THE CONDUCTOR OF LECACHEUX'S PARAMETRIC FAMILY OF CYCLIC QUINTIC FIELDS

ALAN K. SILVESTER*1, BLAIR K. SPEARMAN**2 AND KENNETH S. WILLIAMS***3

*Department of Mathematics and Statistics,
Okanagan University of British Columbia, Kelowna, B.C. Canada V1V 1V7
e-mail: masedman@canada.com

**Department of Mathematics and Statistics,
Okanagan University of British Columbia, Kelowna, B.C. Canada V1V 1V7
e-mail: blair.spearman@ubc.ca

***School of Mathematics and Statistics,
Carleton University, Ottawa, Ontario, Canada K1S 5B6
e-mail: williams@math.carleton.ca

(Received 25 January 2006; after final revision 9 October 2006; accepted 12 October 2006)

A formula for the conductor of Lecacheux's parametric family of cyclic quintic fields is given.

Key Words: Cyclic Quintic Fields; Conductor

1. INTRODUCTION

Spearman and Williams [7] have given a theorem which enables one to determine the discriminant of a cyclic field of odd prime degree directly from the coefficients of a defining polynomial. They applied their theorem to a family of cyclic quintic polynomials due to Lehmer [5]. In this paper we apply the theorem of Spearman and Williams to a family of cyclic quintic polynomials due to Lecacheux [3], [4].

*The first author was supported at The University of British Columbia Okanagan by an undergraduate student research award from the Natural Sciences and Engineering Research Council of Canada.

**The second author was supported by a research grant from the Natural Sciences and Engineering Research Council of Canada.

***The third author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.
In this section we state the theorem of Spearman and Williams [7].

**Theorem 1** — Let $p$ be an odd prime. Let $f(X) = X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ be such that $\text{Gal}(f) \cong \mathbb{Z}/p\mathbb{Z}$ and such that there does not exist a prime $q$ with $q^{p-1} | a_i$ for $i = 0, 1, \ldots, p-2$. Let $\theta \in \mathbb{C}$ be a root of $f(X)$ and set $K = \mathbb{Q}(\theta)$ so that $K$ is a cyclic extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = p$. Then\[d(K) = f(K)^{p-1},\]

where the conductor $f(K)$ is given by\[f(K) = p^\alpha \prod_{q \equiv 1 \pmod{p}, q | a_i \text{ or } q | a_0 \text{ and } q^{p-1} | a_i (i = 0, 1, \ldots, p-2)} q,\]

where $q$ runs through primes and\[\alpha = \begin{cases} 0, & \text{if } p^{p(p-1) \not| \text{disc}(f)} \text{ and } p | a_i \text{ for } i = 1, \ldots, p-2 \text{ does not hold} \\ & \text{or } p^{p(p-1) \not| \text{disc}(f)} \text{ and } p^{p-1} \not| a_0, p^{p-1} \not| a_1, p^{p+1-1} \not| a_i \\ & (i = 2, \ldots, p-2) \text{ does not hold} \\ 2, & \text{if } p^{p(p-1) \not| \text{disc}(f)} \text{ and } p | a_i \text{ for } i = 1, \ldots, p-2 \text{ holds} \\ & \text{or } p^{p(p-1) \not| \text{disc}(f)} \text{ and } p^{p-1} \not| a_0, p^{p-1} \not| a_1, p^{p+1-1} \not| a_i \\ & (i = 2, \ldots, p-2) \text{ holds}. \end{cases}\]

**3. Odile Lecacheux’s Quintics**

Let $t \in \mathbb{Q}$ and set\[f_t(X) = X^5 + a_4(t)X^4 + a_3(t)X^3 + a_2(t)X^2 + a_1(t)X + a_0(t),\]

where\[a_4(t) = t^5 - 3,\]
\[a_3(t) = -t^9 - 2t^8 - 3t^7 - 5t^6 - 6t^5 - 2t^4 + t^3 - t^2 + 3,\]
\[a_2(t) = t^{10} + 2t^9 + 4t^8 + 6t^7 + 10t^6 + 9t^5 + 4t^4 - 2t^3 + 2t^2 - 1,\]
\[a_1(t) = -t^2(t^7 + 2t^6 + 3t^5 + 5t^4 + 5t^3 + 2t^2 - t + 1),\]
\[a_0(t) = t^5.\]

