + t^4 - \frac{2}{5}(p-1)t^3 - \frac{1}{25}\left[6p - 2 - \left(\frac{n}{5}\right)p(4n^2+10n+5)\right]t^2 \\ & + \frac{1}{125}\left[-3p^2 + p(25n^2+75n+119) + 1 + 2\left(\frac{n}{5}\right)p(4n^2+10n+5)\right]t \\ & + \frac{1}{3125}\left\{-15p^2 + 5p(25n^2+75n+123) + 1 \right. \\ & \qquad \left. + \left(\frac{n}{5}\right)\left[p^2(4n^2+10n-45) + 5p(-5n^3+29n^2+160n+255)\right]\right\}. \end{aligned} \tag{5.7}$$

It can be verified that the linear transformation

$$t = y - \left[\left(\frac{n}{5}\right) - n^2\right]/5$$

leads to

$$\begin{aligned} P_5(y) = {} & y^5 + n^2y^4 - 2(n^3+3n^2+5n+5)y^3 + (p - 4n^2 - 10n - 20)y^2 \\ & + (n^3 + 4n^2 + 10n + 10)y + 1 \end{aligned} \tag{5.8}$$

with

$$\theta_i = \left(\frac{n}{5}\right)\eta_i + \left[\left(\frac{n}{5}\right) - n^2\right]/5.$$

The discriminant of $F_5(t)$, given in [7], reduces in this case to

$$D(F_5) = D(P_5) = (n^3 + 5n^2 + 10n + 7)^2 p^4. \tag{5.9}$$

Hence all the prime factors of $n^3 + 5n^2 + 10n + 7$ are quintic residues of p and so are the divisors of all the numbers represented by either equation. We give a list of $P_5(y)$, together with their discriminants, for all appropriate primes $p < 1000$:

p	n	$P_5(y)$	$\sqrt{D/p^2}$	$P_5(1)$
11	-2	$y^5 + 4y^4 + 2y^3 - 5y^2 - 2y + 1$	1	1
31	-3	$y^5 + 9y^4 + 20y^3 + 5y^2 - 11y + 1$	5	5^2
71	1	$y^5 + y^4 - 28y^3 + 37y^2 + 25y + 1$	23	37
101	-4	$y^5 + 16y^4 + 62y^3 + 57y^2 - 30y + 1$	17	107
191	2	$y^5 + 4y^4 - 70y^3 + 135y^2 + 54y + 1$	5.11	5^3
631	-6	$y^5 + 36y^4 + 266y^3 + 527y^2 - 122y + 1$	89	709
941	4	$y^5 + 16y^4 - 274y^3 + 817y^2 + 178y + 1$	191	739

There may possibly be a second case for which

$$p = 25n^4 - 25n^3 + 15n^2 - 5n + 1,$$

but we have not been able to find the coefficients, which could be quite large in this case.

6. The Sextic Case. The sextic period polynomials were given in [5]. Recently, Marie Gras [4] has given a sextic whose roots are units in a real sextic field. In the simplest case, in which

$$4p = L^2 + 27, \qquad p \equiv 1 \pmod{12} \text{ and } L \equiv 1 \pmod{6}, \tag{6.1}$$

her equation can be written with $n = |L|$ as

$$P_6(y) = y^6 - (n-3)y^5 - 5\frac{n+3}{2}y^4 - 20y^3 + 5\frac{n-3}{2}y^2 + (n+3)y + 1. \tag{6.2}$$

If we let φ_i be the roots of the cubic (3.2) with $t = (L-3)/2$, then it was shown in [4] that

$$\varphi_i = -(2\theta_{i+1})/(\theta_{i+2}\theta_i), \tag{6.3}$$

where θ_i are the roots of (6.2). Therefore, we have

$$(2\theta_i + 1)/[(\theta_i + 2)\theta_i] = (2\theta_{i+3} + 1)/[(\theta_{i+3} + 2)\theta_{i+3}],$$

which leads to

$$\theta_i + \theta_{i+3} + 2 = -2\theta_i\theta_{i+3}. \tag{6.4}$$

If we now let η_i' be the roots of the Gaussian cubic (3.1), then the roots of the period sextic η_i satisfy

$$\eta_i + \eta_{i+3} = \eta_i'. \tag{6.5}$$

Experiments show that

$$\theta_i = \begin{cases} \dfrac{L-7}{6} - 2\eta_i - \eta_j' & \text{if } L > 0 \\ \dfrac{-L+1}{6} + 2\eta_i + \eta_j' & \text{if } L < 0 \end{cases} \qquad (i \neq j). \tag{6.6}$$

This can be verified, using (6.4) as follows.

