MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 313–317

THE LEHMER PROJECT

D. H. LEHMER AND EMMA LEHMER

ABSTRACT. It is shown that cyclic differences of cyclotomic periods can be useful in finding units in cyclic extensions of the rationals of degree less than or equal to 6. The polynomials for these differences are simpler than the polynomials for the corresponding periods. The cyclic differences depend on the choice of a primitive root; the question is raised as to which choices of primitive root yield units.

1. INTRODUCTION

The project was to develop an analogue of the classical cyclotomy by replacing the Gaussian cyclotomic periods

$$\eta_i = \sum_{\nu=0}^{e-1} \zeta^{g^{e\nu+i}} \tag{1}$$

by their cyclic differences

$$\delta_i = \eta_i - \eta_{i+1} \qquad (i = 0, 1, \ldots, e-1), \tag{2}$$

which we called the delta cyclotomy.

Our interest in the delta cyclotomy was aroused by the fact that $\eta_i - \eta_{i+1} - 1$ were units in the cubic, quartic, and quintic fields, provided a suitable primitive root was chosen in the quintic case. It was later ascertained that these new units were simply ratios of the known translation units, but new units of this form were found in the sextic case and also for $p = 211$ in the quintic case.

2. THE CUBIC CASE

In this case, for primes p with $4p = L^2 + 27$, the roots of Shanks' simplest cubic [6]

$$P_3(y) = y^3 - \frac{L-3}{2}y^2 - \frac{L+3}{2}y - 1 = \prod_{i=0}^{2}(y - \theta_i) \tag{3}$$

can be ordered by

$$\theta_0, \quad \theta_1 = -1/(\theta_0 + 1), \quad \theta_2 = -1/(\theta_1 + 1) = -(\theta_0 + 1)/\theta_0. \tag{4}$$

Received by the editor October 20, 1992.
1991 *Mathematics Subject Classification.* Primary 11R18, 11R27, 11R16.
This is the title given by D. H. L. to his talk on this subject at the West Coast Number Theory Conference in Asilomar held in 1990.

0025-5718/93 $1.00 + $.25 per page

It was shown in [4] that these roots are related to the cubic Gaussian periods by

$$\theta_i = \eta_i + (L-1)/6. \tag{5}$$

Since η_0 is independent of the primitive root, being the sum over cubic residues, so is θ_0 by (5), and hence θ_1 and θ_2 by (4), and therefore also all the η's by (5). Obviously, $\sum_{i=0}^{2}\delta_i = 0$ by (2), and it is not hard to verify that $\sum\delta_i\delta_j = -p$ and that the product $\delta_0\delta_1\delta_2 = -p$, so that the cubic satisfied by the δ's is simply

$$\Delta_3(y) = y^3 - py + p = \prod_{i=0}^{2}(y-\delta_i). \tag{6}$$

Hence, $\Delta_3(1) = 1$, and $\delta_i - 1$ are units. The unit equation is

$$D_3(y) = y^3 + 3y^2 - (p-3)y + 1 = \prod_{i=0}^{2}(y-(\delta_i - 1)). \tag{7}$$

We note that Shanks' ordering of the roots avoids the usual dependence on the primitive root in the ordering of the η's. It might be of interest to characterize the two reciprocal classes of primitive roots which give positive or negative units. We found that $g = 2$ gives Shanks' arrangement for $p = 37$, 139, and 163, while $g = 10$ gives it for $p = 19$, 97, and 313.

It remains to establish the connection between the units θ_i and $\delta_i - 1$. Using (4), we find that

$$\delta_0 - 1 = \theta_0^2/(\theta_0+1), \quad \delta_1 - 1 = 1/(\theta_0(\theta_0+1)), \quad \delta_2 - 1 = -(\theta_0+1)^2/\theta_0, \tag{8}$$

so that the new units are not fundamental since (8) implies they generate a subgroup of index 3.