These polynomials were introduced by Odile Lecacheux [3] in 1990. We set\[t = u/v, \quad u \in \mathbb{Z}, \quad v \in \mathbb{Z}, \quad (u, v) = 1, \quad v > 0,\]
and define

\[ E_1 = E_1(u, v) = u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4, \]
\[ E_2 = E_2(u, v) = u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4, \]
\[ F = F(u, v) = 2u^2 + 3uv + 3v^2, \]
\[ G = G(u, v) = 4u^3 - u^2v - 2uv^2 + 2v^3, \]
\[ H = H(u, v) = u^3 + u^2v - 3uv^2 + 3v^3, \]
\[ J = J(u, v) = -3u^5 + 4v^5, \]
\[ L = L(u, v) = 4u^{13} + 9u^{12}v - 22u^{11}v^2 + 22u^{10}v^3 + 6u^9v^4 - 74u^7v^6 + 142u^6v^7 - 142u^5v^8 + 96u^3v^{10} - 84u^2v^{11} + 72uv^{12} - 72v^{13}, \]
\[ M = M(u, v) = 7u^3 + 22u^2v + 29uv^2 + 11v^3, \]
\[ N = N(u, v) = 7u^3 + 13u^2v + 24uv^2 - 14v^3, \]
\[ P = P(u, v) = 20u^{12} + 77u^{11}v - 14u^{10}v^2 + 75u^8v^4 + 105u^7v^5 - 282u^6v^6 + 159u^5v^7 - 475u^4v^8 + 5u^2v^{10} + 3uv^{11} + 49v^{12}, \]
\[ Q = Q(u, v) = 5u^3 - 2u^2v + 10uv^2 + 8v^3, \]
\[ R = R(u, v) = 12u^{12} + 47u^{11}v - 33u^{10}v^2 - 75u^8v^3 + 175u^7v^4 - 12u^6v^5 - 267u^5v^6 + 108u^4v^7 + 475u^4v^8 - 1075u^3v^9 + 528u^2v^{10} + 478uv^{11} - 527v^{12}, \]
\[ S = S(u, v) = 3u^3 + 14u^2v + 24uv^2 + 16v^3. \]

Let \( \theta \) be a root of \( f_t(X) \) and set \( K = Q(\theta) \). We prove

**Theorem 2** — Let \( t \) be a rational number such that \( f_t(X) \) is irreducible in \( \mathbb{Q}[X] \). Then \( K \) is a cyclic quintic field.

**Proof:** As \( f_t(X) \) is assumed to be irreducible in \( \mathbb{Q}[X] \), we have

\[ [K : \mathbb{Q}] = \deg(f_t(X)) = 5 \]

so that \( K \) is a quintic field. We next determine the Galois group of \( K \) over \( \mathbb{Q} \). We set

\[ g_t(X) = 5^5 f_t \left( \frac{X - (t^5 - 3)}{5} \right) \]

so that

\[ g_t(X) = X^5 + g_3X^3 + g_2X^2 + g_1X + g_0, \]

where

\[ g_3 = -5(2t^2 + 3t + 3)(t^4 + 3t^3 + 4t^2 + 2t + 1)(t^4 - 2t^3 + 4t^2 - 3t + 1), \]
\[ g_2 = 5(4t^3 - t^2 - 2t + 2) (t^4 - 2t^3 + 4t^2 - 3t + 1)(t^4 + 3t^3 + 4t^2 + 2t + 1)^2, \]
Using MAPLE we find that
\[ \text{disc}(g_t(X)) = 5^{20}t^{18}(t^4 - 2t^3 + 4t^2 - 3t + 1)^4(t^4 + 3t^3 + 4t^2 + 2t + 1)^8. \]

As \( f_0(X) \) is reducible we have \( t \neq 0 \) so that the discriminant of \( g_t(X) \) is a nonzero perfect square. Thus \( \text{Gal}(K) \) is a subgroup of the alternating group \( A_5 \), and so \( \text{Gal}(K) \simeq \mathbb{Z}_5, D_5 \) or \( A_5 \). Using the expression for the resolvent sextic of a quintic polynomial given by Dummit [2], we find using MAPLE that the resolvent sextic of \( g_t(X) \) has the rational root
\[ 5((t^4 - 2t^3 + 4t^2 - 3t + 1)(4t^8 + 4t^7 - 12t^6 + 12t^5 + 78t^3 - 47t^2 + 16t - 16)
\times (t^4 + 3t^3 + 4t^2 + 2t + 1)^2. \]

