Pacific Journal of Mathematics

MINIMAL POLYNOMIALS FOR GAUSS CIRCULANTS AND CYCLOTOMIC UNITS

STANLEY JOSEPH GURAK

Vol. 102, No. 2 February 1982

PACIFIC JOURNAL OF MATHEMATICS
Vol. 102, No. 2, 1982

MINIMAL POLYNOMIALS FOR GAUSS CIRCULANTS AND CYCLOTOMIC UNITS

S. GURAK

To determine the minimal polynomial of the Gauss periods of degree f corresponding to a given rational prime $l > 3$ is a classical problem dating back to Gauss. In this paper I show that at least the beginning coefficients of their minimal polynomial can be computed in an elementary fashion. The methods used here extend to give a similar result for computing the minimal polynomials of the cyclotomic units.

1. Introduction. Let l denote a prime greater than 3 and fix $\zeta = \cos(2\pi/l) + i\sin(2\pi/l)$, a primitive l-root of unity. If $l - 1 = ef$ with $f > 1$ let K be the unique subfield of $Q(\zeta)$ with $[Q(\zeta): K] = f$. Choose a generator s for the subgroup $(Z_l^x)^e$ of e-powers in the full group Z_l^x of reduced residue classes modulo l. Fix a set of integers $t_1, t_2, \cdots, t_e$ to represent the cosets $H_1, H_2, \cdots, H_e$ of $(Z_l^x)/(Z_l^x)^e$. The values

$$\mathrm{Tr}_{Q(\zeta)/K}(\zeta^{t_i}) \qquad (1 \leqq i \leqq e) \tag{1}$$

are the Gauss periods or circulants of degree f corresponding to l [4]. Their common minimal polynomial has the form

$$g(x) = x^e + a_1x^{e-1} + a_2x^{e-2} + \cdots + a_{e-1}x + a_e\ . \tag{2}$$

Determining the coefficients of $g(x)$ is a classical problem dating back to Gauss, and is intimately connected with the determination of the cyclotomic numbers of order e. Gauss himself determined the coefficients of $g(x)$ for fixed values $e \leqq 4$. For instance, when $e = 2$ he found that

$$g(x) = x^2 + x + (1 - (-1)^{(l-1)/2} \cdot l)/4 \qquad [5, \text{art. } 356]\ . \tag{3}$$

In case $e = 3$, the minimal polynomical

$$g(x) = x^3 + x^2 - (l-1)x/3 - ((l-1)/3 + kl)/9 \qquad [5, \text{art. } 358] \tag{4}$$

where the integer k is uniquely determined from the integral representation $4l = (3k-2)^2 + 27N^2$. In particular, for $l = 13$, since $52 = (\pm 5)^2 + 27$ one finds $3k - 2 = -5$ so $k = -1$ and $g(x) = x^3 + x^2 - 4x + 1$ in (4).

For certain larger values, specifically $e = 5, 6, 7, 8, 9, 10, 11, 12, 14, 16, 20, 24, 30,$ the cyclotomic numbers of order e have been determined through the efforts of Dickson, E. Lehmer, Whiteman, Muskat, and more recently, Leonard and Williams (see [6] for an account of these results). For these values of e, the coefficients of the minimal polynomial $g(x)$ for the corresponding Gauss periods are readily computed from the cyclotomic numbers.

In this paper I take another approach-determining the coefficients of $g(x)$ in (2) for a fixed value f. The case $f = 2$ was known to Gauss [5, art. 337]. Here each coefficient a_r is given by a polynomial of degree $[r/2]$ in l; namely,

$$(5)\qquad a_r = (-1)^{[r/2]}\binom{(l-1)/2 - [(r+1)/2]}{[r/2]} \qquad (0 \leqq r \leqq e)$$

where [ ] denotes the greatest integer function. When $f > 2$ it is natural to ask if each coefficient a_r in (2) can be computed in similar fashion by some polynomial in l. Of course, Eisenstein and Gauss' results [1, p. 220] for the next cases $f = 3$ and 4 already indicate this is not so; the determination of the later coefficients becomes increasingly more dependent on the higher reciprocity laws. However, there is still evidence here that the beginning coefficients may follow such a pattern, and indeed I have found this to be the case. If p is the smallest prime factor of f, I will prove that if l is sufficiently larger than r then $a_r = P_r(l)$ where for each r, P_r is a polynomial in l of degree $[r/p]$. The method of proof provides a recursion to compute the P_r.

