

CYCLIC QUARTIC FIELDS WITH RELATIVE INTEGRAL BASES OVER THEIR QUADRATIC SUBFIELDS

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

(Communicated by Larry J. Goldstein)

ABSTRACT. Explicit conditions are given for a cyclic quartic field to have a relative integral basis over its unique quadratic subfield.

Throughout this paper, K denotes a cyclic quartic extension of the rational number field Q . By Theorem 1 of [3] we know that K can be expressed uniquely in the form

$$(1) \quad K = Q\left(\sqrt{A(D + B\sqrt{D})}\right),$$

where A, B, C, D are integers such that

A is squarefree and odd,

$D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$,

$(A, D) = 1$.

K possesses a unique quadratic subfield $k = Q(\sqrt{D})$. Although K possesses an integral basis over Q (an explicit integral basis is given in [4]) it may or may not have a relative integral basis (RIB) over k . In this paper we give a necessary and sufficient condition for K to have a RIB over k . This is done by using the integral basis for K over Q given in [4] to determine the relative discriminant $d(K/k)$ (see Lemma 2 below) and then appealing to the following theorem of Mann [6, Theorem 2].

THEOREM (MANN). *Let F be an algebraic number field and E a quadratic extension of F . Then E has a RIB over F if and only if $E = F(\sqrt{\Delta})$ for some $\Delta \in F$ with $d(E/F) = (\Delta)$.*

Our necessary and sufficient condition for K to have a RIB over k is given in terms of the fundamental unit $\varepsilon (> 1)$ of $k = Q(\sqrt{D})$. Two cases naturally arise according as the norm $N_{k/Q}(\varepsilon) = +1$ or -1 . First we prove

THEOREM 1. *If $N_{k/Q}(\varepsilon) = +1$ then K does not have a RIB over k .*

If $N_{k/Q}(\varepsilon) = -1$ we let (U, V) be the solution in positive integers of $U^2 - DV^2 = -1$ with V least. Setting $\varepsilon = (x + y\sqrt{D})/2$, where x and y are positive integers

Received by the editors January 1, 1987 and, in revised form, June 22, 1987.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 12A30; Secondary 12A50.

Key words and phrases. Cyclic quartic field, relative integral basis, relative different and discriminant.

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

with $x \equiv y \pmod{2}$, $x^2 - Dy^2 = -4$, we have

$$U + V\sqrt{D} = \begin{cases} \varepsilon, & \text{if } x \equiv y \equiv 0 \pmod{2}, \\ \varepsilon^3, & \text{if } x \equiv y \equiv 1 \pmod{2}. \end{cases}$$

We note that the case $x \equiv y \equiv 1 \pmod{2}$ can only occur when $D \equiv 5 \pmod{8}$. It is a classical result (see for example [7, Theorem 5.9]) that if $V > 1$ there is a unique pair of nonnegative coprime integers (S, T) such that

$$(2) \quad V = S^2 + T^2, \quad T \equiv SU \pmod{V}.$$

If $V = 1$ we take $S = 1, T = 0$ so that (2) is satisfied in this case too. A familiar argument shows that S and T satisfy the congruence

$$(S^2 - T^2) + 2STU \equiv 0 \pmod{V^2},$$

so that we may define nonnegative integers M and N by

$$M = \frac{|U(S^2 - T^2) - 2STU|}{V^2}, \quad N = \frac{|(S^2 - T^2) + (2ST)U|}{V^2}.$$

As $M^2 + N^2 = D$, and $D (> 1)$ is squarefree, M and N must be positive integers. Moreover we have

$$(3) \quad (U + V\sqrt{D})(X + Y\sqrt{D})^2 = (\pm M) + \sqrt{D},$$

where

$$X = (T - SU)/V, \quad Y = S.$$

We prove

THEOREM 2. *If $N_{k/Q}(\varepsilon) = -1$ then K has a RIB over k if and only if*

$$(B, C) = \begin{cases} (N, M), & \text{if } D \equiv 1 \pmod{4}, B \equiv 1 \pmod{2}, \\ (M, N), & \text{otherwise.} \end{cases}$$

It follows from Theorems 1 and 2 that if A and D are given integers such that

- A is squarefree and odd,
- $D (> 1)$ is squarefree and representable as the sum of two squares,
- $GCD(A, D) = 1,$

then either there are no pairs of positive integers (B, C) with $B^2 + C^2 = D$ for which $K = Q(\sqrt{A(D + B\sqrt{D})})$ has a RIB over k or there are one or two pairs according as $D \equiv 2 \pmod{8}$ or $D \equiv 1 \pmod{4}$.

EXAMPLE 1. $K = Q(\sqrt{5 + 2\sqrt{5}})$. Here $A = 1, B = 2, C = 1, D = 5,$
 $k = Q(\sqrt{5}), \varepsilon = (1 + \sqrt{5})/2, N_{k/Q}(\varepsilon) = -1, U = 2, V = 1, S = 1, T = 0, M = 2,$
 $N = 1,$ and so, by Theorem 2, K has a RIB over k .