Thus \( \text{Gal}(K) \) is a solvable group and so \( \text{Gal}(K) \simeq \mathbb{Z}_5 \) or \( D_5 \). Suppose that \( \text{Gal}(K) \simeq D_5 \). Let \( \theta_1, \ldots, \theta_5 \in \mathbb{C} \) be the roots of \( g_t(X) \). Set
\[ g_t(X) = \prod_{i,j=1}^5 (x - (\theta_i - \theta_j)) \in \mathbb{Q}[X]. \]
Soicher [6] (see also [1]) has shown that \( g_t(X) \) can be determined by using resultants as
\[ g_t(X) = \frac{\text{resultant} (g_t(x + X), g_t(x))}{X^5}. \]

MAPLE gives
\[ g_t(X) = q_1(X)q_2(X)q_3(X)q_4(X), \]
where each \( q_i(X) \) is a quintic polynomial in \( \mathbb{Q}[X] \). Using MAPLE we find that
\[ \text{resultant}(q_i(X), q_j(X)) \neq 0 \text{ for } t \neq 0, \ 1 \leq i < j \leq 4, \]
and
\[ \text{resultant}(q_i(X), q_t'(X)) \neq 0 \text{ for } t \neq 0, \ i = 1, 2, 3, 4, \]
so that \( g_t(X) \) is a squarefree polynomial in \( \mathbb{Q}[X] \). Then, by [1, Theorem 3.1.ii]), \( g_t(X) \) factors as a product of two irreducible polynomials of degree 10 in \( \mathbb{Q}[X] \). Thus \( \text{Gal}(K) \neq D_5 \). Therefore \( \text{Gal}(K) \simeq \mathbb{Z}_5 \). \( \square \)
4. THE CONDUCTOR OF $K$.

We apply Spearman and Williams' theorem to prove the following result.

**Theorem 3** — Let $t$ be a rational number such that $f_t(X)$ is irreducible in $Q[X]$. Let $\theta$ be a root of $f_t(X)$. Set $K = Q(\theta)$ so, by Theorem 2, $K$ is a cyclic quintic field. Then the conductor $f(K)$ is given by

$$f(K) = 5^a \prod_{q \equiv 1 \pmod{5}, q \notin \{1, 2\} \pmod{5}, q \text{ is prime}} q,$$

where $q$ runs through primes.

$$\alpha = \begin{cases} 0, & \text{if } 2u - v \not\equiv 0 \pmod{5}, \\ 2, & \text{if } 2u - v \equiv 0 \pmod{5}, \end{cases}$$

and

$$q^{\alpha}(E_1 E_2) \mid E_1 E_2.$$

**Proof:** As in the proof of Theorem 2, we set

$$g_t(X) = 5^6 f_t \left( \frac{X - (t^5 - 3)}{5} \right) = X^5 + g_3 X^3 + g_2 X^2 + g_1 X + g_0,$$

where $g_2, g_1, g_0$ are given in the proof of Theorem 2. Next we set

$$h_{u,v}(X) = v^{25} g_{u,v}(X/v^5) = X^5 + h_3 X^3 + h_2 X^2 + h_1 X + h_0,$$

where

$$h_3 = -5(u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4) \times (u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)(2u^2 + 3uv + 3v^2),$$

$$h_2 = 5(u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4)(u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)^2 \times (4u^3 - u^2v - 2uv^2 + 2v^3),$$

$$h_1 = 5(u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4)(u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)^2 \times (u^3 + u^2v - 3uv^2 + 3v^3)(-3u^2 + 4v^5),$$

$$h_0 = (u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4)(u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)^2 \times (4u^{13} + 9u^{12}v - 22u^{11}v^2 + 22u^{10}v^3 + 6u^9v^4 - 74u^8v^5 + 142u^6v^7$$

$$- 142u^5v^8 + 96u^3v^{10} - 84u^2v^{11} + 72uv^{12} - 72v^{13}),$$

so that, from the definitions given in Section 3, we have

$$h_3 = -5E_1 E_2 F, \quad h_2 = 5E_1 E_2^2 G, \quad h_1 = 5E_1 E_2^2 H J, \quad h_0 = E_1 E_2^2 L.$$  

