Publ. Math. Debrecen
48 / 1-2 (1996), 13–43

The conductor of a cyclic quartic field

By BLAIR K. SPEARMAN (Kelowna) and KENNETH S. WILLIAMS (Ottawa)

Abstract. Explicit formulae are obtained for the conductor and the discriminant of a cyclic quartic field $K = Q(\theta)$, where θ is a root of an irreducible polynomial $q(X) = X^4 + AX^2 + BX + C \in Z[X]$, and the integers A, B, C are such that there are no primes p with $p^2 \mid A$, $p^3 \mid B$, $p^4 \mid C$.

Let Z denote the domain of rational integers, let Q denote the field of rational numbers, and let K be a cyclic quartic extension field of Q, that is, $[K:Q] = 4$ and $Gal(K/Q) \simeq Z/4Z$. As K is a normal extension of Q and $Gal(K/Q)$ is an abelian group, K is an abelian field, and so by the Kronecker-Weber Theorem there exists a positive integer f such that $K \subseteq Q(\exp(2\pi i/f))$. The least such positive integer f is called the conductor of K and is denoted by $f(K)$. In this paper we take K in the form $K = Q(\theta)$, where θ is a root of an irreducible polynomial $q(X) = X^4 + AX^2 + BX + C \in Z[X]$, and determine $f(K)$ explicitly in terms of the coefficients A, B, C of $q(X)$. As $q(X)$ is irreducible over Z, we cannot have $A^2 - 4C = B = 0$. From [3] and [4] it is easy to deduce a necessary and sufficient condition for the splitting field K of the irreducible polynomial $q(X)$ to be cyclic.

For a prime p and a non-zero integer m, we denote by $v_p(m)$ the largest exponent k such that $p^k \mid m$, and write $p^{v_p(m)} \parallel m$. If for any prime p we have

$$v_p(A) \geq 2, \quad v_p(B) \geq 3, \quad v_p(C) \geq 4,$$

Mathematics Subject Classification: Primary 11R16, 11R29.

Key words and phrases: Cyclic quartic field, conductor, discriminant.

Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

then θ/p is an algebraic integer, which is a root of the irreducible polynomial

$$X^4 + (A/p^2)X^2 + (B/p^3)X + (C/p^4) \in Z[X],$$

and $K = Q(\theta/p)$. Therefore we can make the following simplifying assumption:

(1) there does not exist a prime p such that $p^2 \mid A,\ p^3 \mid B,\ p^4 \mid C$.

Our main result is the following theorem.

Theorem 1. *Let $K = Q(\theta)$ be a cyclic quartic extension of Q, where θ is a root of the irreducible polynomial $q(X) = X^4 + AX^2 + BX + C \in Z[X]$ with coefficients A, B, C satisfying* (1).

Case (i): $A^2 - 4C \neq 0,\ B \neq 0$: Set

$$\ell = v_2(A^2 - 4C), \quad b = v_2(B),$$

and for a prime $p \neq 2$ set

$$e_p = \min(v_p(A^2 - 4C),\ v_p(B)).$$

Then

$$f(K) = 2^{\alpha} \prod_{\substack{p \neq 2 \\ e_p \text{ odd}}} p \prod_{\substack{p \neq 2 \\ e_p(\text{even}) \geq 2, p \mid A}} p,$$

where the values of α are given in TABLE (i).

Case (ii): $A^2 - 4C = 0,\ B \neq 0$: Here

$$f(K) = 2^{\beta} \prod_{\substack{p \neq 2 \\ v_p(B) \text{ odd}}} p \prod_{\substack{p \neq 2 \\ v_p(B)(\text{even}) \geq 2, p \mid A}} p,$$

where the values of β are given in TABLE (ii).

Case (iii): $A^2 - 4C \neq 0,\ B = 0$: Here

$$f(K) = 2^{\gamma} \prod_{\substack{p \neq 2 \\ p \mid A, p \mid C}} p,$$

where the values of γ are given in TABLE (iii).

Proof of Theorem 1. We just treat case (i) ($A^2 - 4C \neq 0,\ B \neq 0$) as cases (ii) and (iii) can be treated in a similar but easier manner.

We begin by outlining the ideas involved in the proof. First we solve the quartic equation $q(\theta) = \theta^4 + A\theta^2 + B\theta + C = 0$ for θ in terms of

A, B, C and the unique integral root t of the cubic resolvent of $q(X)$, see (2) and (3). We then use this solution to express $K = Q(\theta)$ in the form $K = Q(\sqrt{m + n\sqrt{S}})$, where m, n, S are integers such that (m, n) and S are both squarefree and $m + n\sqrt{S}$ is not a square in $Q(\sqrt{S})$, see (11) and (12). Various relationships involving A, B, C, t, S, m, n are recorded in (4)–(10) for later use. For K expressed in the form $Q(\sqrt{m + n\sqrt{S}})$, Huard, Spearman and Williams have given an explicit expression for $d(K)$ in terms of m, n and S [2, Corollary 4]. Using the discriminant- conductor formula, it is easy to deduce from their result an explicit expression for the conductor $f(K)$ of K in terms of m, n and S, see (13)–(15). From this formula for $f(K)$ in terms of m, n and S, it is easy to see what arithmetic relations between m, n, S and A, B, C must be proved in order to deduce the form of $f(K)$ given in Theorem 1, see (16) and (17). The remainder of the proof of Theorem 1 requires a lot of technical but straightforward arithmetic results, see (18)–(56).

TABLE (i)/1: Values of α

α	congruence conditions
0	$A \equiv 1(4)$, $B \equiv 0(4)$, $C \equiv 1(2)$
	$A \equiv 1(4)$, $B \equiv 2(4)$, $C \equiv 0(2)$
	$A \equiv 3(4)$, $B \equiv 0(4)$, $C \equiv 0(2)$
	$A \equiv 3(4)$, $B \equiv 2(4)$, $C \equiv 1(2)$
	$A \equiv 0(2)$, $B \equiv 1(2)$, $C \equiv 1(2)$
	$A \equiv 2(8)$, $B \equiv 0(16)$, $C \equiv 5(8)$
	$A \equiv 10(16)$, $B \equiv 8(16)$, $C \equiv 5(8)$
	$A \equiv 6(8)$, $B \equiv 0(64)$, $C \equiv 1(8)$, $b \geq \ell(\text{even}) \geq 6$, $(A^2 - 4C)/2^\ell \equiv 1(4)$
	$A \equiv 6(16)$, $B \equiv 32(64)$, $C \equiv 1(8)$, $(A^2 - 4C)/2^\ell \equiv 1(4)$
	$A \equiv 6(16)$, $B \equiv 0(128)$, $C \equiv 1(8)$, $\ell(\text{even}) = b + 1 \geq 8$, $(A^2 - 4C)/2^\ell \equiv 3(4)$
	$A \equiv 6(16)$, $B \equiv 0(128)$, $C \equiv 1(8)$, $\ell(\text{odd}) = b + 2 \geq 9$, $(A^2 - 4C)/2^\ell \equiv 3(4)$
	$A \equiv 14(16)$, $B \equiv 32(64)$, $C \equiv 1(8)$, $(A^2 - 4C)/2^\ell \equiv 3(4)$
	$A \equiv 14(16)$, $B \equiv 0(128)$, $C \equiv 1(8)$, $\ell(\text{odd}) = b + 2 \geq 9$, $(A^2 - 4C)/2^\ell \equiv 1(4)$
2	$A \equiv 1(4)$, $B \equiv 0(4)$, $C \equiv 0(2)$
	$A \equiv 1(4)$, $B \equiv 2(4)$, $C \equiv 1(2)$
	$A \equiv 3(4)$, $B \equiv 0(4)$, $C \equiv 1(2)$
	$A \equiv 3(4)$, $B \equiv 2(4)$, $C \equiv 0(2)$
	$A \equiv 0(8)$, $B \equiv 0(8)$, $C \equiv 4(8)$
	$A \equiv 2(8)$, $B \equiv 0(16)$, $C \equiv 1(8)$, $\ell \geq 6$
	$A \equiv 2(16)$, $B \equiv 8(16)$, $C \equiv 5(8)$
	$A \equiv 4(8)$, $B \equiv 8(16)$, $C \equiv 4(8)$
	$A \equiv 6(8)$, $B \equiv 0(16)$, $C \equiv 5(8)$
	$A \equiv 6(8)$, $B \equiv 0(64)$, $C \equiv 1(8)$, $b \geq \ell(\text{even}) \geq 6, (A^2 - 4C)/2^\ell \equiv 3(4)$
	$A \equiv 6(16)$, $B \equiv 32(64)$, $C \equiv 1(8)$, $(A^2 - 4C)/2^\ell \equiv 3(4)$
	$A \equiv 6(16)$, $B \equiv 0(128)$, $C \equiv 1(8)$, $\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 1(4)$
	$A \equiv 6(16)$, $B \equiv 0(128)$, $C \equiv 1(8)$, $\ell(\text{even}) = b + 1 \geq 8, (A^2 - 4C)/2^\ell \equiv 1(4)$
	$A \equiv 14(16)$, $B \equiv 32(64)$, $C \equiv 1(8)$, $(A^2 - 4C)/2^\ell \equiv 1(4)$
	$A \equiv 14(16)$, $B \equiv 0(128)$, $C \equiv 1(8)$, $\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 3(4)$
3	$A \equiv 0(4)$, $B \equiv 0(4)$, $C \equiv 1(2)$
	$A \equiv 2(4)$, $B \equiv 0(8)$, $C \equiv 0(4)$
	$A \equiv 2(8)$, $B \equiv 0(16)$, $C \equiv 1(8), \ell = 5$
	$A \equiv 6(8)$, $B \equiv 16(32)$, $C \equiv 1(8)$
	$A \equiv 6(8)$, $B \equiv 0(64)$, $C \equiv 1(8), \ell(\text{even}) = b + 2 \geq 8$
	$A \equiv 6(16)$, $B \equiv 0(64)$, $C \equiv 1(8), \ell(\text{odd}) = b + 1 \geq 7$
	$A \equiv 14(16)$, $B \equiv 0(128)$, $C \equiv 1(8), b \geq \ell(\text{odd}) \geq 7$
	$A \equiv 4(8)$, $B \equiv 0(16)$, $C \equiv 4(8), b = \ell - 1 \geq 5$ or $b \geq \ell$