In the next section I actually consider the more general question of determining the coefficients of the minimal polynomial for a sum of Gauss periods (1). This leads me to establish similar results for the cyclotomic units in §3.

2. The minimal polynomial for a sum of Gauss periods. Let C denote a finite set of k positive integers (repetitions allowed). I wish to determine the beginning coefficients for the minimal polynomial of the sum,

$$(6)\qquad \theta = \mathrm{Tr}_{Q(\zeta)/K}\Big(\sum_{c \in C} \zeta^c\Big)$$

of Gauss periods (1), which I shall *always* assume generates K over Q. Under these hypotheses the minimal polynomial of θ has the form (2) and equals $g(x) = \prod_{i=1}^{e}(x - \theta^{(i)})$, where for $1 \leqq i \leqq e$, the $\theta^{(i)} = \mathrm{Tr}\,(\sum_C \zeta^{ct_i}) = \sum_C (\zeta^{ct_i} + \zeta^{cst_i} + \cdots + \zeta^{cs^{f-1}t_i})$ denote the distinct conjugates of θ in K. It is well known from the theory of equations [3] that the coefficients a_r of $g(x)$ can be computed in terms of the symmetric power sums $S_n = \sum (\theta^{(i)})^n$. Specifically, this is expressed by Newton's identities

$$(7)\qquad S_r + a_1 S_{r-1} + a_2 S_{r-2} + \cdots + a_{r-1} S_1 + r a_r = 0 \qquad (1 \leqq r \leqq e)\,,$$

or equivalently in determinant form,

$$(8)\qquad a_r = \frac{(-1)^r}{r!}\begin{vmatrix} S_1 & 1 & 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ S_2 & S_1 & 2 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ S_3 & S_2 & S_1 & 3 & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ S_{r-1} & S_{r-2} & S_{r-3} & \cdot & \cdot & \cdot & \cdot & S_1 & r-1 \\ S_r & S_{r-1} & S_{r-2} & \cdot & \cdot & \cdot & \cdot & S_2 & S_1 \end{vmatrix} \qquad (1 \leqq r \leqq e)\,.$$

Already $a_1 = -S_1 = -\mathrm{Tr}_{Q(\zeta)/Q}(\sum_C \zeta^c) = k$ if no $c \equiv 0 \pmod{l}$. To compute the higher power sums I first note that the number $N(n)$ of ones (ζ^0) occurring in the multinomial expansion of any $(\theta^{(i)})^n = (\sum_C \zeta^{ct_i} + \zeta^{cst_i} + \cdots + \zeta^{cs^{f-1}t_i})^n$ is the number of tuples $(c_1, c_2, \cdots, c_n)$ in C^n satisfying a relation

$$(9)\qquad s^{\alpha_1}c_1 + s^{\alpha_2}c_2 + \cdots + s^{\alpha_n}c_n \equiv 0 \pmod{l}$$

for some choice of exponents $\alpha_i = 0, 1, 2, \cdots, f-1$ $(1 \leqq i \leqq n)$. Since the total number of terms in expanding $(\theta^{(i)})^n$ is $(fk)^n$, the number of nonones in the multinomial expansion of $(\theta^{(i)})^n$ is $(fk)^n - N(n)$. Taking into account the contribution of each term $(\theta^{(i)})^n$ in the power sum S_n, one finds a total of $(l-1)N(n)/f$ ones, and $(l-1)((fk)^n - N(n))/f$ nonones, exactly $((fk)^n - N(n))/f$ occurrences of each of the $(l-1)$ primitive l-roots of unity. Since $\sum_{i=1}^{l-1}\zeta^i = -1$, the value S_n must be $(l-1)N(n)/f - ((kf)^n - N(n))/f$, or equivalently

$$(10)\qquad S_n = lN(n)/f - k^n f^{n-1}\,.$$

I now establish the main result concerning the minimal polynomial of θ in (6). Let η be a fixed primitive f-root of unity and p be the smallest prime factor of f. For each $2 \leqq r \leqq e$ let $M(r)$ be the maximum of the sums

$$(11)\qquad (c_1 + c_2 + \cdots + c_r)^{\phi(f)}\,, \qquad c_i \text{ in } C\,,$$

where ϕ denotes, as customary, the Euler totient function. The beginning coefficients a_r can be computed as follows.