(4.1)
Let $m$ denote the largest positive integer such that

$$m^2 \mid h_3, \ m^3 \mid h_2, \ m^4 \mid h_1, \ m^5 \mid h_0,$$

and set

$$k_{u,v}(X) = h_{u,v}(mX)/m^5 = X^5 + k_3 X^3 + k_2 X^2 + k_1 X + k_0,$$

where

$$k_3 = h_3/m^2, \ k_2 = h_2/m^3, \ k_1 = h_1/m^4, \ k_0 = h_0/m^5.$$

Appealing to MAPLE, we find

$$\text{disc} (k_{u,v}(X)) = m^{20} E_1^4 E_2^8 u^{11} v^{34} / m^{20},$$

$$E_1 M - E_2 N = 5^2 v^7,$$

$$E_1 P - L Q = 5^4 v^{16},$$

and

$$E_2 R - L S = 5^4 v^{16}.$$

Clearly $k_{u,v}(X)$ is a defining polynomial for the cyclic quintic field $K$. Hence, by Theorem 1, we have

$$f(K) = 5^a \prod_{q \equiv 1 \pmod{5}} q,$$

where $q$ runs through primes and

$$\alpha = \begin{cases} 
0, & \text{if } 5^{20} \nmid \text{disc}(k_{u,v}) \text{ and } 5 \mid k_1, 5 \mid k_2, 5 \mid k_3 \text{ does not hold} \\
5^{20} \mid \text{disc}(k_{u,v}) \text{ and } 5^4 \nmid k_0, 5^4 \mid k_1, 5^4 \mid k_2, 5^3 \mid k_3 \\
2, & \text{if } 5^{20} \nmid \text{disc}(k_{u,v}) \text{ and } 5 \mid k_1, 5 \mid k_2, 5 \mid k_3 \\
5^{20} \mid \text{disc}(k_{u,v}) \text{ and } 5^4 \mid k_0, 5^4 \mid k_1, 5^4 \mid k_2, 5^3 \mid k_3 \end{cases}$$

Let $q$ be a prime with

$$q \equiv 1 \pmod{5}, \ q \mid k_3, \ q \mid k_2, \ q \mid k_1, \ q \mid k_0.$$

We show that

$$q \mid E_1 E_2, \ \nu_q(E_1 E_2) \neq 0 \pmod{5}.$$

As $q \equiv 1 \pmod{5}$ we have $q \neq 2, 3, 5$. Suppose $q \mid u$. As $q \mid h_0$, we see by (4.1) that $q \mid E_1$ or $q \mid E_2$ or $q \mid L$. If $q \mid E_1$ or $q \mid E_2$ then from the definitions of $E_1$ and $E_2$ we see that $q \mid v$, contradicting $(u,v) = 1$. If $q \mid L$ then as $q \neq 2, 3$ we see from the definition of $L$ that $q \mid v$, contradicting $(u,v) = 1$. Hence $q \nmid u$. Suppose $q \mid v$. As $q \mid h_0$, we see by (4.1) that $q \mid E_1$
or \( q \mid E_2 \) or \( q \mid L \). If \( q \mid E_1 \) or \( q \mid E_2 \) then from the definitions of \( E_1 \) and \( E_2 \) we have \( q \mid u \), contradicting \((u, v) = 1\). If \( q \mid L \) then as \( q \neq 2 \) we have from the definition of \( L \) that \( q \mid u \), contradicting \((u, v) = 1\). Thus \( q \nmid uv \). As \( q \mid f(K) \) we have \( q \mid \text{disc} (k_{u,v}) \). It follows by (4.5) that \( q \mid E_1 \) or \( q \mid E_2 \) as \( q \mid u, v, 5 \). By (4.6) we see that \( q \mid E_1 \) or \( q \mid E_2 \) but not both. Assume that \( q \mid E_1 \). If \( v_q(E_1 E_2) \equiv 0 \pmod{5} \) then \( v_q(E_1) = 5w \) for some \( w \in \mathbb{N} \). By (4.7) we have \( q \nmid L \). Thus by (4.1) we have

\[
q^{5w} \mid h_3, \quad q^{5w} \mid h_2, \quad q^{5w} \mid h_1, \quad q^{5w} \mid h_0,
\]

and by (4.2) we deduce that

\[
q^w \parallel m.
\]