TABLE (i)/2: Values of α		
α	examples	
0	$X^4-55X^2-60X+145$	$f(K)=3\cdot 5$
	$X^4-51X^2-34X+68$	$f(K)=17$
	$X^4-65X^2-260X-260$	$f(K)=5\cdot 13$
	$X^4-17X^2-34X-17$	$f(K)=17$
	$X^4-26X^2-39X+13$	$f(K)=3\cdot 13$
	$X^4-182X^2-624X-299$	$f(K)=3\cdot 13$
	$X^4-102X^2-136X+221$	$f(K)=17$
	$X^4-170X^2-1088X-1751$	$f(K)=17$
	$X^4-170X^2-544X+2329$	$f(K)=17$
	$X^4-490X^2-1920X+9145$	$f(K)=3\cdot 5$
	$X^4-714X^2-2176X+33881$	$f(K)=17$
	$X^4-130X^2-480X+145$	$f(K)=3\cdot 5$
	$X^4-2210X^2-8320X+946465$	$f(K)=5\cdot 13$
2	$X^4-119X^2-68X+5848$	$f(K)=2^2\cdot 17$
	$X^4-15X^2-10X+5$	$f(K)=2^2\cdot 5$
	$X^4-45X^2-20X+305$	$f(K)=2^2\cdot 5$
	$X^4-85X^2-102X+34$	$f(K)=2^2\cdot 3\cdot 17$
	$X^4-272X+884$	$f(K)=2^2\cdot 17$
	$X^4-102X^2-544X+6953$	$f(K)=2^2\cdot 17$
	$X^4-30X^2-40X+5$	$f(K)=2^2\cdot 5$
	$X^4-20X^2-40X-20$	$f(K)=2^2\cdot 5$
	$X^4-50X^2-80X+205$	$f(K)=2^2\cdot 5$
	$X^4+102X^2-1088X+2873$	$f(K)=2^2\cdot 17$
	$X^4-90X^2-160X+905$	$f(K)=2^2\cdot 5$
	$X^4-330X^2-640X+18905$	$f(K)=2^2\cdot 5$
	$X^4-170X^2-640X+505$	$f(K)=2^2\cdot 5$
	$X^4-50X^2-160X-95$	$f(K)=2^2\cdot 5$
	$X^4+1054X^2-2176X+297313$	$f(K)=2^2\cdot 17$
3	$X^4-20X^2-20X-5$	$f(K)=2^3\cdot 5$
	$X^4-50X^2-40X+220$	$f(K)=2^3\cdot 5$
	$X^4-70X^2-240X-95$	$f(K)=2^3\cdot 3\cdot 5$
	$X^4-50X^2-80X+145$	$f(K)=2^3\cdot 5$
	$X^4-490X^2-960X+43705$	$f(K)=2^3\cdot 3\cdot 5$
	$X^4-90X^2-320X-55$	$f(K)=2^3\cdot 5$
	$X^4-1170X^2-16640X-59215$	$f(K)=2^3\cdot 5\cdot 13$
	$\left\{\begin{matrix} X^4-60X^2-160X+20 \\ X^4-180X^2-320X+4820 \end{matrix}\right\}$	$f(K)=2^3\cdot 5$

TABLE (i)/3: Values of α	
α	congruence conditions
4	$A \equiv 0(8)$, $B \equiv 0(8)$, $C \equiv 0(8)$ $A \equiv 0(8)$, $B \equiv 0(8)$, $C \equiv 2(4)$ $A \equiv 4(8)$, $B \equiv 0(16)$, $C \equiv 2(8)$ $A \equiv 4(8)$, $B \equiv 0(16)$, $C \equiv 4(8), b = \ell - 1 = 4$ or $b \leq \ell - 2$

TABLE (i)/4: Values of α		
α	examples	
4	$X^4 - 24X^2 - 32X + 8$	$f(K) = 2^4$
	$X^4 - 8X^2 - 8X - 2$	$f(K) = 2^4$
	$X^4 - 20X^2 - 16X + 34$	$f(K) = 2^4$
	$\left\{ \begin{matrix} X^4-12X^2-16X-4 \\ X^4-20X^2-32X+4 \end{matrix} \right\}$	$f(K) = 2^4$

TABLE (ii): Values of β			
β	conditions	examples	
0	$v_2(B) = 0$	$X^4 + 10X^2 + 25X + 25$	$f(K) = 5$
2	$v_2(B) \equiv 1(2)$	$X^4 + 442X^2 - 9248X + 48841$	$f(K) = 2^2 \cdot 17$
3	$v_2(B) = 4$	$X^4 + 190X^2 + 400X + 9025$	$f(K) = 2^3 \cdot 5$
4	$v_2(B) = 6$	$X^4 + 28X^2 + 64X + 196$	$f(K) = 2^4$

TABLE (iii): Values of γ			
γ	congruence conditions	examples	
0	$A \equiv 1\ (4)$, $C \equiv 1\ (2)$	$X^4 - 15X^2 + 45$	$f(K) = 3 \cdot 5$
	$A \equiv 3\ (4)$, $C \equiv 0\ (4)$	$X^4 - 17X^2 + 68$	$f(K) = 17$
	$A \equiv 2\ (8)$, $C \equiv 5\ (8)$	$X^4 - 78X^2 + 1053$	$f(K) = 3 \cdot 13$
	$A \equiv 6\ (8)$, $C \equiv 1\ (8)$	$X^4 - 34X^2 + 17$	$f(K) = 17$
2	$A \equiv 1\ (4)$, $C \equiv 0\ (4)$	$X^4 - 51X^2 + 612$	$f(K) = 2^2 \cdot 3 \cdot 17$
	$A \equiv 3\ (4)$, $C \equiv 1\ (2)$	$X^4 - 5X^2 + 5$	$f(K) = 2^2 \cdot 5$
	$A \equiv 2\ (8)$, $C \equiv 1\ (8)$	$X^4 + 34X^2 + 17$	$f(K) = 2^2 \cdot 17$
	$A \equiv 6\ (8)$, $C \equiv 5\ (8)$	$X^4 - 10X^2 + 5$	$f(K) = 2^2 \cdot 5$
3	$A \equiv 2\ (4)$, $C \equiv 0\ (4)$	$X^4 - 10X^2 + 20$	$f(K) = 2^3 \cdot 5$
	$A \equiv 4\ (8)$, $C \equiv 4\ (16)$	$X^4 - 68X^2 + 68$	$f(K) = 2^3 \cdot 17$
4	$A \equiv 4\ (8)$, $C \equiv 2\ (8)$	$X^4 - 4X^2 + 2$	$f(K) = 2^4$
	$A \equiv 8\ (16)$, $C \equiv 8\ (32)$	$X^4 - 8X^2 + 8$	$f(K) = 2^4$

By [3: Theorem 1 (iv)] the cubic resolvent $c(X) = X^3 - AX^2 - 4CX + (4AC - B^2)$ of $q(X)$ has exactly one root $t \in Z$. Thus we have

$$(2) \qquad (t - A)(t^2 - 4C) = B^2.$$

Clearly we see that $t - A \neq 0$, $t^2 - 4C \neq 0$, as $B \neq 0$. Solving the quartic equation $\theta^4 + A\theta^2 + B\theta + C = 0$ we find

$$(3) \qquad \theta = \frac{\varepsilon(t - A) + \delta\sqrt{(A^2 - t^2) - 2B\varepsilon\sqrt{t - A}}}{2\sqrt{t - A}},$$

where $\varepsilon = \pm 1$, $\delta = \pm 1$. If $t - A \in Z^2$ then we have $[K : Q] = [Q(\theta) : Q] = 1$ or 2, contradicting $[K : Q] = 4$. Hence $t - A \notin Z^2$ and we can write

$$(4) \qquad t - A = R^2 S,$$

where $S (\neq 1)$ is squarefree. From (2) and (4) we see that $RS \mid B$ so that

$$(5) \qquad B = B_1 RS,$$

$$(6) \qquad t^2 - 4C = B_1^2 S.$$

From (4) and (6) we obtain

$$(7) \qquad A^2 - 4C = S(B_1^2 - R^2(t + A)).$$

The unique quadratic subfield of K is

$$(8) \qquad k = Q\left(\sqrt{t - A}\right) = Q\left(\sqrt{S}\right).$$

As k is real, we have $S \geq 2$. The splitting field of the cubic resolvent

$$c(X) = (X - t)(X^2 + (t - A)X + (t^2 - At - 4C))$$

is

$$Q\left(\sqrt{(t - A)^2 - 4(t^2 - At - 4C)}\right) = Q\left(\sqrt{-3t^2 + 2At + (A^2 + 16C)}\right).$$

Since K is cyclic, by [3: Theorem 1 (iv)], we must have

$$Q\left(\sqrt{-3t^2 + 2At + (A^2 + 16C)}\right) = k = Q\left(\sqrt{S}\right),$$

so there exists an integer z such that

$$(9) \qquad -3t^2 + 2At + (A^2 + 16C) = Sz^2.$$

Equivalent forms of (9) are

$$(9)' \qquad (t + A)^2 - 4(t^2 - 4C) = Sz^2,$$

$$(9)'' \qquad (t - A)^2 - 4t(t - A) + 16C = Sz^2.$$

Further, from (3), we see that

$$\begin{aligned} K = Q(\theta) &= Q\left(\sqrt{(A^2-t^2) - 2B\varepsilon\sqrt{t-A}}\right) \\ &= Q\left(\sqrt{(A^2-t^2) + 2B\sqrt{t-A}}\right) \\ &= Q\left(\sqrt{-R^2S(t+A) + 2B_1R^2S\sqrt{S}}\right), \quad \text{by (4), (5),} \\ &= Q\left(\sqrt{-(t+A) + 2B_1\sqrt{S}}\right). \end{aligned}$$

Now let M^2 denote the largest square dividing both $t+A$ and $2B_1$. Set

(10) $$t + A = -M^2 m, \ 2B_1 = M^2 n,$$

so that

(11) $$(m, n) \text{ is squarefree,}$$

and

(12) $$K = Q\left(\sqrt{m + n\sqrt{S}}\right).$$

Appealing to [2, Corollary 4], as well as the conductor-discriminant formula, we obtain

$$f(K) = 2^{\lambda} \frac{(m,n)S}{(m,n,S)},$$

where the values of λ are given in TABLE (iv).

Thus

(13) $$f(K) = f_E(K) f_O(K),$$

where the 2-part $f_E(K)$ of $f(K)$ is

(14) $$f_E(K) = \begin{cases} 2^{\lambda}, & \text{if } 2 \nmid (m,n), \ 2 \nmid S, \\ 2^{\lambda+1}, & \text{otherwise,} \end{cases}$$

and the odd part $f_O(K)$ of $f(K)$ is

(15) $$f_O(K) = \prod_{\substack{p \neq 2 \\ (p \mid S) \text{ or } (p \nmid S, p \mid (m,n))}} p,$$

where p runs through primes.

