Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Blair K. Spearman, Kenneth S. Williams

Normal integral bases for Emma Lehmer's parametric family of cyclic quintics

Tome 16, nº 1 (2004), p. 215-220.

<http://jtnb.cedram.org/item?id=JTNB_2004__16_1_215_0>

Journal de Théorie des Nombres de Bordeaux **16** (2004), 215–220

Normal integral bases for Emma Lehmer's parametric family of cyclic quintics

par Blair K. SPEARMAN et Kenneth S. WILLIAMS

Résumé. Nous donnons des bases normales entières explicites pour des extensions cycliques quintiques définies par la famille paramétrée de quintiques d'Emma Lehmer.

Abstract. Explicit normal integral bases are given for some cyclic quintic fields defined by Emma Lehmer's parametric family of quintics.

1. Introduction

Let $n \in \mathbb{Z}$. Emma Lehmer's quintic polynomials $f_n(x) \in \mathbb{Z}[x]$ are defined by

$$f_n(x) = x^5 + n^2x^4 - (2n^3 + 6n^2 + 10n + 10)x^3 + (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 + (n^3 + 4n^2 + 10n + 10)x + 1, \tag{1.1}$$

see [4, p. 539]. Schoof and Washington [6, p. 548] have shown that $f_n(x)$ is irreducible for all $n \in \mathbb{Z}$. Let $\rho_n \in \mathbb{C}$ be a root of $f_n(x)$. Set $L_n = \mathbb{Q}(\rho_n)$ so that $[L_n : \mathbb{Q}] = 5$. It is known that L_n is a cyclic field [6, p. 548]. The discriminant $d(L_n)$ of L_n has been determined by Jeannin [3, p. 76] and, as a special case of a more general result, by Spearman and Williams [7, Theorem 2], namely

$$d(L_n) = f(L_n)^4, \tag{1.2}$$

where the conductor $f(L_n)$ is given by

$$f(L_n) = 5^{\alpha} \prod_{\substack{p \equiv 1 \pmod 5 \\ p \mid n^4 + 5n^3 + 15n^2 + 25n + 25 \\ v_p(n^4 + 5n^3 + 15n^2 + 25n + 25) \not\equiv 0 \pmod 5}} p, \tag{1.3}$$

Manuscrit reçu le 18 octobre 2002.

Both authors were supported by research grants from the Natural Sciences and Engineering Research Council of Canada.

where $v_p(k)$ denotes the exponent of the largest power of the prime p dividing the nonzero integer k and

$$\alpha = \begin{cases} 0, & \text{if } 5 \nmid n, \\ 2, & \text{if } 5 \mid n. \end{cases} \tag{1.4}$$

Gaál and Pohst [2, p. 1690] have given an integral basis for L_n when $p^2 \nmid n^4 + 5n^3 + 15n^2 + 25n + 25$ for any prime $p \neq 5$. They also discuss the existence of a power integral basis for L_n [2, p. 1695]. It is known that

$$\begin{aligned} &L_n \text{ has a normal integral basis (NIB)} \\ &\quad \Longleftrightarrow L_n \subseteq \mathbb{Q}(e^{\frac{2\pi i}{m}}) \text{ for some squarefree integer } m \\ &\quad \Longleftrightarrow f(L_n) \mid m \text{ for some squarefree integer } m \\ &\quad \Longleftrightarrow f(L_n) \text{ squarefree} \\ &\quad \Longleftrightarrow 5 \nmid n, \end{aligned}$$

see [5, p. 175]. From this point on we assume that $5 \nmid n$ so that n possesses a normal integral basis. Acciaro and Fieker [1] have given an algorithm for finding a normal integral basis (when it exists) for a cyclic field of prime degree. Applying this algorithm to the 800 fields L_n with $1 \leq n \leq 1000$ and $(n, 5) = 1$ they found that 766 of these fields had a normal integral basis of the form

$$\left\{a + \rho_n, a + \rho_n', a + \rho_n'', a + \rho_n''', a + \rho_n''''\right\}$$

for some $a \in \mathbb{Z}$, where ρ_n, ρ_n', ρ_n'', ρ_n''', ρ_n'''' are the conjugates of ρ_n. We explain this phenomenon by proving the following theorem in Section 2.

Theorem. *Let $n \in \mathbb{Z}$ be such that $5 \nmid n$. Then L_n has a normal integral basis of the form*

$$\left\{v + w\rho_n, v + w\rho_n', v + w\rho_n'', v + w\rho_n''', v + w\rho_n''''\right\} \quad (v, w \in \mathbb{Z})$$

if and only if

$$n^4 + 5n^3 + 15n^2 + 25n + 25 \text{ is squarefree}, \quad w = \pm 1, \quad v = \frac{w}{5}\left(n^2 - \left(\frac{n}{5}\right)\right),$$

where $\left(\frac{n}{5}\right)$ is the Legendre symbol modulo 5.