Thus

\[
q \nmid \frac{h_0}{m^5} = k_0,
\]

contradicting \( q \mid k_0 \). Hence \( v_q(E_1) \neq 0 \pmod{5} \). Now assume \( q \mid E_2 \). If \( v_q(E_2) \equiv 0 \pmod{5} \) then \( v_q(E_2) = 5w \) for some \( w \in \mathbb{N} \). By (4.8) we see that \( q \nmid L \). As \( q^{5w} \parallel E_2 \) we have \( q^{10w} \parallel E_2^2 \). Thus by (4.1) we see that

\[
q^{5w} \mid h_3, \quad q^{10w} \mid h_2, \quad q^{10w} \mid h_1, \quad q^{10w} \mid h_0,
\]

and by (4.2) we have

\[
q^{2w} \parallel m.
\]

Thus

\[
q \nmid \frac{h_0}{m^5} = k_0,
\]

contradicting \( q \mid k_0 \). Hence \( v_q(E_2) \neq 0 \pmod{5} \). Thus \( v_q(E_1 E_2) \neq 0 \pmod{5} \).

Now conversely let \( q \) be a prime with

\[
q \equiv 1 \pmod{5}, \quad q \mid E_1 E_2, \quad v_q(E_1 E_2) \neq 0 \pmod{5}
\]

We show that

\[
q \equiv 1 \pmod{5}, \quad q \mid k_3, \quad q \mid k_2, \quad q \mid k_1, \quad q \mid k_0.
\]

By (4.6) we see that either \( q \mid E_1 \) or \( q \mid E_2 \) but not both. As \( v_q(E_1 E_2) \neq 0 \pmod{5} \) we have \( q^{5z+r} \parallel E_1 E_2 \) for some nonnegative integer \( z \) and \( r \in \{1, 2, 3, 4\} \). Assume \( q \mid E_1 \). Then by (4.7) we see that \( q \nmid L \). We have by (4.1)

\[
q^{5z+r} \mid h_3, \quad q^{5z+r} \mid h_2, \quad q^{5z+r} \mid h_1, \quad q^{5z+r} \parallel h_0,
\]

and by (4.2) we have

\[
q^r \parallel m
\]

so

\[
q^{3z+r} \mid k_3, \quad q^{2z+r} \mid k_2, \quad q^{z+r} \mid k_1, \quad q^r \mid k_0.
\]

Thus

\[
q \mid k_3, \quad q \mid k_2, \quad q \mid k_1, \quad q \mid k_0.
\]
Now assume \( q \mid E_2 \). Then by (4.8) we have \( q \mid h \). As \( v_q(E_2) = 5z + r \) we see that \( q^{10z+2r} \parallel E_2^2 \).

Thus by (4.1) we have

\[
q^{5z+r} \mid h_3, \quad q^{10z+2r} \mid h_2, \quad q^{10z+2r} \mid h_1, \quad q^{10z+2r} \mid h_0.
\]

From the definition of \( m \) it follows that \( q^{2z} \parallel m \) if \( r = 1, 2 \) and \( q^{2z+1} \parallel m \) if \( r = 3, 4 \). In the second case we note that \((5x + r) - (4z + 2) = z + (r - 2) > 0 \) so \( q \mid k_3 \). Thus

\[
q \mid k_3, \quad q \mid k_2, \quad q \mid k_1, \quad q \mid k_0.
\]

We have proved

\[
q = \prod_{q \equiv 1 \pmod{5}, \quad v_q(E_1, E_2) \equiv 0 \pmod{5}} q = \prod_{q \equiv 1 \pmod{5}, \quad v_q(E_1, E_2) \equiv 0 \pmod{5}} q.
\]

It remains to show that

\[
\alpha = \begin{cases} 
0, & \text{if } 2u - v \not\equiv 0 \pmod{5}, \\
2, & \text{if } 2u - v \equiv 0 \pmod{5}.
\end{cases}
\]

The following simple divisibility result will be useful.

**Lemma** —

(a) \( 5 \mid E_1, E_2, F, G, H, J, L, \) if \( 2u - v \not\equiv 0 \pmod{5} \).