TABLE (iv): Values of λ	
λ	congruence conditions
-1	$m \equiv 2 \pmod 8,\ n \equiv 2 \pmod 4,\ S \equiv 1 \pmod 8$ $m \equiv 6 \pmod 8,\ n \equiv 2 \pmod 4,\ S \equiv 5 \pmod 8$
0	$m \equiv 1 \pmod 4,\ n \equiv 0 \pmod 4,\ S \equiv 1 \pmod 8$ $m \equiv 3 \pmod 4,\ n \equiv 2 \pmod 4,\ S \equiv 5 \pmod 8$
1	$m \equiv 6 \pmod 8,\ n \equiv 2 \pmod 4,\ S \equiv 1 \pmod 8$ $m \equiv 2 \pmod 8,\ n \equiv 2 \pmod 4,\ S \equiv 5 \pmod 8$
2	$m \equiv 2 \pmod 4,\ n \equiv 0 \pmod 4,\ S \equiv 1 \pmod 4$ $m \equiv 3 \pmod 4,\ n \equiv 0 \pmod 4,\ S \equiv 1 \pmod 8$ $m \equiv 1 \pmod 4,\ n \equiv 2 \pmod 4,\ S \equiv 5 \pmod 8$
3	$m \equiv 1 \pmod 2,\ n \equiv 1 \pmod 2,\ S \equiv 1 \pmod 4$ $m \equiv 4 \pmod 8,\ n \equiv 2 \pmod 4,\ S \equiv 2 \pmod 8$ $m \equiv 2 \pmod 4,\ n \equiv 1 \pmod 2,\ S \equiv 2 \pmod 8$

Thus, to complete the proof, we must show that

(16) $$\alpha = \begin{cases} \lambda, & \text{if } 2 \nmid (m,n),\ 2 \nmid S, \\ \lambda + 1, & \text{otherwise,} \end{cases}$$

where the values of α are given in TABLE (i), and that for odd primes p we have

(17) $$(p \mid S) \text{ or } (p \mid m, p \mid n, p \nmid S) \iff (e_p \equiv 1 \pmod 2) \text{ or } (e_p \equiv 0 \pmod 2,\ e_p \geq 2,\ p \mid A),$$

where $e_p = \min(v_p(A^2 - 4C),\ v_p(B))$. We prove (17) first and then (16).

Proof of (17). Although we use b for $v_2(B)$ and ℓ for $v_2(A^2 - 4C)$, just for the proof of (17), we set for an odd prime p

(18) $$b = v_p(B),\ \ell = v_p(A^2 - 4C)$$

and

(19) $$b_1 = v_p(B_1),\ u = v_p(t + A).$$

We need a number of preliminary results ((20) to (45) below). By (5) we have

(20) $$0 \leq b_1 \leq b$$

and

$$(21) \qquad v_p(R) = \begin{cases} b - b_1, & \text{if } p \nmid S, \\ b - b_1 - 1, & \text{if } p \mid S. \end{cases}$$

Further, from (4), we see that

$$(22) \qquad v_p(t - A) = \begin{cases} 2(b - b_1), & \text{if } p \nmid S, \\ 2(b - b_1) - 1, & \text{if } p \mid S, \end{cases}$$

and, from (6), that

$$(23) \qquad v_p(t^2 - 4C) = \begin{cases} 2b_1, & \text{if } p \nmid S, \\ 2b_1 + 1, & \text{if } p \mid S. \end{cases}$$

Considering the power of p in both sides of (7), we see that exactly one of the following three possibilities must occur

$$(24) \qquad \begin{cases} \ell = 2x < 2(b - x) + u, & \text{if } p \nmid S, \\ \ell - 1 = 2x < 2(b - x - 1) + u, & \text{if } p \mid S, \end{cases}$$

$$(25) \qquad \begin{cases} 2x > 2(b - b_1) + u = \ell, & \text{if } p \nmid S, \\ 2x > 2(b - b_1 - 1) + u = \ell - 1, & \text{if } p \mid S, \end{cases}$$

$$(26) \qquad \begin{cases} 2x = 2(b - b_1) + u \le \ell, & \text{if } p \nmid S, \\ 2x = 2(b - b_1 - 1) + u \le \ell - 1, & \text{if } p \mid S. \end{cases}$$

From (24), (25) and (26), we see immediately that

$$(27) \qquad (p \nmid S,\ \ell \equiv 1 \pmod 2) \text{ or } (p \mid S,\ \ell \equiv 0 \pmod 2) \implies (24) \text{ cannot occur}$$

$$(28) \qquad (p \nmid S,\ \ell \not\equiv u \pmod 2) \text{ or } (p \mid S,\ \ell \equiv u \pmod 2) \implies (25) \text{ cannot occur,}$$

$$(29) \qquad u \equiv 1 \pmod 2 \implies (26) \text{ cannot occur.}$$

Next, from (10), (11) and (19), we see that

$$(30) \qquad u \equiv 1 \pmod 2,\ b_1 \ge u \implies p \mid (m, n),$$

$$(31) \qquad x \equiv 1 \pmod 2,\ b_1 \le u \implies p \mid (m, n),$$

(32) $$u \equiv 0 \pmod 2,\ b_1 \geq u \implies p \nmid m,$$

(33) $$x \equiv 0 \pmod 2,\ b_1 \leq u \implies p \nmid n.$$

From (5) and (10) we have

(34) $$p \nmid B \implies p \nmid S,\ p \nmid n.$$

From (7) and (10) we have

(35) $$\ell = 0 \implies p \nmid S,\ p \nmid (m,n).$$

From (5) and (7) we have

(36) $$b \geq 1,\ \ell \geq 1,\ p \nmid S \implies b_1 \geq 1.$$

From (10) and (20) we have

(37) $$u = 0 \implies p \nmid m.$$

Next we show that

(38) $$p \nmid S,\ b \geq 1,\ \ell \geq 1,\ u = 0 \implies p \nmid A.$$

Suppose $p \mid A$. Then, by (18), we have $p \mid B,\ p \mid A^2 - 4C, p \mid C$. As $p \nmid S$, by (5), p divides one of B_1 and R. By (7) p must divide both of B_1 and R. Hence, by (4), we have $p \mid t - A$ and thus, by (9)$''$, $p \mid z$. By (6) we have $p \mid t^2 - 4C$ and so, by (9)$'$, $p \mid t + A$, contradicting $u = 0$. This completes the proof of (38).

Our next result asserts that

(39) $$p \nmid A,\ u \geq 1 \implies b_1 = b.$$

As $p \nmid A$ and $u \geq 1$ we have $p \nmid t - A$, so that, by (4), we have $p \nmid RS$, and thus, by (5), $b_1 = b$. This completes the proof of (39).

We now prove that

(40) $$p \nmid S,\ p \nmid A,\ \ell \geq 2 \implies u \neq 1.$$

Suppose $u = 1$, that is, $p \parallel t + A$. By (7) we see that $p \mid B_1$ and $p \mid R$. Then, by (4), we have $p \mid t - A$ and so $p \mid A$, contradicting $p \nmid A$. This completes the proof of (40).

We next show that

(41) $$p \nmid S,\ b_1 \geq 2,\ u \geq 2 \implies b_1 = b.$$

Suppose $b_1 \neq b$. By (20) and (21) we have $p \mid R$. Then, by (4), we have $p^2 \mid t - A$, so that as $p^2 \mid t + A$ we have $p^2 \mid t$ and $p^2 \mid A$. Further, as

TABLE (v)
(p (prime) $\neq 2$, $b = v_p(B)$, $\ell = v_p(A^2 - 4C)$)

case	conditions	conclusion
1	$b = 0$	$p \nmid S$, $p \nmid (m,n)$
2	$\ell = 0$	$p \nmid S$, $p \nmid (m,n)$
3	b (even) ≥ 2, ℓ (even) ≥ 2, $b \geq \ell$, $p \mid A$	$p \nmid S$, $p \mid (m,n)$
4	b (even) ≥ 2, ℓ (even) ≥ 2, $b < \ell$, $p \mid A$	$p \mid S$
5	b (even) ≥ 2, ℓ (even) ≥ 2, $b \geq \ell$, $p \nmid A$	$p \nmid S$, $p \nmid (m,n)$
6	b (even) ≥ 2, ℓ (even) ≥ 2, $b < \ell$, $p \nmid A$	$p \nmid S$, $p \nmid (m,n)$
7	b (odd) ≥ 1, ℓ (even) ≥ 2, $b \geq \ell$, $p \mid A$	$p \nmid S, p \mid (m,n)$
8	b (odd) ≥ 1, ℓ (even) ≥ 2, $b < \ell$, $p \mid A$	$p \mid S$
9	b (odd) ≥ 1, ℓ (even) ≥ 2, $b \geq \ell$, $p \nmid A$	$p \nmid S$, $p \nmid (m,n)$
10	b (odd) ≥ 1, ℓ (even) ≥ 2, $b < \ell$, $p \nmid A$	$p \nmid S$, $p \mid (m,n)$
11	b (even) ≥ 2, ℓ (odd) ≥ 1, $b \geq \ell$, $p \mid A$	$p \mid S$, if $v_p(C)$ odd $p \nmid S$, $p \mid (m,n)$, if $v_p(C)$ even
12	b (even) ≥ 2, ℓ (odd) ≥ 1, $b < \ell$, $p \mid A$	$p \mid S$
13	b (even) ≥ 2, ℓ (odd) ≥ 1, $b \geq \ell$, $p \nmid A$	$p \nmid S$, $p \mid (m,n)$
14	b (even) ≥ 2, ℓ (odd) ≥ 1, $b < \ell$, $p \nmid A$	$p \nmid S$, $p \nmid (m,n)$
15	b (odd) ≥ 1, ℓ (odd) ≥ 1, $b \geq \ell$, $p \mid A$	$p \mid S$, if $v_p(C)$ odd $p \nmid S$, $p \mid (m,n)$, if $v_p(C)$ even
16	b (odd) ≥ 1, ℓ (odd) ≥ 1, $b < \ell$, $p \mid A$	$p \mid S$
17	b (odd) ≥ 1, ℓ (odd) ≥ 1, $b \geq \ell$, $p \nmid A$	$p \nmid S$, $p \mid (m,n)$
18	b (odd) ≥ 1, ℓ (odd) ≥ 1, $b < \ell$, $p \nmid A$	$p \nmid S$, $p \mid (m,n)$

$p^2 \mid B_1$, $p \mid R$, from (5), we see that $p^3 \mid B$. Then, from (6), as $p^4 \mid t^2$ and $p^4 \mid B_1^2$, we see that $p^4 \mid C$. This contradicts (1) and so we must have $b_1 = b$ as claimed.

Next we prove that

$$(42) \qquad p \nmid A \implies p \nmid S.$$

Suppose $p \nmid A$ yet $p \mid S$. Then, by (4), we have $p \mid t - A$, and, by (6), we deduce $p \mid t^2 - 4C$. Then, appealing to (9)$'$, we see that $p \mid t + A$. Hence we have $p \mid A$, which is a contradiction, proving (42).