THEOREM 1. *For all primes $l \equiv 1 \pmod{f}$ and greater than $M(r)$ the coefficient a_r of the minimal polynomial of θ in* (6) *satisfies $a_r = P_r(l)$, where for each r, P_r is a polynomial of degree $[r/p]$ in l.*

Proof. I begin with two initial remarks. First, since $l \equiv 1 \pmod f$ each prime lying above l in $Q(\eta)$ has residue degree one. Thus the condition $l > M(r)$ ensures that for $n \leqq r$, no sum

$$s^{\alpha_1}c_1 + s^{\alpha_2} \cdot c_2 + \cdots + s^{\alpha_n}c_n \equiv 0 \pmod l \tag{12}$$

where $c_i \in C$ and $\alpha_i = 0, 1, 2, \cdots, f-1$ $(1 \leqq i \leqq n)$ unless

$$\eta^{\alpha_1}c_1 + \eta^{\alpha_2}c_2 + \cdots + \eta^{\alpha_n}c_n = 0\ , \tag{13}$$

since otherwise $l \leqq N_{Q(\eta)/Q}(\eta^{\alpha_1}c_1 + \cdots + \eta^{\alpha_n}c_n) \leqq M(r)$. Second, since each $c_i > 0$, if relation (12) holds the number n of terms in the sum is at least p.

Now it follows from the above remarks that $N(n) = 0$ for $1 \leqq n < p$, so $S_n = -k^n f^{n-1}$ $(1 \leqq n < p)$ in (10). If $p | n$ then $N(n) > 0$ since clearly the n-tuple $(c, c, \cdots, c)$, for any c in C, satisfies (13) by choosing n/p repetitions of $\eta^{f/p}c + \eta^{2f/p}c + \cdots + \eta^f c = 0$. Thus S_n is a polynomial expression of degree one in l whenever $p|n$.

I now proceed to prove the theorem by inducting on r. It easily follows from the preceding discussion that for $1 \leqq r < p$, the coefficients a_r are positive constants. Indeed, since $S_n = -k^n f^{n-1}$ $(1 \leqq n < p)$, one finds from (8) that

$$a_r = k^r((r-1)f+1)((r-2)f+1) \cdots (2f+1)(f+1)/r! \quad \text{for} \quad 1 < r < p\ . \tag{14}$$

Now assume that $r \geqq p$ and that each coefficient a_n, for $n < r$, satisfies $a_n = P_n(l)$, where for each n, P_n is a polynomial of degree $[n/p]$ whose leading term has sign $(-1)^{[n/p]}$. Next write $r = up + v$ for integers u and v with $0 \leqq v < p$. Then one has from (7) that

$$\begin{aligned} ra_r = & -a_{r-1}S_1 - \cdots - a_{r-v}S_v - \cdots \\ & - a_{r-p}S_p - \cdots - a_{r-p-v}S_{p+v} - \cdots - a_0 S_r\ . \end{aligned} \tag{15}$$

From the induction hypothesis and the above remarks concerning the symmetric power sums S_n $(1 \leqq n \leqq p)$, the first v terms of the sum in (15) and the pth term each have leading term of degree $[r/p]$ and sign $(-1)^{[r/p]}$. The remaining terms are either of lower degree or have a leading term of degree $[r/p]$ and sign $(-1)^{[r/p]}$ also. Thus it follows that $a_r = P_r(l)$ for some polynomial expression P_r of degree $[r/p]$ in l whose leading term has sign $(-1)^{[r/p]}$. This completes the induction and the proof of the theorem.

The special choice $C = \{1\}$ yields the following corollary concerning the minimal polynomial of the Gauss periods (1).

COROLLARY. *The coefficient a_r for the minimal polynomial of* *the Gauss periods given in* (1) *satisfies* $a_r = P_r(l)$ *if* $r < \sqrt[\phi(f)]{l}$, *where for each* r, P_r *is a polynomial of the degree* $[r/p]$. *In particular, for* $1 < r < p$, $P_r = 1/r!((r-1)f+1)((r-2)f+1)\cdots(2f+1)(f+1)$.