(b) \( 5 \parallel E_1, E_2, F, G, H \) and \( 5^2 \mid J, L, \) if \( 2u - v \equiv 0 \pmod{5} \).

**Proof:** (a) Suppose \( 2u - v \not\equiv 0 \pmod{5} \). Then \( u + 2v \not\equiv 0 \pmod{5} \) and

\[
E_1 \equiv (u + 2v)^5 \not\equiv 0 \pmod{5},
\]

\[
E_2 \equiv (u + 2v)^5 \not\equiv 0 \pmod{5},
\]

\[
F \equiv 2(u + 2v)^2 \not\equiv 0 \pmod{5},
\]

\[
G \equiv 4(u + 2v)^3 \not\equiv 0 \pmod{5},
\]

\[
H \equiv (u + 2v)^3 \not\equiv 0 \pmod{5},
\]

\[
J \equiv 2(u + 2v)^5 \not\equiv 0 \pmod{5},
\]

\[
L \equiv 4(u + 2v)^3 \not\equiv 0 \pmod{5}.
\]

(b) Suppose \( 2u - v \equiv 0 \pmod{5} \). Then \( v = 2u + 5w \) for some \( w \in \mathbb{Z} \). Thus

\[
E_1 \equiv 5u^4 \pmod{25},
\]

\[
E_2 \equiv 5u^4 \pmod{25},
\]

\[
F \equiv 20u^2 \pmod{25},
\]

\[
G \equiv 10u^3 \pmod{25},
\]

\[
H \equiv 15u^3 \pmod{25},
\]

\[
J \equiv 0 \pmod{25},
\]

\[
L \equiv 0 \pmod{25}.
\]
As \((u, v) = 1\) we have \(5 \nmid u\). Thus \(5 \mid E_1, 5 \mid E_2, 5 \mid F, 5 \mid G, 5 \mid H, 5^2 \mid J\) and \(5^2 \mid L\). □

We now show that \(2u - v \not\equiv 0 \pmod 5\) implies \(\alpha = 0\). By the Lemma we have

\[
5 \mid E_1, E_2, F, G, H, J, L, \quad (4.12)
\]

and by (4.1)

\[
5 \mid h_3, 5 \mid h_2, 5 \mid h_1, 5 \mid h_0.
\]

Thus by (4.2) we have

\[
5 \nmid m \quad (4.13)
\]

and by (4.4) we have

\[
5 \mid k_3, 5 \mid k_2, 5 \mid k_1, 5 \mid k_0. \quad (4.14)
\]

Now by (4.5), (4.13) and (4.14) we have \(5^{20} \mid \text{disc} (k_{u,v})\). By (4.13) the conditions \(5^4 \mid k_0, 5^4 \mid k_1, 5^4 \mid k_2, 5^4 \mid k_3\) do not hold. Thus by (4.10) we have \(\alpha = 0\).

Finally we show that \(2u - v \equiv 0 \pmod 5\) implies \(\alpha = 2\). In this case \(5 \nmid u, 5 \nmid v\). By the Lemma we have

\[
5 \mid E_1, E_2, F, G, H\text{ and }5^2 \mid J, L, \quad (4.15)
\]

and by (4.1)

\[
5^4 \mid h_3, 5^5 \mid h_2, 5^7 \mid h_1, 5^5 \mid h_0.
\]

As \(5^5 \mid h_0\) and \(5^5 \mid h_2\), we see from (4.2) that

\[
5 \mid m \quad (4.16)
\]

and thus from (4.4) we have

\[
5^2 \mid k_3, 5^2 \mid k_2, 5^3 \mid k_1. \quad (4.17)
\]

Now, by (4.5), (4.15) and (4.16), we have \(5^{12} \mid \text{disc} (k_{u,v})\) so that \(5^{20} \nmid \text{disc} (k_{u,v})\). By (4.17) the conditions \(5 \mid k_1, 5 \mid k_2, 5 \mid k_3\) hold. So by (4.10) we have \(\alpha = 2\). Thus

\[
\alpha = \begin{cases} 0, & \text{if } 2u - v \not\equiv 0 \pmod 5, \\ 2, & \text{if } 2u - v \equiv 0 \pmod 5. \end{cases} \quad (4.18)
\]

Theorem 3 now follows from (4.9), (4.10), (4.11) and (4.18). □

REFERENCES