We now show that

$$(43) \qquad p \nmid S,\ u = 1 \implies \ell \leq b.$$

We know that exactly one of the possibilities (24), (25), (26) must occur. If (24) holds with $u = 1$ then $\ell = 2b_1 < 2(b-b_1)+1$, so $\ell = 2b_1 \leq 2(b-b_1)$, that is, $\ell = 2b_1 \leq b$. If (25) holds with $u = 1$ then $\ell = 1 + 2(b - b_1) < 2b_1$, so $\ell = 1+2(b-b_1) \leq 2b_1 - 1$, and thus $\ell = 1+2b-2b_1 \leq b$. The possibility (26) cannot occur with $u = 1$ by (29). This completes the proof of (43).

TABLE (v) (p (prime) $\neq 2$, $b = v_p(B)$, $\ell = v_p(A^2 - 4C)$)		
case	examples	
1	$X^4 - 20X^2 - 40X - 20$	$p = 3,\ b = 0,\ S = 5,\ m = 5,\ n = -2$
2	$X^4 - 20X^2 - 40X - 20$	$p = 7,\ \ell = 0,\ S = 5,\ m = 5,\ n = -2$
3	$X^4 - 120X^2 - 200X + 1550$	$p = 5,\ b = 2,\ \ell = 2, S = 2,\ m = 10,\ n = -5$
4	$X^4 - 210X^2 - 800X + 1025$	$p = 5,\ b = 2,\ \ell = 4,\ S = 5,\ m = 25,\ n = -10$
5	$X^4 - 100X^2 - 360X - 20$	$p = 3,\ b = 2,\ \ell = 2,\ S = 5,\ m = 5,\ n = -2$
6	$X^4 - 7592X^2 - 314600X - 3286634$	$p = 5,\ b = 2,\ \ell = 4,\ S = 26,\ m = 26,\ n = 5$
7	$X^4 - 336X^2 - 216X + 24318$	$p = 3,\ b = 3,\ \ell = 2,\ S = 2,\ m = 6,\ n = 3$
8	$X^4 - 260X^2 - 500X + 11275$	$p = 5,\ b = 3,\ \ell = 4,\ S = 5,\ m = 5,\ n = -1$
9	$X^4 - 200X^2 - 1080X - 890$	$p = 3,\ b = 3,\ \ell = 2,\ S = 10,\ m = 10,\ n = 3$
10	$X^4 - 104X^2 - 40X + 2254$	$p = 5,\ b = 1,\ \ell = 2,\ S = 2,\ m = 50,\ n = 5$
11	$X^4 - 260X^2 - 100X + 14395$ $X^4 - 1968X^2 - 2658X + 182286$	$p = 5,\ b = 2,\ \ell = 1,\ S = 5,\ m = 1,\ n = 2$ $p = 3,\ b = 4,\ \ell = 3,\ S = 82,\ m = 246,\ n = -27$
12	$X^4 - 60X^2 - 200X - 100$	$p = 5,\ b = 2,\ \ell = 3,\ S = 5,\ m = -25,\ n = -10$
13	$X^4 - 2368X^2 - 22200X + 657046$	$p = 5,\ b = 2,\ \ell = 1,\ S = 74,\ m = 1110,\ n = 75$
14	$X^4 - 504X^2 - 200X + 60254$	$p = 5,\ b = 2,\ \ell = 3,\ S = 2,\ m = 10,\ n = 1$
15	$X^4 - 442X^2 - 1664X + 24713$ $X^4 - 1560X^2 - 13000X + 254150$	$p = 13,\ b = 1,\ \ell = 1,\ S = 13,\ m = 13,\ n = 2$ $p = 5,\ b = 3,\ \ell = 3,\ S = 26,\ m = 13,\ n = 25$
16	$X^4 - 5080X^2 - 36000X + 40266$	$p = 5,\ b = 3,\ \ell = 5,\ S = 10,\ m = 250,\ n = 45$
17	$X^4 - 1036X^2 - 8880X + 70300$	$p = 3,\ b = 1,\ \ell = 1,\ S = 74,\ m = 444,\ n = 30$
18	$X^4 - 204X^2 - 80X + 9404$	$p = 5,\ b = 1,\ \ell = 3,\ S = 2,\ m = 100,\ n = -10$

Next we prove

$$(44) \qquad p \nmid S, u = 0 \implies \begin{cases} \ell < b, & \text{if (24) or (25) holds,} \\ \ell \geq b, & \text{if (26) holds.} \end{cases}$$

If (24) holds with $u = 0$ then $2b_1 < 2(b - b_1)$, $2b_1 < b$, $\ell < b$. If (25) holds with $u = 0$ then $2b_1 > 2(b - b_1)$, $2b_1 > b$, $\ell = 2(b - b_1) < b$. If (26) holds with $u = 0$ then $2b_1 = 2(b - b_1)$, $b = 2b_1 \leq \ell$. This completes the proof of (44).

Our last preliminary result is the following

$$(45) \qquad p \nmid S, \quad b = b_1, \quad u \geq 1 \implies p \nmid A.$$

As $b = b_1$, by (21), we have $p \nmid R$. Hence, by (4), we deduce $p \nmid t - A$. But $u \geq 1$ so that $p \mid t + A$. Thus we must have $p \nmid A$ as asserted.

We are now ready to prove (17). We do this by justifying the assertions of TABLE (v) above.

Cases 1 and 2 of TABLE (v) follow immediately from (34) and (35). It remains to treat cases 3–18. For these cases we have $b \geq 1$ and $\ell \geq 1$. To complete the proof of the table we must show that

(46) $p \nmid S$, cases $3, 5, 6, 7, 9, 10, 11$ ($v_p(C)$ even),
$13, 14, 15$ ($v_p(C)$ even), $17, 18$,

(47) $p \mid S$, cases $4, 8, 11$ ($v_p(C)$ odd), $12, 15$ ($v_p(C)$ odd), 16,

$$(48)\qquad \begin{cases} p \mid (m,n), & \text{cases } 3,\ 7,\ 10,\ 11\ (v_p(C) \text{ even}), \\ & 13,\ 15\ (v_p(C) \text{ even}),\ 17,\ 18, \\ p \nmid (m,n), & \text{cases } 5,\ 6,\ 9,\ 14. \end{cases}$$

Clearly (46) follows from (42) in cases 5, 6, 9, 10, 13, 14, 17, 18. We establish (46) for cases 3 and 7 by proving that

$$b \geq \ell(\text{even}) \geq 2, \quad p \mid A \implies p \nmid S.$$

We assume that $p \parallel S$ and obtain a contradiction. As $p \mid S$, by (4), we see that $p \mid t - A$, and thus $p \mid t + A$. If $p \parallel t - A$ then by (4) $p \nmid R$. Hence by (5) $p^{b-1} \parallel B_1$ so that by (6) $p^{2b-1} \parallel t^2 - 4C$. As $b \geq \ell > 1$ we have $2b - 1 > \ell$ so that $p^\ell \mid p^{2b-1} \parallel SB_1^2$. Hence by (7) we see that $p^\ell \parallel SR^2(t + A)$, that is, $p^{\ell-1} \parallel t + A$. It is clear from (9)$'$ that $v_p\Big((t + A)^2 - 4(t^2 - 4C)\Big) = v_p(Sz^2) \equiv 1 \pmod 2$ so that

$$\min\Big(2(\ell - 1), 2b - 1\Big) = 2b - 1,$$

implying $b \leq \ell - 1$, which contradicts $b \geq \ell$. If $p \parallel t + A$ then as $p \mid A$ we have $p \mid t$. Next, as $\ell \geq 2$, we have $p^2 \mid A^2 - 4C$ so $p^2 \mid C$, and thus $p^2 \mid t^2 - 4C$. By (6), $v_p(t^2 - 4C) = v_p(B_1^2 S) \equiv 1 \pmod 2$ so that $p^3 \mid t^2 - 4C$. Then, by (9)$'$, we see that $v_p\Big((t + A)^2 - 4(t^2 - 4C)\Big) = 2$, contradicting that $v_p(Sz^2) \equiv 1 \pmod 2$. Hence we must have $p^2 \mid t - A$ and $p^2 \mid t + A$. Thus $p^2 \mid A$ and, by (4), we have $p \mid R$. Next, as $\ell \geq 2$, from (7) we see that $p \mid B_1$, and thus, by (5), $p^3 \mid B$. Then, from (7), we see that $p^3 \mid A^2 - 4C$. But ℓ is even so $p^4 \mid A^2 - 4C$ and thus $p^4 \mid C$, contradicting (1).

We establish (46) for cases 11 and 15 when $v_p(C)$ is even by proving that

$$b \geq \ell(\text{odd}) \geq 1,\ p \mid A,\ p^{2k} \parallel C \implies p \nmid S.$$

As $\ell \geq 1$ we have $p \mid A^2 - 4C$ so that $p \mid C$, and thus $k \geq 1$. Hence $p^2 \mid C$ so $p^2 \mid A^2 - 4C$ showing that $\ell \geq 2$. But ℓ is odd so we must have $\ell \geq 3$. Further, as $p^\ell \parallel A^2 - 4C$, where ℓ is odd, and $p^{2k} \parallel C$, we see that $p^{2k} \parallel A^2$, that is $p^k \parallel A$. Moreover, as $b \geq \ell \geq 3$, we have $p^3 \mid B$. If $k \geq 2$ then $p^2 \mid A$, $p^3 \mid B$, $p^4 \mid C$, contradicting (1). Hence we must have $k = 1$, that is $p \parallel A$ and $p^2 \parallel C$. Suppose now that $p \mid S$, so that $p \parallel S$, we will obtain a contradiction. We consider two cases according as $p \nmid R$ or $p \mid R$. If $p \nmid R$ then by (4) we have $p \parallel t - A$. From (5) we see that $p^{b-1} \parallel B_1$, so that $p^{2b-1} \mid SB_1^2$, where $2b - 1 \geq 2\ell - 1 > \ell$. Hence from (7) we deduce that $p^\ell \parallel SR^2(t + A)$, that is, $p^{\ell-1} \parallel t + A$. From (6) we see that $p^{2b-1} \parallel t^2 - 4C$. Then, from (9)$'$, as Sz^2 is divisible by an odd power of p, we deduce that $2b - 1 < 2\ell - 2$, that is, $b \leq \ell - 1$, which contradicts $b \geq \ell$. We now turn to the case $p \mid R$, say, $p^r \parallel R$, where $r \geq 1$. From (4) we deduce that $p^{2r+1} \parallel t - A$. As $p \parallel A$ and $p^3 \mid t - A$ we have $p \parallel t + A$. From (5) we deduce that $p^{b-r-1} \parallel B_1$, so that by (6) $p^{2(b-r-1)+1} \parallel t^2 - 4C$. Then, from (9)$'$, as Sz^2 is divisible by an odd power of p, we must have $2(b - r - 1) + 1 = 1$, that is $r = b - 1$, and hence $p \parallel t^2 - 4C$. On the other hand we have $p \mid t$ and $p^2 \mid C$ so that $p^2 \mid t^2 - 4C$, which is the required contradiction. This completes the proof of (46).