It might be worth noting that in the case of $4p = 1 + 27M^2$, the cubic units found by Lettl [5] are of the form

$$\theta_i = 3\delta_i + (9M-1)/2. \tag{9}$$

We have not discovered a counterpart of this result for $e > 3$.

3. The quartic case

It was shown in [4] that in this case there are translation units (i.e., integer translates of periods η_i) for primes $p = a^2 + 16$, with $a \equiv 1 \pmod 4$, namely

$$\theta_i = -\eta_i + (a-1)/4. \tag{10}$$

Here, η_0 and η_2 are independent of the primitive root, while η_1 and η_3 interchange if the primitive root is replaced by its reciprocal. Hence, there are again two classes of primitive roots. Interchanging these classes throws δ_i into $-\delta_{3-i}$ and therefore $\delta_i - 1$ into $-(\delta_{3-i}+1)$, so that, if $\prod_{i=0}^{3}(\delta_i - 1) = 1$, then $\prod_{i=0}^{3}(\delta_{3-i}+1) = 1$, and we get a unit in either case. Which primitive root gives which type of unit is an open question.

The unit equation given in [4] is

$$P_4(y) = y^4 - ay^3 - 6y^2 + ay + 1 = \prod_{i=0}^{3}(y-\theta_i), \tag{11}$$

while the delta equation is simply

$$\Delta_4(y) = y^4 - p(y-\varepsilon)^2 = \prod_{i=0}^{3}(y-\delta_i), \qquad \varepsilon = \pm 1, \tag{12}$$

so that $\Delta_4(\varepsilon) = 1$ and $\delta_i - \varepsilon$ are units. The delta unit equation is

$$D_4(y) = y^4 + 4\varepsilon y^3 - (p-6)y^2 + 4\varepsilon y + 1 = \prod_{i=0}^{3}(y-(\delta_i - \varepsilon)). \tag{13}$$

These units can again be shown to be ratios of the corresponding translation units.

For example, for $p = 137 = 11^2 + 16$, so that $a = -11$ and $\theta_i = \eta_i + 3$ by (10), we have for $g = 3$

$$\begin{aligned} \eta_0 &= -3.087414388, & \eta_1 &= -4.19157521, \\ \eta_2 &= 8.439764344, & \eta_3 &= -2.16077475, \\ \delta_0 - 1 &= .104160824, & \delta_1 - 1 &= -13.63133955, \\ \delta_2 - 1 &= 9.600539093, & \delta_3 - 1 &= -.073360369; \end{aligned}$$

for $g = 5$, however, η_1 and η_3 interchange and

$$\begin{aligned} \delta_0 + 1 &= .073360369, & \delta_1 + 1 &= -9.600539093, \\ \delta_2 + 1 &= 13.63133955, & \delta_3 + 1 &= -.10416082, \end{aligned}$$

so that

$$\prod_{i=0}^{3}(\eta_i + 3) = 1, \qquad \prod_{i=0}^{3}(\delta_i - 1) = 1 \quad \text{for } g = 3,$$

and

$$\prod_{i=0}^{3}(\delta_i + 1) = 1 \quad \text{for } g = 5.$$

4. The quintic case

This case presents some new problems. We now have four kinds of primitive roots, which come in reciprocal pairs. One of these pairs leads to positive or negative units, while the other pair does not give any units. The unsolved problem is how to characterize the primitive roots which lead to units.

Translation units were found in [4] for primes

$$p = n^4 + 5n^3 + 15n^2 + 25n + 25, \tag{14}$$

namely

$$\theta_i = \left(\frac{n}{5}\right)\eta_i + \left[\left(\frac{n}{5}\right) - n^2\right]\Big/ 5. \tag{15}$$

The unit quintic given there is

$$\begin{aligned} P_5(y) = {} & y^5 + n^2y^4 - 2(n^3 + 3n^2 + 5n + 5)y^3 + (p - 4n^2 - 10n - 20)y^2 \\ & + (n^3 + 4n^2 + 10n + 10)y + 1. \end{aligned} \tag{16}$$

We found that the delta quintic is much simpler, namely

$$\Delta_5(y) = y^5 - py^3 + p(n+2)\varepsilon y^2 - pny - p\varepsilon \qquad (\varepsilon = \pm 1), \tag{17}$$

so that $\Delta_5(\varepsilon) = \varepsilon$, and hence $\delta_i + \varepsilon$ are units.