First suppose that $L > 0$; then by (6.4) and (6.6) we have

$$\begin{aligned} -2\theta_i\theta_{i+3} &= \frac{L-7}{3} - 2(\eta_i' + \eta_j') + 2 = \frac{L-7}{3} - 2(-1 - \eta_k') + 2 \\ &= \frac{L+5}{3} + 2\eta_k', \\ -\prod_{i=0}^{5}\theta_i &= \prod_{k=0}^{2}\left(\frac{L+5}{6} + \eta_k'\right) = -F_3\left(-\frac{L+5}{6}\right) = -1. \end{aligned}$$

This can be easily verified by substituting $-(L+5)/6$ into (3.1).

Similarly, for $L < 0$ we find that $F_3((-L+1)/6) = 1$.

It is possible that there might exist another case of the sextic for $4p = 1 + 27M^2$ corresponding to the second cubic case, but one may expect very large coefficients in that case.

7. The Octic Case. In this case we consider primes of the form $p = n^4 + 16$ which implies that $p = (n^2 - 4)^2 + 2(2n)^2$. We let

$$\theta_i = \eta_i + \eta_{i+2} - (n^2 - 1)/4 \qquad (i = 0(1)7). \tag{7.1}$$

Then obviously $\theta_i + \theta_{i+4} = \theta_{i+2} + \theta_{i+6}$ and it can be easily seen that $\theta_i\theta_{i+2} = 1/\theta_{i+4}\theta_{i+6}$, so that the θ_{2i} and the θ_{2i+1} respectively satisfy the two quartics

$$x^4 + (n^2 - \sqrt{p})x^3 + \tfrac{1}{2}[n^4 + 4 - \sqrt{p}(n^2 + 2)]x^2 + \tfrac{1}{2}[n^4 - 2n^2 + 16 - \sqrt{p}(n^2 - 2)]x + 1$$

and

$$x^4 + (n^2 + \sqrt{p})x^3 + \tfrac{1}{2}[n^4 + 4 + \sqrt{p}(n^2 + 2)]x^2 + \tfrac{1}{2}[n^4 - 2n^2 + 16 + \sqrt{p}(n^2 - 2)]x + 1,$$

whose product is

$$\begin{aligned} P_8(x) = {} & x^8 + 2n^2x^7 + (p - 28)x^6 - (p + 14n^2)x^5 - [p(n^2 + 3) - 70]x^4 \\ & + [14n^2 - p(n^2 - 4)]x^3 + (5p - 28)x^2 + (p - 2n^2)x + 1, \end{aligned} \tag{7.2}$$

so that the θ's are units. We note that $P_8(-1) = -n^4$.

The discriminant of this equation can be written as

$$D = D_1^2 \cdot D_2^2 \cdot D_3^2 \cdot D_4,$$

where

$$D_j = \prod_{i=1}^{7}(\theta_i - \theta_{i+j}) \qquad (j = 1(1)4).$$

We find that

$$\begin{aligned} D_1 &= p[(n - 4)p + 6n^3 - 24n + 68], & D_2 &= n^4p, \\ D_3 &= p[-(n + 4)p - 6n^3 + 24n + 68], & D_4 &= 16n^4p, \end{aligned}$$

so that D_1 and D_3 interchange with the change of sign of n. All prime factors of D_1 and D_3 are octic residues of p, but 2 and n are only quadratic. For example, for $p = 641$, $n = 5$ and $D_1/p = 13 \cdot 103$, $D_3/p = 13 \cdot 487$.

It remains to be seen whether the θ's are actually relative units in the field defined by (7.2), but we expect this to be the case.

1180 Miller Avenue
Berkeley, California 94708

1. MARIE-NICOLE GRAS, "Sur les corps cubiques cycliques dont l'anneau des entiers est monogène," *Ann. Sci. Univ. Besançon Math.* (3), No. 6, 1973, pp. 1–26.

2. MARIE-NICOLE GRAS, "Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de Q," *Publ. Math. Besançon*, fasc. 2, 1977/78, pp. 1–26, 1–53.

3. MARIE-NICOLE GRAS, "Familles d'unités dans les extensions cycliques réelles de degré 6 de Q," *Publ. Math. Besançon* 1984/85–1985/86.

4. MARIE-NICOLE GRAS, "Special units in real cyclic sextic fields," *Math Comp.*, v. 48, 1987, pp. 179–182.

5. D. H. LEHMER & EMMA LEHMER, "The sextic period polynomials," *Pacific J. Math.*, v. 111, 1984, pp. 341–355.

6. EMMA LEHMER, "The quintic character of 2 and 3," *Duke Math. J.*, v. 18, 1951, pp. 11–18.

7. EMMA LEHMER, "On the divisors of the discriminant of the period equation," *Amer. J. Math.*, v. 90, 1968, pp. 375–379.

8. GÜNTER LETTL, "A lower bound for the class number of certain cubic number fields," *Math. Comp.*, v. 46, 1986, pp. 659–666.

9. RENÉ SCHOOF & LAWRENCE C. WASHINGTON, "Quintic polynomials and real cyclotomic fields with large class numbers," *Math. Comp.*, v. 50, 1988, pp. 543–556.

10. DANIEL SHANKS, "The simplest cubic fields," *Math Comp.*, v. 28, 1974, pp. 1137–1152.