Next we prove (47). First we treat cases 4 and 12. We prove

$$(49)_1 \qquad b(\text{even}) \geq 2,\quad b < \ell,\quad p \mid A,\quad p^i \parallel C \quad (i = 2, 3) \implies p \mid S$$

and

$$(49)_2 \quad b(\text{even}) \geq 2,\quad b < \ell,\quad p \mid A,$$
$$p^i \parallel C\ (i = 0, 1 \text{ or } i \geq 4) \text{ cannot occur.}$$

<u>$i = 0, 1$</u>. Here $\ell > b \geq 2$ so $p^2 \mid A^2 - 4C$. But $p \mid A$, so $p^2 \mid A^2$, and thus $p^2 \mid C$, contradicting $i = 0, 1$. This case cannot occur.

<u>$i = 2$</u>. Here $p^2 \parallel C$, $\ell > b \geq 2$ so $\ell \geq 3$, $p^3 \mid A^2 - 4C$, and thus $p \parallel A$. Assume $p \nmid S$. Then, by (5), we have $p \mid B_1$ or $p \mid R$. If $p \nmid R$, so that $p \mid B_1$,

we have by (4) $p \nmid t - A$. But, by (7), we have $p^2 \mid t + A$, contradicting $p \mid A$. Hence we must have $p \mid R$. Then, by (7), we see that $p \mid B_1$. By (4) we have $p^2 \mid t - A$ so, as $p \parallel A$, we have $p \parallel t + A$, that is $u = 1$. Hence, by (43), we have $\ell \leq b$, contradicting $b < \ell$. Thus we must have $p \mid S$ in this case.

$\underline{i = 3}$. Here $p^3 \parallel C$, $\ell > b \geq 2$, $\ell \geq 3$, $p^3 \mid A^2 - 4C$, so that $p^2 \mid A$. Assume $p \nmid S$. Then, by (5), we have $p \mid B_1$ or $p \mid R$. If $p \nmid R$, so that $p \mid B_1$, by (4) we have $p \nmid t - A$. But, by (7), we have $p^2 \mid t + A$ contradicting $p \mid A$. Hence we must have $p \mid R$. Then, by (7), we see that $p \mid B_1$. From (6), we see that $p^3 \parallel t^2 - SB_1^2$, so that $p \parallel B_1$, $p \parallel t$. Hence we have $p^2 \parallel S\left(B_1^2 - R^2(t + A)\right)$, contradicting $p^3 \mid A^2 - 4C$. Thus we must have $p \mid S$ in this case.

$\underline{i \geq 4}$. As $\ell > b \geq 2$, we have $\ell \geq 3$, so $p^3 \mid A^2 - 4C$. But $p^4 \mid C$, so $p^3 \mid A^2$, $p^2 \mid A$. Now $p^2 \mid B$ so, by (5), we have either $p \mid R$ or $p \nmid R$, $p \mid B_1$. Suppose $p \mid R$. Then, by (4), we have $p^2 \mid t - A$, and thus $p^2 \mid t + A$, $p^4 \mid R^2(t + A)$, so that $p^3 \mid SB_1^2$ by (7). If $p \mid S$ then $p \mid B_1$, $p^3 \mid B$, contradicting (1). If $p \nmid S$ then $p^3 \mid B_1^2$, $p^2 \mid B_1, p^3 \mid B$, contradicting (1). Thus we must have $p \nmid R, p \mid B_1$. By (7) we have $p^2 \mid t + A$, so $p^2 \mid t - A$, $p^2 \mid R^2S$, $p \mid R$, contradicting $p \nmid R$. Thus this case cannot occur. This completes the proof of (49), and hence of (47), for cases 4 and 12.

We now prove (47) for cases 8 and 16. We prove

$$\ell > b(\text{odd}) \geq 1, \quad p \mid A \implies p \mid S.$$

Assume that $p \nmid S$. As $\ell \geq 2$ we have $p^2 \mid A^2 - 4C$ so that $p^2 \mid C$. As $b \geq 1$ we have $p \mid B$ so by (2) either $p \mid t - A$ or $p \mid t^2 - 4C$. For both possibilities we must have $p \mid t$, so that $p \mid t - A$, $p \mid t + A$, $p^2 \mid t^2 - 4C$. Hence $u = v_p(t + A) \geq 1$. If $u = 1$, by (43), we have $\ell \leq b$ contradicting $\ell > b$. Hence $u \geq 2$ so that $p^2 \mid t + A$. From (6) we deduce $p \mid B_1$, and from (4) that $p \mid R$ and $p^2 \mid t - A$. Hence $p^2 \mid A$. From (5) we see that $p^2 \mid B$ so that $b \geq 2$. But b is odd so $b \geq 3$, and $p^3 \mid B$. As $\ell > b \geq 3$ we have $\ell \geq 4$ so $p^4 \mid A^2 - 4C$, and thus $p^4 \mid C$, contradicting (1). This completes the proof of (47) for cases 8 and 16.

We now prove (47) for cases 11 and 15 when $v_p(C)$ is odd by proving that

$$b \geq \ell(\text{odd}) \geq 1, \quad p \mid A, \quad p^{2k+1} \parallel C \implies p \mid S.$$

Let $a = v_p(A)$ so that $p^a \parallel A$, where $a \geq 1$. As $p^\ell \parallel A^2 - 4C$, where ℓ is odd, $p^{2a} \parallel A^2$ and $p^{2k+1} \parallel C$, we must have $\ell = 2k+1 < 2a$. If $k \geq 2$ then $b \geq \ell \geq 5$ and $a \geq 3$, so that $p^3 \mid A$, $p^5 \mid B$, $p^5 \mid C$, which contradicts (1). Hence we must have $k = 0$ or $k = 1$ that is $\ell = 1$ or $\ell = 3$. We suppose that $p \nmid S$ and obtain a contradiction. We consider two cases according as $p \nmid R$ or $p \mid R$. If $p \nmid R$ then by (4) we see that $p \nmid t - A$. As $p \mid A$ we have $p \nmid t$. On the other hand as $p \mid B$ and $p \nmid t - A$ from (2) we see that $p \mid t^2 - 4C$, so that as $p \mid C$, we have the contradiction $p \mid t$. If $p \mid R$ then $p^r \parallel R$ for some $r \geq 1$. From (4) we deduce that $p^{2r} \parallel t - A$ and thus as $p \mid A$ we have $p \mid t$ and $p \mid t + A$. From (5) we obtain $p^{b-r} \parallel B_1$. Thus, from (7), as

$$p^\ell \parallel A^2 - 4C \ (\ell = 1 \text{ or } 3), \quad p^{2(b-r)} \parallel SB_1^2,$$
$$p^{2r+v_p(t+A)} \mid SR^2(t+A), 2r + v_p(t+A) \geq 3,$$

we must have

$$\ell = 3,\ b - r \geq 2,\ 2r + v_p(t+A) = 3.$$

Hence

$$k = 1,\ a \geq 2,\ r = v_p(t+A) = 1,\ b \geq 3,$$

and thus

$$p^3 \parallel C,\ p \parallel R,\ p^2 \parallel t - A,\ p \parallel t + A,$$
$$p^2 \mid A,\ p \parallel t,\ p^2 \parallel t^2 - 4C,\ p \parallel B_1 \text{ (by (6))},$$

$p^2 \parallel B$ (by (5)), $b = 2$, contradicting $b \geq 3$. This completes the proof of (47).

We now prove (48). Let p be an odd prime with $p \nmid S$, so that we are in cases 3, 5–7, 9–10, 11 ($v_p(C)$ even), 13–14, 15 ($v_p(C)$ even), 17–18. By (36) we have $x \geq 1$. Exactly one of (24), (25), (26) occurs.

We begin by supposing that (24) occurs, so ℓ is even, and we are in cases 3, 5–7, 9–10. (48) follows from the table below.

	cases	assertion	reason
$u=0$	3,7, 6, 10 5,9	cannot occur cannot occur $p \nmid m$	(38) (44) (32)
$u=1$	3,7 6, 10 5,9	$p \mid (m,n)$ cannot occur cannot occur	(30) (43) (40)
$u \geq 2,\ b_1 = 1$	3,7, 10 6 5,9	$p \mid (m,n)$ cannot occur cannot occur	(31) (24) (39)
$u \geq 2,\ b_1 \geq 2$	3,5,7,9 10 6	cannot occur $p \mid (m,n)$ $p \nmid n$	$\ell = 2b_1 = 2b > b(24),(41)$ $(24),(31),(41)$ $(24),(33),(41)$

Next we suppose that (25) occurs, so that $\ell \equiv u \pmod 2$. In cases 3, 5–7, 9–10, ℓ and u are both even, whereas, in cases 11, 13–15, 17–18, ℓ and u are both odd. (48) follows from the table below.

	cases	assertion	reason
$u=0$	3, 7, 11, 13, 14, 15, 17, 18 6, 10 5, 9	cannot occur cannot occur cannot occur $p \nmid m$	(38) u odd (44) (32)
$u=1$	11, 13, 15, 17, 18 14 3, 5, 6, 7, 9, 10	$p \mid (m,n)$ cannot occur cannot occur	(30) (43) u even
$u \geq 2, b_1 = 1$	3, 7, 10, 11, 13, 15, 17, 18 5, 6, 9, 14	$p \mid (m,n)$ cannot occur	(31) (39)
$u \geq 2, b_1 \geq 2$	10, 18 6, 14 5, 9 11, 13, 15, 17 3, 7	$p \mid (m,n)$ $p \nmid n$ $p \nmid m$ $p \mid (m,n)$ cannot occur	(25), (31), (41) (25), (33), (41) (25), (32), (41) (25), (30), (41) (41), (45)

Finally we suppose that (26) occurs, so that u is even. (48) follows from the table below.

	cases	assertion	reason
$u=0$	5, 6, 14	$p \nmid m$	(37)
	7, 9, 11, 13	cannot occur	(44)
	3, 15	cannot occur	(38)
	10, 17, 18	cannot occur	(26)
$u \geq 2, b_1 = 1$	3, 7, 10, 11, 13, 15, 17, 18	$p \mid (m, n)$	(31)
	5, 6, 9, 14	cannot occur	(39)
$u \geq 2, b_1 \geq 2$	3, 5, 7, 9, 11, 13, 15, 17	cannot occur	(26), (41)
	6, 14	$p \nmid n$	(26), (33), (41)
	10, 18	$p \mid (m, n)$	(26), (31), (41)

This completes the proof of (17).