Finally, there exists an ordering of the roots for which the delta unit equation is

$$D_5(y) = y^5 + 5y^4\varepsilon - (p-10)y^3 + [p(n-1)+10]y^2\varepsilon + [p(n+1)+5]y + \varepsilon. \tag{18}$$

These units are again ratios of translation units given in [4]. We found the following to be true for these primes:

	p	31	71	101	191	631	941	
good	g	3	7	8	21	3	3	(gives delta units)
bad	g	17	21	2	19	12	2	(no delta units)
	ε	-1	-1	1	-1	-1	1	

but we were not able to characterize them in any way.

We also discovered a delta unit for $p = 211$, although no translation units are known in this case. Our attempts at finding a class of primes to which 211 belongs were unsuccessful.

5. The sextic case

In this case no translation units are known to exist, but units which are linear combinations of the Gaussian periods are given in [4] for primes of the form $4p = L^2 + 27$.

We now find units in case $p = n^2 + 108$, so $4p = L^2 + 27M^2$ with L and M both even. Units in fields of this type were studied by Gras [1]. The reduced period polynomial is given in [3]. We give here the unreduced version to illustrate its complexity in contrast with the delta sextic which follows,

$$\begin{aligned}\Psi_6(y) = {} & y^6 + y^5 - 5(p-1)y^4/12 - 5(p(L+3)-1)y^3/54 \\ & + 5[p(p-(L^2+4L+6))+1]y^2/432 \\ & + \{p[p(2L+5)-(L^3+5L^2+10L+10)]+1\}y/1296 \\ & - \{p[p^2-3p(L^2+4L+5)+L^4+6L^3+15L^2+20L+15]-1\}/46656.\end{aligned} \tag{19}$$

The delta sextic can be easily obtained by first considering the two delta cubics for the even- and odd-numbered deltas. These are easily seen to be

$$y^3 \pm \sqrt{p}(y^2 - 3y + 2) = y^3 \pm \sqrt{p}(y-1)(y-2), \tag{20}$$

so that their product is simply

$$P_6(y) = y^6 - p(y-1)^2(y-2)^2, \tag{21}$$

and hence

$$\Delta_6(1) = 1,$$

so that $\delta_i - 1$ are units. The unit equation is

$$D_6(y) = y^6 + 6y^5 - (p-15)y^4 + (2p+20)y^3 - (p-15)y^2 + 6y + 1. \tag{22}$$

Since in this case there are no known translation units, it would be of interest to find out if the delta units are fundamental.

We have a few sporadic results for the case of $e = 7$, namely $p = 29$, $\delta_i + 1$ are units with $g = 2$, but not with $g = 3$; $p = 143$, $\delta_i - 2$ are units with $g = 3$, but not with $g = 5$.

In the octic case, units $\theta_i = \eta_i + \eta_{i+2} - (n^2 - 1)/4$ are given for $p = n^4 + 16$ in [4]. No new units were discovered. Lazarus [2] has proved the converses of some of the theorems in this paper.

Bibliography

1. M.-N. Gras, *Special units in real cyclic sextic fields*, Math. Comp. **48** (1987), 179–182.
2. A. J. Lazarus, *Cyclotomy and delta units*, Math. Comp. **61** (1993), 295–305.
3. D. H. Lehmer and Emma Lehmer, *The sextic period polynomial*, Pacific J. Math. **111** (1984), 341–355.
4. Emma Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541.
5. Günter Lettl, *A lower bound for the class number of certain cubic number fields*, Math. Comp. **46** (1986), 659–666.
6. Daniel Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

1180 Miller Avenue, Berkeley, California 94708-1755