It is easy to check that there are exactly 766 values of $n \in \mathbb{Z}$ such that $1 \leq n \leq 1000$, $5 \nmid n$ and $n^4 + 5n^3 + 15n^2 + 25n + 25$ is squarefree.

2. Proof of Theorem.

We begin by determining a cyclic permutation of the roots of $f_n(x)$. This was done by Schoof and Washington [6, p. 548] by means of a rational function. For our purposes we require polynomial expressions for the roots. The restriction $5 \nmid n$ is not needed in the Proposition below.

Proposition. *Let $n \in \mathbb{Z}$. Let y_0 be any root of $f_n(x)$. Then the other four roots of $f_n(x)$ are*

$$\begin{aligned} y_1 = ((n+2)^2 y_0^4 &+ (n+2)(n+1)(n^2+n-1)y_0^3 \\ &+ (-2n^5 - 14n^4 - 43n^3 - 76n^2 - 80n - 39)y_0^2 \\ &+ (n+1)(n^5 + 8n^4 + 29n^3 + 60n^2 + 71n + 36)y_0 \\ &+ (n+2)(n^3 + 6n^2 + 14n + 11))/(n^3 + 5n^2 + 10n + 7), \end{aligned}$$

$$\begin{aligned} y_2 = ((-2n-3)y_0^4 &- (2n^3 + 4n^2 + 3n + 2)y_0^3 \\ &+ (3n^4 + 14n^3 + 31n^2 + 41n + 24)y_0^2 \\ &- (n+3)(n^4 + 4n^3 + 9n^2 + 9n + 2)y_0 \\ &- (n+2)(2n+3))/(n^3 + 5n^2 + 10n + 7), \end{aligned}$$

$$\begin{aligned} y_3 = (-(n+2)(n+1)y_0^4 &- (n^2+n-1)(n+1)^2 y_0^3 \\ &+ (2n^5 + 12n^4 + 33n^3 + 54n^2 + 53n + 23)y_0^2 \\ &- (n+2)(n+1)(n^4 + 5n^3 + 12n^2 + 16n + 9)y_0 \\ &- (n^5 + 7n^4 + 24n^3 + 47n^2 + 52n + 25))/(n^3 + 5n^2 + 10n + 7), \end{aligned}$$

$$\begin{aligned} y_4 = ((n+1)y_0^4 &+ (n^3 + 2n^2 + 3n + 3)y_0^3 \\ &- (n+2)(n+1)(n^2 + n + 4)y_0^2 \\ &- (n^4 + 7n^3 + 19n^2 + 29n + 19)y_0 \\ &+ (n+1)(n^3 + 5n^2 + 11n + 9))/(n^3 + 5n^2 + 10n + 7). \end{aligned}$$

Let $\sigma \in Gal(f_n)$ be such that

$$\sigma(y_0) = y_1. \tag{2.1}$$

Then

$$\sigma^j(y_0) = y_j, \quad j = 0, 1, 2, 3, 4, \tag{2.2}$$

and the polynomial $P_n(y) \in \mathbb{Q}[y]$ given by

$$\begin{aligned} P_n(y) = ((n+2)^2 y^4 &+ (n+2)(n+1)(n^2+n-1)y^3 \\ &+ (-2n^5 - 14n^4 - 43n^3 - 76n^2 - 80n - 39)y^2 \\ &+ (n+1)(n^5 + 8n^4 + 29n^3 + 60n^2 + 71n + 36)y \\ &+ (n+2)(n^3 + 6n^2 + 14n + 11))/(n^3 + 5n^2 + 10n + 7), \end{aligned} \tag{2.3}$$

is such that

$$P_n^j(y_0) = \sigma^j(y_0), \quad j = 0, 1, 2, 3, 4. \tag{2.3}$$

Proof of Proposition. Using MAPLE we find that there exist polynomials $g_n(y)$, $h_n(y)$, $k_n(y)$, $l_n(y) \in \mathbb{Q}[y]$ such that

$$f_n(y_1) = f_n(y_0)g_n(y_0) = 0,$$

$$f_n(y_2) = f_n(y_0)h_n(y_0) = 0,$$

$$f_n(y_3) = f_n(y_0)k_n(y_0) = 0,$$

$$f_n(y_4) = f_n(y_0)l_n(y_0) = 0,$$

where y_1, y_2, y_3, y_4 are defined in the statement of the Proposition. Clearly y_0, y_1, y_2, y_3, y_4 are all distinct as y_0 is a root of an irreducible quintic polynomial. Thus y_0, y_1, y_2, y_3, y_4 are the five distinct roots of $f_n(x)$. With $P_n(y)$ as defined in (2.3), we see from the definition of y_1 that