PROOF of (16). We treat each of the cases specified in TABLE (iv) separately. We just give the details for the case

$$m \equiv 2 \pmod 8, \quad n \equiv 2 \pmod 4, \quad S \equiv 1 \pmod 8,$$

as this serves as a model for the rest of the cases. Recall that $2^b \parallel B$, $2^\ell \parallel A^2 - 4C$. We define the integers r and μ by $2^r \parallel R$, $2^\mu \parallel M$, so that

$$(50) \qquad \begin{cases} R \equiv 2^r \pmod{2^{r+1}}, & \\ R^2 \equiv 2^{2r} \pmod{2^{2r+3}}, & \\ t - A \equiv 2^{2r} \pmod{2^{2r+3}}, & \text{by (4)}, \\ M \equiv 2^\mu \pmod{2^{\mu+1}}, & \\ t + A \equiv -2^{2\mu+1} \pmod{2^{2\mu+3}}, & \text{by (10)}, \\ B_1 \equiv 2^{2\mu} \pmod{2^{2\mu+1}}, & \text{by (10)}, \\ b = 2\mu + r, & \text{by (5)}. \end{cases}$$

From the congruences for $t - A$ and $t + A$, we obtain the following congruences:

$$(51)\quad \begin{cases} t \equiv -2^{2\mu} \pmod{2^{2\mu+2}}, & \\ A \equiv -2^{2\mu} \pmod{2^{2\mu+2}}, & \text{if } r \geq \mu+2, \\ t \equiv 2^{2\mu} \pmod{2^{2\mu+2}}, & \\ A \equiv 2^{2\mu} \pmod{2^{2\mu+1}}, & \text{if } r = \mu+1, \\ t \equiv -2^{2\mu-1} \pmod{2^{2\mu+2}}, & \\ A \equiv 5 \cdot 2^{2\mu-1} \pmod{2^{2\mu+1}}, & \text{if } r = \mu, \\ t \equiv 2^{2r-1} \pmod{2^{2r+2}}, & \\ A \equiv -2^{2r-1} \pmod{2^{2r+2}}, & \text{if } r \leq \mu-1. \end{cases}$$

Appealing to (7) we see that there are integers g and h such that

$$A^2 - 4C = (8g+1)2^{4\mu} + (4h+1)2^{2r+2\mu+1},$$

so that

$$(52)\quad \ell = \begin{cases} 4\mu, & \text{if } r \geq \mu, \\ 2r+2\mu+1, & \text{if } r \leq \mu-1, \end{cases}$$

and

$$(53)\quad (A^2-4C)/2^{\ell} \equiv \begin{cases} 1 \pmod 8, & \text{if } r \geq \mu+1, \\ 3 \pmod 8, & \text{if } r = \mu, \\ 3 \pmod 4, & \text{if } r = \mu-1, \\ 1 \pmod 4, & \text{if } r \leq \mu-2. \end{cases}$$

Next, from (6), we obtain

$$(54)\quad \begin{cases} C \equiv 0 \pmod{2^{4\mu+1}}, & \text{if } r \geq \mu+1, \\ C \equiv 2^{4\mu-4} - 2^{4\mu-2} \pmod{2^{4\mu-1}}, & \text{if } r = \mu, \\ C \equiv 2^{4r-4} \pmod{2^{4r-1}}, & \text{if } r \leq \mu-1. \end{cases}$$

Thus we have

$$(55)\quad \begin{cases} 2^{2\mu} \parallel A,\ 2^{3\mu+2} \mid B,\ 2^{4\mu+1} \mid C, & \text{if } r \geq \mu+2, \\ 2^{2\mu} \parallel A,\ 2^{3\mu+1} \mid B,\ 2^{4\mu+1} \mid C, & \text{if } r = \mu+1, \\ 2^{2\mu-1} \parallel A,\ 2^{3\mu} \parallel B,\ 2^{4\mu-4} \parallel C, & \text{if } r = \mu, \\ 2^{2r-1} \parallel A,\ 2^{3r+2} \mid B,\ 2^{4r-4} \parallel C, & \text{if } r \leq \mu-1, \end{cases}$$

and so, by (1), we have

$$
(56) \qquad \begin{cases} \mu = 0, & \text{if } r \geq \mu + 2, \\ \mu = 0, & \text{if } r = \mu + 1, \\ \mu = 1, & \text{if } r = \mu, \\ r = 1, & \text{if } r \leq \mu - 1. \end{cases}
$$

Appealing to (50), (51), (52), (53), (54), and (56), we have:

I: $m \equiv 2 \pmod 8$, $n \equiv 2 \pmod 4$, $S \equiv 1 \pmod 8$		
$A \equiv 3 \pmod 4$,	$B \equiv 0 \pmod 4$,	$C \equiv 0 \pmod 2$,
$b \geq 2, \ell = 0, (A^2 - 4C)/2^\ell \equiv 1 \pmod 8$,		
$A \equiv 1 \pmod 4$,	$B \equiv 2 \pmod 4$,	$C \equiv 0 \pmod 2$,
$b = 1, \ell = 0, (A^2 - 4C)/2^\ell \equiv 1 \pmod 8$,		
$A \equiv 10 \pmod{16}$,	$B \equiv 8 \pmod{16}$,	$C \equiv 5 \pmod 8$
$b = 3, \ell = 4, (A^2 - 4C)/2^\ell \equiv 3 \pmod 8$,		
$A \equiv 14 \pmod{16}$,	$B \equiv 32 \pmod{64}$,	$C \equiv 1 \pmod 8$
$b = 5, \ell = 7, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$,		
$A \equiv 14 \pmod{16}$,	$B \equiv 0 \pmod{128}$,	$C \equiv 1 \pmod 8$,
$\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$.		

Similarly for the remaining eleven cases in TABLE (iv) we obtain:

II: $m \equiv 6 \pmod 8$, $n \equiv 2 \pmod 4$, $S \equiv 5 \pmod 8$		
$A \equiv 1 \pmod 4$,	$B \equiv 0 \pmod 4$,	$C \equiv 1 \pmod 2$,
$\ell = 0, b \geq 2, (A^2 - 4C)/2^\ell \equiv 5 \pmod 8$		
$A \equiv 3 \pmod 4$,	$B \equiv 2 \pmod 4$,	$C \equiv 1 \pmod 2$,
$\ell = 0, b = 1, (A^2 - 4C)/2^\ell \equiv 5 \pmod 8$		
$A \equiv 6 \pmod{16}$,	$B \equiv 32 \pmod{64}$,	$C \equiv 1 \pmod 8$,
$\ell = 7, b = 5, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$		
$A \equiv 6 \pmod{16}$,	$B \equiv 0 \pmod{128}$,	$C \equiv 1 \pmod 8$,
$\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$		
$A \equiv 10 \pmod{16}$,	$B \equiv 8 \pmod{16}$,	$C \equiv 5 \pmod 8$,
$\ell = 4, b = 3, (A^2 - 4C)/2^\ell \equiv 3 \pmod 8$		

III: $m \equiv 1 \pmod 4$, $n \equiv 0 \pmod 4$, $S \equiv 1 \pmod 8$
$A \equiv 1 \pmod 4$, $B \equiv 0 \pmod 4$, $C \equiv 1 \pmod 2$, $\ell = 0, b \geq 2, (A^2 - 4C)/2^\ell \equiv 5 \pmod 8$
$A \equiv 1 \pmod 4$, $B \equiv 2 \pmod 4$, $C \equiv 0 \pmod 4$, $\ell = 0, b = 1, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 3 \pmod 4$, $B \equiv 0 \pmod 4$, $C \equiv 0 \pmod 2$, $\ell = 0, b \geq 2, (A^2 - 4C)/2^\ell \equiv 1 \pmod 8$
$A \equiv 3 \pmod 4$, $B \equiv 2 \pmod 4$, $C \equiv 3 \pmod 4$, $\ell = 0, b = 1, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 6 \pmod 8$, $B \equiv 0 \pmod{64}$, $C \equiv 1 \pmod 8$, $b \geq \ell(\text{even}) \geq 6, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 6 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell = 7, b = 5, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 6 \pmod{16}$, $B \equiv 0 \pmod{64}$, $C \equiv 1 \pmod 8$, $b \geq \ell = 6, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 6 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 1 \pmod 8$, $\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$
$A \equiv 14 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell = 7, b = 5, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$
$A \equiv 14 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 1 \pmod 8$, $\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 14 \pmod{16}$, $B \equiv 0 \pmod{256}$, $C \equiv 1 \pmod 8$, $b \geq \ell(\text{even}) \geq 8, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$

IV: $m \equiv 3 \pmod 4$, $n \equiv 2 \pmod 4$, $S \equiv 5 \pmod 8$
$A \equiv 0 \pmod 2$, $B \equiv 1 \pmod 2$, $C \equiv 1 \pmod 2$, $\ell \geq 2, b = 0, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 2 \pmod 8$, $B \equiv 0 \pmod{16}$, $C \equiv 5 \pmod 8$, $b \geq \ell = 4, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 6 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 1 \pmod 8$, $\ell(\text{even}) = b + 1 \geq 8, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$
$A \equiv 14 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell = 6, b = 5, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$

V: $m \equiv 6 \pmod 8$, $n \equiv 2 \pmod 4$, $S \equiv 1 \pmod 8$
$A \equiv 1 \pmod 4$, $B \equiv 0 \pmod 4$, $C \equiv 0 \pmod 2$, $\ell = 0, b \geq 2, (A^2 - 4C)/2^\ell \equiv 1 \pmod 8$
$A \equiv 3 \pmod 4$, $B \equiv 2 \pmod 4$, $C \equiv 0 \pmod 2$, $\ell = 0, b = 1, (A^2 - 4C)/2^\ell \equiv 1 \pmod 8$
$A \equiv 2 \pmod{16}$, $B \equiv 8 \pmod{16}$, $C \equiv 5 \pmod 8$, $\ell = 4, b = 3, (A^2 - 4C)/2^\ell \equiv 7 \pmod 8$
$A \equiv 14 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell = 7, b = 5, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 14 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 1 \pmod 8$, $\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$