EXAMPLE 1. Upon calculating the numbers $N(1) = N(2) = 0$, $N(3) = 3$ and $N(4) = N(5) = 0$ in (10) for the choice $\{C\} = 1$ in the case $f = 3$ of the above corollary, one finds the following polynomial expressions for the coefficients a_r $(0 \leqq r \leqq 5)$ of the minimal polynomial of the period $\zeta + \zeta^s + \zeta^{s^2}$ from (7):

$$a_0 = 1\,, \quad a_1 = 1\,, \quad a_2 = 2\,, \quad a_3 = -2(l-7)/3\,, \quad a_4 = -(2l-35)/3\,,$$

and

$$a_5 = -(4l-91)/3\,.$$

The pattern of these coefficients is exhibited below for primes $l < 37$.

l	Minimal polynomial $g(x)$
7	$x^2 + x + 2$
13	$x^4 + x^3 + 2x^2 - 4x + 3$
19	$x^6 + x^5 + 2x^4 - 8x^3 - x^2 + 5x + 7$
31	$x^{10} + x^9 + 2x^8 - 16x^7 - 9x^6 - 11x^5 + 43x^4 + 6x^3 + 63x^2 + 20x + 25$

3. Minimal polynomials for the cyclotomic units.

I shall now apply the results of the last section to determine the beginning coefficients of the minimal polynomials for the cyclotomic units of the maximal real subfield K of $Q(\zeta)$. The cyclotomic units are customarily indexed $\theta_j = \sin(\pi j/l)/\sin(\pi/l)$ for $j = 2, 3, \cdots, (l-1)/2$ [2, p. 360]. However, it is convenient here to reindex them as

$$\theta_k = \sin(2\pi k/l)/\sin(\pi/l) \qquad \text{for} \quad 1 \leqq k \leqq (l-3)/2\,. \tag{16}$$

It is easy to show that $\theta_k = -2\sum_{i=1}^{k}\cos(\pi(l-(2i-1))/l)$ and hence is conjugate to $-(\zeta^{-(2k-1)} + \zeta^{-(2k-3)} + \cdots + \zeta^{-1} + \zeta^{1} + \cdots + \zeta^{2k-3} + \zeta^{2k-1})$. Thus $-\theta_k$ has the same minimal polynomial as the sum of Gauss periods of degree $f = 2$ having the form (6) with $C = \{1, 3, 5, \cdots, 2k-1\}$. Noting that $M(r) = (2k-1)r$ for $r \geqq 2$ from (11), it follows from Theorem 1 that if $l > (2k-1)r$ the coefficient b_r of the minimal polynomial

$$f(x) = x^{(l-1)/2} + b_1 x^{(l-3)/2} + \cdots + b_r x^{(l-2r-1)/2} + \cdots + b_{(l-1)/2} \tag{17}$$

for θ_k satisfies a polynomial of degree $[r/2]$ in l. I actually prove the stronger result:

THEOREM 2. *If* $l > (2k-1)r$ *then* $b_r = P_r(k, l)$ *in* (17), *where for each* r, P_r *is a polynomial in* k *and* l *of degree* $[r/2]$ *in* l *and* *of total degree* r. *For* $0 \leqq r \leqq 5$ *these polynomials* P_r *are given by*

$$P_0 = 1\,, \qquad P_1 = -k\,, \qquad P_2 = -k(l-3k)/2\,, \qquad P_3 = k^2(l-5k)/2\,,$$
$$P_4 = k^2(l-5k)(l-7k)/8 + (k^3-k)l/12\,,$$

and

$$P_5 = -k^3(l-7k)(l-9k)/8 - (k^4-k^2)l/12\,.$$

Before proving the Theorem I need the next combinatorial result.

LEMMA. *The number* $N(k, n)$ *of solutions of the equation* $c_1 + c_2 + \cdots + c_n = 0$ *with each integer* $-(2k-1) \leqq c_i \leqq 2k-1$ *and odd for* $1 \leqq i \leqq n$ *and* $k > 0$, *is given by*

$$(18) \qquad N(k, n) = \begin{cases} \sum_{i=0}^{n/2-1} (-1)^i \binom{n}{i}\binom{k(n-2i)+n/2-1}{n-1} & \text{if } n \text{ is even}\,, \\ 0 \quad \text{if } n \text{ is odd}\,. \end{cases}$$

Proof. If n is odd the result is immediate, so assume that n is even. The number $N(k, n)$ is seen to be the coefficient of the constant term in the expansion

$$(x^{-(2k-1)} + x^{-(2k-3)} + \cdots + x^{-1} + x + \cdots + x^{2k-3} + x^{2k-1})^n\,,$$

or that of the term $x^{(2k-1)n}$ in the expansion $(1 + x^2 + \cdots + x^{4k-2})^n$. Replacing x by $x^{1/2}$ everywhere in the latter expression one finds that $N(k, n)$ is the coefficient of $x^{(2k-1)n/2}$ in the expansion

$$(19) \qquad (1 + x + \cdots + x^{2k-1})^n = \left(\frac{1-x^{2k}}{1-x}\right)^n = (1-x^{2k})^n(1 + x + x^2 + \cdots)^n\,.$$

It is well-known that $(1 + x + x^2 + \cdots)^n = \sum \binom{m+n-1}{n-1} x^m$. Upon comparing coefficients in (19) it follows that $N(k, n) = \sum_{i=0}^{[n/2-n/4k]} (-1)^i \binom{n}{i}\binom{(2k-1)n/2-2ki+n-1}{n-1}$ which is the expression given in (18).