$$y_1 = P_n(y_0). \tag{2.4}$$

Another MAPLE calculation shows that

$$P_n^2(y_0) = P_n(y_1) = y_2,$$

$$P_n^3(y_0) = P_n(y_2) = y_3,$$

$$P_n^4(y_0) = P_n(y_3) = y_4,$$

so that

$$P_n^j(y_0) = y_j, \quad j = 0, 1, 2, 3, 4.$$

With $\sigma \in \mathrm{Gal}(f_n)$ defined in (2.1), we see from (2.5) that

$$P_n(y_0) = \sigma(y_0).$$

Finally, as $\sigma \in \mathrm{Gal}(f_n)$ and $P_n(y) \in \mathbb{Q}[y]$, we obtain

$$P_n^2(y_0) = P_n(P_n(y_0)) = P_n(\sigma(y_0)) = \sigma(P_n(y_0)) = \sigma^2(y_0)$$

and similarly $P_n^3(y_0) = \sigma^3(y_0)$ and $P_n^4(y_0) = \sigma^4(y_0)$. $\square$

Proof of Theorem. Let $n \in \mathbb{Z}$ be such that $5 \nmid n$. Let $v, w \in \mathbb{Z}$. Using MAPLE we find that

$$\begin{aligned} & D(v + w\rho_n, v + w\rho_n', v + w\rho_n'', v + w\rho_n''', v + w\rho_n'''') \\ & \qquad = D(v + wy_0, v + wy_1, v + wy_2, v + wy_3, v + wy_4) \\ & \qquad = \left|\det\left(v + wy_{i+j \pmod 5}\right)_{i,j=0,1,2,3,4}\right|^2 \\ & \qquad = w^8(5v - wn^2)^2(n^4 + 5n^3 + 15n^2 + 25n + 25)^4. \end{aligned}$$

Then, by (1.2) and (1.3), we have

$$\left\{v + w\rho_n, v + w\rho_n', v + w\rho_n'', v + w\rho_n''', v + w\rho_n''''\right\} \text{ is a NIB for } L_n$$

$$\Longleftrightarrow D(v + w\rho_n, v + w\rho_n', v + w\rho_n'', v + w\rho_n''', v + w\rho_n'''') = d(L_n)$$

$$\Longleftrightarrow w^8(5v - wn^2)^2(n^4 + 5n^3 + 15n^2 + 25n + 25)^4 = \prod_{\substack{p \equiv 1 \pmod 5 \\ p \mid n^4 + 5n^3 + 15n^2 + 25n + 25 \\ v_p(n^4 + 5n^3 + 15n^2 + 25n + 25) \not\equiv 0 \pmod 5}} p^4$$

$$\Longleftrightarrow w^8 = (5v - wn^2)^2 = 1 \text{ and } n^4 + 5n^3 + 15n^2 + 25n + 25 \text{ squarefree}$$

$$\Longleftrightarrow w = \pm 1, \quad v = \frac{w}{5}\left(n^2 - \left(\frac{n}{5}\right)\right), \quad n^4 + 5n^3 + 15n^2 + 25n + 25 \text{ squarefree},$$

completing the proof of the Theorem. □

The authors would like to thank Raylene Senger who did some computing for them in connection with this work.

References

[1] V. Acciaro and C. Fieker, *Finding normal integral bases of cyclic number fields of prime degree.* J. Symbolic Comput. **30** (2000), 239–252.

[2] I. Gaál and M. Pohst, *Power integral bases in a parametric family of totally real cyclic quintics.* Math. Comp. **66** (1997), 1689–1696.

[3] S. Jeannin, *Nombre de classes et unités des corps de nombres cycliques quintiques d' E. Lehmer.* J. Théor. Nombres Bordeaux **8** (1996), 75–92.

[4] E. Lehmer, *Connection between Gaussian periods and cyclic units.* Math. Comp. **50** (1988), 535–541.

[5] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers.* Springer - Verlag, Berlin 1990.

[6] R. Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*. Math. Comp. **50** (1988), 543–556.
[7] B. K. Spearman and K. S. Williams, *The discriminant of a cyclic field of odd prime degree*. Rocky Mountain J. Math. To appear.

Blair K. Spearman
Department of Mathematics and Statistics
Okanagan University College
Kelowna, B.C. Canada V1V 1V7
E-mail : `bspearman@okanagan.bc.ca`

Kenneth S. Williams
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
E-mail : `williams@math.carleton.ca`