VI: $m \equiv 2 \pmod 8$, $n \equiv 2 \pmod 4$, $S \equiv 5 \pmod 8$
$A \equiv 1 \pmod 4$, $B \equiv 2 \pmod 4$, $C \equiv 1 \pmod 2$, $\ell = 0, b = 1, (A^2 - 4C)/2^\ell \equiv 5 \pmod 8$
$A \equiv 3 \pmod 4$, $B \equiv 0 \pmod 4$, $C \equiv 1 \pmod 2$, $\ell = 0, b \geq 2, (A^2 - 4C)/2^\ell \equiv 5 \pmod 8$
$A \equiv 2 \pmod{16}$, $B \equiv 8 \pmod{16}$, $C \equiv 5 \pmod 8$, $\ell = 4, b = 3, (A^2 - 4C)/2^\ell \equiv 7 \pmod 8$
$A \equiv 6 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell = 7, b = 5, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$
$A \equiv 6 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 1 \pmod 8$, $\ell(\text{odd}) = b + 2 \geq 9, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$

VII: $m \equiv 2 \pmod 4$, $n \equiv 0 \pmod 4$, $S \equiv 1 \pmod 4$
$A \equiv 2 \pmod 8$, $B \equiv 0 \pmod{16}$, $C \equiv 1 \pmod 8$, $\ell = 5, b \geq 4, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 4 \pmod 8$, $B \equiv 0 \pmod{32}$, $C \equiv 4 \pmod{16}$, $b + 1 \geq \ell \geq 6, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 6 \pmod{16}$, $B \equiv 0 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell(\text{odd}) = b + 1 \geq 7, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 14 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 1 \pmod 8$, $b \geq \ell(\text{odd}) \geq 7, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$

VIII: $m \equiv 3 \pmod 4$, $n \equiv 0 \pmod 4$, $S \equiv 1 \pmod 8$
$A \equiv 0 \pmod 8$, $B \equiv 0 \pmod{16}$, $C \equiv 4 \pmod{16}$, $b \geq \ell = 4, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$
$A \equiv 2 \pmod 8$, $B \equiv 0 \pmod{64}$, $C \equiv 1 \pmod 8$, $b \geq \ell(\text{even}) \geq 6, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 2 \pmod 8$, $B \equiv 0 \pmod{32}$, $C \equiv 1 \pmod 8$, $\ell \geq b(\text{odd}) + 3 \geq 8, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 6 \pmod{16}$, $B \equiv 0 \pmod{64}$, $C \equiv 1 \pmod 8$, $b \geq \ell = 6, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$
$A \equiv 14 \pmod{16}$, $B \equiv 0 \pmod{256}$, $C \equiv 1 \pmod 8$, $b \geq \ell(\text{even}) \geq 8, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$

IX: $m \equiv 1 \pmod 4$, $n \equiv 2 \pmod 4$, $S \equiv 5 \pmod 8$
$A \equiv 4 \pmod 8$, $B \equiv 8 \pmod{16}$, $C \equiv 12 \pmod{16}$, $\ell = 5, b = 3, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 6 \pmod 8$, $B \equiv 0 \pmod{16}$, $C \equiv 5 \pmod 8$, $\ell = 4, b \geq 4, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 6 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 1 \pmod 8$, $\ell(\text{even}) = b + 1 \geq 8, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 14 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell = 6, b = 5, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$

X: $m \equiv 1 \pmod 2$, $n \equiv 1 \pmod 2$, $S \equiv 1 \pmod 4$
$A \equiv 0 \pmod 4$, $B \equiv 4 \pmod 8$, $C \equiv 3 \pmod 4$, $\ell = b = 2, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 2 \pmod 4$, $B \equiv 0 \pmod 8$, $C \equiv 0 \pmod 4$, $\ell = 2, b \geq 3, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 6 \pmod 8$, $B \equiv 16 \pmod{32}$, $C \equiv 1 \pmod 8$, $\ell \geq 7, b = 4, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 6 \pmod 8$, $B \equiv 0 \pmod{64}$, $C \equiv 1 \pmod 8$, $\ell(\text{even}) = b + 2 \geq 8, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$

XI: $m \equiv 4 \pmod 8$, $n \equiv 2 \pmod 4$, $S \equiv 2 \pmod 8$
$A \equiv 4 \pmod{16}$, $B \equiv 16 \pmod{32}$, $C \equiv 28 \pmod{32}$, $\ell = 5, b = 4, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 8 \pmod{16}$, $B \equiv 0 \pmod{32}$, $C \equiv 8 \pmod{32}$, $\ell = 5, b \geq 5, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 12 \pmod{16}$, $B \equiv 64 \pmod{128}$, $C \equiv 4 \pmod{32}$, $\ell \geq 10, b = 6, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$
$A \equiv 12 \pmod{16}$, $B \equiv 0 \pmod{256}$, $C \equiv 4 \pmod{32}$, $\ell(\text{odd}) = b + 3 \geq 11, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$

XII: $m \equiv 2 \pmod 4$, $n \equiv 1 \pmod 2$, $S \equiv 2 \pmod 8$
$A \equiv 0 \pmod 8$, $B \equiv 8 \pmod{16}$, $C \equiv 6 \pmod 8$, $\ell = b = 3, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 4 \pmod 8$, $B \equiv 0 \pmod{16}$, $C \equiv 2 \pmod 8$, $\ell = 3, b \geq 4, (A^2 - 4C)/2^\ell \equiv 1 \pmod 4$
$A \equiv 12 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 4 \pmod{32}$, $\ell = 7, b = 5, (A^2 - 4C)/2^\ell \equiv 3 \pmod 4$
$A \equiv 12 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 4 \pmod{32}$, $\ell(\text{even}) = b + 3 \geq 10, (A^2 - 4C)/2^\ell \equiv 1 \pmod 2$

From these tables, and TABLES (i) and (iv), we obtain the following values of λ and α

I	$\lambda = -1$,	$\alpha = 0$	VII	$\lambda = 2$,	$\alpha = 3$
II	$\lambda = -1$,	$\alpha = 0$	VIII	$\lambda = 2$,	$\alpha = 2$
III	$\lambda = 0$,	$\alpha = 0$	IX	$\lambda = 2$,	$\alpha = 2$
IV	$\lambda = 0$,	$\alpha = 0$	X	$\lambda = 3$,	$\alpha = 3$
V	$\lambda = 1$,	$\alpha = 2$	XI	$\lambda = 3$,	$\alpha = 4$
VI	$\lambda = 1$,	$\alpha = 2$	XII	$\lambda = 3$,	$\alpha = 4$

which proves (16).

This completes the proof of case (i) of Theorem 1. □

We now give the special case $A = 0$ as a corollary to Theorem 1.

Corollary. *Let $K = Q(\theta)$ be a cyclic quartic extension of Q, where θ is a root of the irreducible polynomial $X^4 + BX + C$, where B and C are (nonzero) integers for which there does not exist a prime p with $p^3 \mid B$, $p^4 \mid C$. Then the conductor $f(K)$ of K is given by*

$$f(K) = 2^{\delta} \prod_{\substack{p \neq 2 \\ p \mid B, p \mid C}} p,$$

where the values of δ are given in Table (vi).

TABLE (vi): Values of δ			
δ	congruence conditions	examples	
0	$B \equiv C \equiv 1 \pmod 2$	$X^4 - 5X + 5$	$f(K) = 5$
2	$B \equiv 0 \pmod 8,\ C \equiv 4 \pmod 8$	$X^4 - 272X + 884$	$f(K) = 2^2 \cdot 17$
3	$B \equiv 0 \pmod 4,\ C \equiv 1 \pmod 2$	$X^4 - 20X + 95$	$f(K) = 2^3 \cdot 5$
4	$B \equiv 0 \pmod 8,\ C \equiv 2 \pmod 4$	$X^4 + 8X + 14$	$f(K) = 2^4$

PROOF. We first show that we cannot have

$$A = 0,\ B \equiv 0 \pmod 8,\ C \equiv 0 \pmod 8)$$

in case (i) of the theorem. Suppose this possibility occurs. Then, by (1), we must have $C \equiv 8 \pmod{16}$, and, by Proposition 1, we have $S \equiv 1, 2$, or $5 \pmod 8$. Define the integers r, s and x by

$$2^r \parallel R,\ 2^s \parallel S,\ 2^x \parallel B_1.$$

As S is squarefree we have $s = 0$ or 1. From (4) (with $A = 0$) and (5) we obtain

$$2^{2r+s} \parallel t, \quad 2^{x+r+s} \parallel B.$$

As $B \equiv 0 \pmod 8$ we must have

$$x + r + s \geq 3.$$

From (6) we have

$$4C = t^2 - B_1^2 S.$$

Note that $2^{4r+2s} \parallel t^2$ and $2^{2x+s} \parallel B_1^2 S$. We consider three cases

(a) $4r + 2s < 2x + s$,

(b) $4r + 2s = 2x + s$,

(c) $4r + 2s > 2x + s$.

Case (a). In this case we have $2^{4r+2s} \parallel 4C$, so that $4r+2s=5$, which is impossible.

Case (b). In this case $4r+2s=2x+s\leq 5$ so that $s=0$, $x=2r$, $r=0$ or 1. If $r=0$ then we have $x=0$ contradicting $x+r+s\geq 3$. Hence we have $r=1, x=2, s=0$, so that

$$2 \parallel R, S \equiv 1 \pmod 4,\ 2^2 \parallel B_1,\ 2^2 \parallel t,\ 2^3 \parallel B,\ 2^3 \parallel C.$$

Setting

$$t=4t_1,\ B_1=4B_2,\ C=8C_1,$$

where t_1, B_2, C_1 are all odd, in $4C=t^2-B_1^2S$, and dividing by 2^4, we obtain $2C_1=t_1^2-B_2^2S$. Taking this equation modulo 4 we obtain

$$2 \equiv 2C_1 \equiv t_1^2-B_2^2S \equiv 1-1 \equiv 0 \pmod 4,$$

which is impossible.

Case (c). In this case we have $4r+s>2x$ and $2^{2x+s} \parallel 4C$ so that $2x+s=5$. Hence we have $s=1$, $x=2$ and $r\geq 1$. Thus we have

$$2^r \parallel R,\ S\equiv 2 \pmod 8,\ 2^2 \parallel B_1,\ 2^{2r+1} \parallel t,\ 2^{r+3} \parallel B,\ 2^3 \parallel C.$$

Setting

$$t=2^{2r+1}t_1,\ B_1=4B_2,\ C=8C_1,\ S=2S_1,$$

where $t_1\equiv B_2\equiv C_1\equiv 1 \pmod 2$, $S_1\equiv 1 \pmod 4$, in $4C=t^2-B_1^2S$, and dividing by 2^5, we obtain $C_1=2^{4r-3}t_1^2-B_2^2S_1$. Taking this equation modulo 4 we obtain

$$C_1 \equiv \begin{cases} 2-1\equiv 1 \pmod 4, & \text{if } r=1, \\ 0-1\equiv 3 \pmod 4, & \text{if } r\geq 2. \end{cases}$$

From (9) with $A=0$ we have $16C-3t^2=Sz^2$, so that $S_1z^2=2^6C_1-3\cdot 2^{4r+1}t_1^2$. If $r=1$ then we have $2^5 \parallel S_1z^2$, which is impossible. Hence we have $r\geq 2$ and so $2^6 \parallel S_1z^2$, $2^6 \parallel z^2$, $2^3 \parallel z$, say $z=2^3z_1$, where z_1 is odd. Thus $S_1z_1^2=C_1-3\cdot 2^{4r-5}t_1^2$. Taking this equation modulo 4 we obtain

$$1\equiv S_1z_1^2 \equiv C_1-3\cdot 2^{4r-5}t_1^2 \equiv 3 \pmod 4,$$

which is impossible.