Proof of Theorem 2. For $r = 0$ and 1 it is clear that $P_0 = 1$ and $P_1 = -k$, so I shall assume $r \geqq 2$. From the lemma above and in view of the initial remarks in the proof of Theorem 1, one finds that each S_n in (10) for $l > (2r-1)k$ and $n \leqq r$ is a polynomial expression in k and l of total degree n. A simple extension of the induction argument used in the proof of Theorem 1 and based on the Newton identities (7) now yields the first statement of Theorem 2.

It remains to compute the polynomials P_r $(2 \leqq r \leqq 5)$ explicitly.

I actually compute the coefficients for the minimal $g(x)$ for $-\theta_k$ of the form (2) first using the lemma and (7). For $r = 2$, since $N(k, 2) = 2k$ one has $S_1 = -k$ and $S_2 = k - 2k^2$ in (10). Here $a_1 = k$ so $a_2 = 1/2(-a_1S_1 - S_2) = -k(l - 3k)/2$ from (7). For $r = 3$, one also has $S_3 = -4k^3$ so $a_3 = (-a_2S_1 - a_1S_2 - S_3)/3 = -k^2(l - 5k)/2$ again from (7). For $r = 4$, since $N(k, 4) = (16k^3 + 2k)/3$ one finds $S_4 = (8k^3 + k)/3 - 8k^4$. Thus $a_4 = 1/4(-a_3S_1 - a_2S_2 - a_1S_3 - S_4) = k^2(l - 5k)(l - 7k)/8 + (k^3 - k)l/12$. Finally, in the case $r = 5$ since $S_5 = -16k^5$ one finds $a_5 = k^3(l - 7k)(l - 9k)/8 + (k^4 - k^2)l/12$ using (7).

According for the sign changes in the coefficients of the minimal polynomial for θ_k and $-\theta_k$, one immediately obtains the desired expressions P_r for the coefficients b_r $(2 \leqq r \leqq 5)$.

EXAMPLE 2. The pattern of the coefficients b_r for the minimal polynomial (17) of the cyclotomic unit θ_2 in (16) is exhibited below for primes $l < 20$.

l	Minimal polynomial $f(x)$
7	$x^3 - 2x^2 - x + 1$
11	$x^5 - 2x^4 - 5x^3 + 2x^2 + 4x + 1$
13	$x^6 - 2x^5 - 7x^4 + 6x^3 + 5x^2 - 5x + 1$
17	$x^8 - 2x^7 - 11x^6 + 14x^5 + 19x^4 - 14x^3 - 11x^2 + 2x + 1$
19	$x^9 - 2x^8 - 13x^7 + 18x^6 + 32x^5 - 24x^4 - 26x^3 + 7x^2 + 7x + 1$

I wish to express my gratitude to Basil Gordon for his assistance in locating some of the material referenced in this paper, and to Dwight Bean for his patience and helpfulness in obtaining some valuable numerical evidence with the computer.

REFERENCES

1. P. Bachmann, *Die Lehre von der Kreistheilung*, Zahlentheorie III, Leipzig, 1872.
2. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
3. L. E. Dickson, *Elementary Theory of Equations*, Wiley, New York.
4. ———, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math., **57** (1935), 391-424.
5. C. F. Gauss, *Disquisitiones Arithmeticae*, Yale University Press, New Haven, 1966.
6. P. A. Leonard and K. S. Williams, *The cyclotomic numbers of order eleven*, Acta Arith., **26** (1975), 365-383.

Received February 17, 1981 and in revised form October 5, 1981.

UNIVERSITY OF SAN DIEGO
SAN DIEGO, CA 92110

PACIFIC JOURNAL OF MATHEMATICS

Mathematical parers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Please propose a heading for the odd unmbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

50 reprints to each author are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966, Regular subscription rate: $114.00 a year (6 Vol., 12 issues). Special rate: $57.00 a year to individual members of supporting institution.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address shoud be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION
Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.).
8-8, 3-chome, Takadanobaba, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics

Vol. 102, No. 2 February, 1982