This completes the proof that $B\equiv C\equiv 0 \pmod 8$ does not occur when $A=0$. The corollary now follows from case (i) of Theorem 1 with $A=0$. □

Our next two results give the unique quadratic subfield k (Theorem 2) and the discriminant $d(K)$ (Theorem 3) of the cyclic quartic field $K=Q(\theta)$, where $\theta^4+A\theta^2+B\theta+C=0$, explicitly in terms of the prime factors of A, B and C.

Theorem 2. *With the notation of Theorem 1, the unique quadratic subfield of the cyclic quartic field $K = Q(\theta)$ where $\theta^4 + A\theta^2 + B\theta + C = 0$, is $k = Q\left(\sqrt{S}\right)$, where S is given as follows:*

<u>*Case (i)*: $A^2 - 4C \neq 0, B \neq 0$</u>.

$$S = 2^{\theta} \prod_{\substack{p \neq 2 \\ p \mid A, p \mid B, p \mid C \\ v_p(B) < v_p(A^2-4C)}} p \prod_{\substack{p \neq 2 \\ p \mid A, p \mid B, p \mid C \\ v_p(A^2-4C)(\text{odd}) \leq v_p(B), v_p(C) \text{ odd}}} p,$$

where $\theta = 0$ except in the following cases when $\theta = 1$:

$A \equiv 4 \pmod{16}$, $B \equiv 16 \pmod{32}$, $C \equiv 28 \pmod{32}$,
$\ell = 5$, $b = 4$, $(A^2 - 4C)/2^{\ell} \equiv 1 \pmod 4$,

$A \equiv 8 \pmod{16}$, $B \equiv 0 \pmod{32}$, $C \equiv 8 \pmod{32}$,
$\ell = 5$, $b \geq 5$, $(A^2 - 4C)/2^{\ell} \equiv 1 \pmod 4$,

$A \equiv 12 \pmod{16}$, $B \equiv 64 \pmod{128}$, $C \equiv 4 \pmod{32}$,
$\ell \geq 10$, $b = 6$,

$A \equiv 12 \pmod{16}$, $B \equiv 0 \pmod{256}$, $C \equiv 4 \pmod{32}$,
$\ell(\text{odd}) = b + 3 \geq 11$,

$A \equiv 0 \pmod 8$, $B \equiv 8 \pmod{16}$, $C \equiv 6 \pmod 8$,
$\ell = b = 3$, $(A^2 - 4C)/2^{\ell} \equiv 1 \pmod 4$,

$A \equiv 4 \pmod 8$, $B \equiv 0 \pmod{16}$, $C \equiv 2 \pmod 8$,
$\ell = 3$, $b \geq 4$, $(A^2 - 4C)/2^{\ell} \equiv 1 \pmod 4$,

$A \equiv 12 \pmod{16}$, $B \equiv 32 \pmod{64}$, $C \equiv 4 \pmod{32}$,
$\ell = 7$, $b = 5$, $(A^2 - 4C)/2^{\ell} \equiv 3 \pmod 4$,

$A \equiv 12 \pmod{16}$, $B \equiv 0 \pmod{128}$, $C \equiv 4 \pmod{32}$,
$\ell(\text{even}) = b + 3 \geq 10$,

where $\ell = v_2(A^2 - 4C)$ and $b = v_2(B)$.

<u>*Case (ii)*: $A^2 - 4C = 0, B \neq 0$</u>.

$$S = 2^{\phi} \prod_{\substack{p \neq 2 \\ p \mid A, p^2 \| B}} p \prod_{\substack{p \neq 2 \\ p \| A, p^3 \mid B}} p,$$

where $\phi = 0$ except where $v_2(B) = 6$ in which case $\phi = 1$.

<u>*Case (iii)*: $A^2 - 4C \neq 0, B = 0$</u>.

$$S = 2^{\rho} \prod_{\substack{p \neq 2 \\ v_p(C) \text{ odd}}} p,$$

where

$$\rho = \begin{cases} 0, & \text{if } v_2(C) \text{ even}, \\ 1, & \text{if } v_2(C) \text{ odd}. \end{cases}$$

PROOF. We just treat Case (i). By (8) we have $k = Q\left(\sqrt{S}\right)$. From the tables immediately following (56), we see that the 2-part of S is 2^θ, where

$$\theta = \begin{cases} 0, & \text{in cases I–X}, \\ 1, & \text{in cases XI, XII}. \end{cases}$$

From Table (v), remembering that S is squarefree, we see that the odd part of S is

$$\prod_{\substack{p\neq 2 \\ p|A,p|B,p|C \\ v_p(B)<v_p(A^2-4C)}} p \prod_{\substack{p\neq 2 \\ p|A,p|B,p|C \\ v_p(A^2-4C)(\text{odd})\leq v_p(B) \\ v_p(C) \text{ odd}}} p.$$

This proves the asserted formula for S. □

Before stating our next theorem, we recall that $\alpha, \beta, \gamma, \theta, \phi, \rho$ are defined in Table (i), Table (ii), Table (iii), Theorem 2 (Case (i)), Theorem 2 (Case (ii)), Theorem 2 (Case (iii)) respectively.

Theorem 3. *With the notation of Theorems 1 and 2, the discriminant $d(K)$ of the cyclic quartic field $K = Q(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$, is given as follows:*

Case (i): $A^2 - 4C \neq 0,\ B \neq 0$.

$$d(K) = 2^{2\alpha+3\theta} \prod_{p\in S_2} p^2 \prod_{p\in S_3} p^3,$$

where

$$S_2 = \Big\{p \neq 2 \,\Big|\, v_p(B)(odd) < v_p(A^2-4C),\ p\nmid C \text{ or } v_p(A^2-4C)(odd) \leq v_p(B),\ v_p(C) \text{ even or } 2 \leq v_p(A^2-4C)(even) \leq v_p(B),\ p \mid C\Big\}$$

and

$$S_3 = \Big\{p \neq 2 \,\Big|\, 1 \leq v_p(B) < v_p(A^2-4C),\ p \mid C \text{ or } v_p(A^2-4C)(odd) \leq v_p(B),\ v_p(C) \text{ odd}\Big\}.$$

Case (ii): $\mathbf{A^2 - 4C = 0,\ B \neq 0}$.

$$d(K) = 2^{2\beta+3\phi} \prod_{p \in S_2} p^2 \prod_{p \in S_3} p^3,$$

where

$$S_2 = \left\{ p \neq 2 \;\middle|\; p \parallel B \quad or \quad p \nmid A,\ v_p(B)(odd) \geq 3 \right\},$$

and

$$S_3 = \left\{ p \neq 2 \;\middle|\; p \mid A,\ p^2 \parallel B \quad or \quad p \parallel A,\ p^3 \mid B \right\}.$$

Case (iii): $\mathbf{A^2 - 4C \neq 0, B = 0}$

$$d(K) = 2^{2\gamma+3\rho} \prod_{p \in S_2} p^2 \prod_{p \in S_3} p^3,$$

where

$$S_2 = \left\{ p \neq 2 \;\middle|\; p \mid A,\ v_p(C)(even) \geq 2 \right\},$$

and

$$S_3 = \left\{ p \neq 2 \;\middle|\; v_p(C)\ odd \right\}.$$

PROOF. This theorem follows from $d(K) = f(K)^2 d(k)$, $d(k) = 2^{2v_2(S)} S$, Theorem 1 and Theorem 2. □

Our final theorem gives a necessary and sufficient condition for a cyclic quartic field to be totally imaginary.

Theorem 4. *With the notation of Theorem 1, let K be the cyclic quartic field $Q(\theta)$, where θ is a root of $\theta^4 + A\theta^2 + B\theta + C = 0$. Then*

Case (i): *K is totally imaginary* $\iff 2A^3 - 8AC + B^2 > 0$,
Case (ii): *K is always totally imaginary,*
Case (iii): *K is totally imaginary* $\iff A > 0$.

PROOF. We just treat Case (i). We have $K = Q\left(\sqrt{m + n\sqrt{S}}\right)$. As K is cyclic we have $K = Q\left(\sqrt{m \pm |n|\sqrt{S}}\right)$, and there exists an integer $k (\neq 0)$ such that $m^2 - Sn^2 = Sk^2$. Thus $|m| > |n|\sqrt{S}$. If $m > 0$ then $m > |n|\sqrt{S}$ so $m - |n|\sqrt{S} > 0$ and K is totally real. If $m < 0$ then

$-m > |n|\sqrt{S}$ so $m + |n|\sqrt{S} < 0$ and K is totally imaginary. We have thus shown that

$$K \text{ is totally imaginary} \iff m < 0.$$

By (10) we have

$$m < 0 \iff t + A > 0,$$

and, as $t + A$ is the unique real root of the polynomial

$$X^3 - 4AX^2 + (5A^2 - 4C)X + (-2A^3 + 8AC - B^2),$$

we have

$$t + A > 0 \iff -2A^3 + 8AC - B^2 < 0,$$

completing the proof. □

We close by remarking that Theorem 5 of [1] follows easily from Theorem 1.

References

[1] K. Hardy, R. Hudson, D. Richman, K.S. Williams and N.M. Holtz, Calculation of the class numbers of imaginary cyclic quartic fields, Carleton-Ottawa Mathematical Lecture Note Series Number 7, July, 1986, 201 pp.
[2] J.G. Huard, B.K. Spearman and K.S. Williams, Integral bases for quartic fields with quadratic subfields, *J. Number Theory* **51** (1995), 87–102.
[3] L.-C. Kappe and B. Warren, An elementary test for the galois group of a quartic polynomial, *Amer. Math. Monthly* **96** (1989), 133–137.
[4] W.C. Schulz, Cubics with a rational root, *Math. Mag.* **64** (1991), 172–175.

BLAIR K. SPEARMAN
DEPARTMENT OF MATHEMATICS AND STATISTICS
OKANAGAN UNIVERSITY COLLEGE
KELOWNA, B.C. V1V 1V7
CANADA

KENNETH S. WILLIAMS
DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO K1S 5B6
CANADA

(Received May 2, 1994)