EXAMPLE 2. $K = Q(\sqrt{10 + \sqrt{10}})$. Here $A = 1, B = 1, C = 3, D = 10,$
 $k = Q(\sqrt{10}), \varepsilon = 3 + \sqrt{10}, N_{k/Q}(\varepsilon) = -1, U = 3, V = 1, S = 1, T = 0, M = 3,$
 $N = 1,$ and so, by Theorem 2, K does not have a RIB over k .

In the case when K has a RIB over k we give an explicit relative integral basis for K/k .

THEOREM 3. *If K has a RIB over k then a RIB over K/k is given by*

$$\begin{aligned} & \left\{ 1, \sqrt{A\sqrt{D}(U + V\sqrt{D})} \right\}, \quad \text{if } D \equiv 2 \pmod{8} \text{ or } D \equiv 1 \pmod{4}, \\ & \qquad \qquad \qquad B \equiv 0 \pmod{2}, \quad A + B \equiv 3 \pmod{4}; \\ & \left\{ 1, \sqrt{2A\sqrt{D}(U + V\sqrt{D})} \right\}, \quad \text{if } D \equiv 1 \pmod{4}, \quad B \equiv 1 \pmod{2}; \\ & \left\{ 1, \frac{1}{2}(1 + \sqrt{A\sqrt{D}(U + V\sqrt{D})}) \right\}, \quad \text{if } D \equiv 1 \pmod{4}, \\ & \qquad \qquad \qquad B \equiv 0 \pmod{2}, \quad A + B \equiv 1 \pmod{4}. \end{aligned}$$

EXAMPLE 1 (CONT). Set $\alpha = \sqrt{5 + 2\sqrt{5}}$, $\beta = \sqrt{5 - 2\sqrt{5}}$, so that

$$\sqrt{5}\alpha = 2\alpha + \beta, \quad \sqrt{5}\beta = \alpha - 2\beta.$$

By Theorem 3 a RIB for $K = Q(\sqrt{5 + 2\sqrt{5}})$ over $k = Q(\sqrt{5})$ is given by $\{1, \alpha\}$. This is easily seen directly, as every integer of K is of the form (see [4])

$$\begin{aligned} & x + y \left(\frac{1 + \sqrt{5}}{2} \right) + z \left(\frac{\alpha + \beta}{2} \right) + w \left(\frac{\alpha - \beta}{2} \right) \\ & = \left(x + y \left(\frac{1 + \sqrt{5}}{2} \right) \right) 1 + \left((2w - z) + (z - w) \left(\frac{1 + \sqrt{5}}{2} \right) \right) \alpha, \end{aligned}$$

where x, y, z, w are integers.

EXAMPLE 2 (CONT). We show directly that $K = Q(\sqrt{10 + \sqrt{10}})$ does not possess a RIB over $k = Q(\sqrt{10})$. We set $\alpha = \sqrt{10 + \sqrt{10}}$, $\beta = \sqrt{10 - \sqrt{10}}$, so that

$$\sqrt{10}\alpha = \alpha + 3\beta, \quad \sqrt{10}\beta = 3\alpha - \beta.$$

The integers of K are of the form (see [4]) $x + y\sqrt{10} + z\alpha + w\beta$, where x, y, z, w are integers. Suppose that K has a relative integral basis over k . Such a basis may be taken in the form $\{1, \gamma\}$, where $\gamma = t\alpha + u\beta$ with integers t and u not both zero. Thus there must be integers a, b, c, d, e, f, g, h such that

$$\begin{aligned} \alpha &= (a + b\sqrt{10})1 + (c + d\sqrt{10})(t\alpha + u\beta), \\ \beta &= (e + f\sqrt{10})1 + (g + h\sqrt{10})(t\alpha + u\beta), \end{aligned}$$

and so we have

$$\begin{aligned} \alpha &= a + b\sqrt{10} + (tc + (t + 3u)d)\alpha + (uc + (3t - u)d)\beta, \\ \beta &= e + f\sqrt{10} + (tg + (t + 3u)h)\alpha + (ug + (3t - u)h)\beta. \end{aligned}$$

Equating coefficients of $1, \sqrt{10}, \alpha, \beta$, we obtain $a = b = e = f = 0$, and

$$\left\{ \begin{aligned} tc + (t + 3u)d &= 1 \\ uc + (3t - u)d &= 0 \end{aligned} \right\}, \quad \left\{ \begin{aligned} tg + (t + 3u)h &= 0 \\ ug + (3t - u)h &= 1 \end{aligned} \right\}.$$

Solving for c, d and g, h , we obtain

$$\begin{aligned} c &= \frac{3t - u}{3t^2 - 2tu - 3u^2}, & d &= \frac{-u}{3t^2 - 2tu - 3u^2}, \\ g &= \frac{-t - 3u}{3t^2 - 2tu - 3u^2}, & h &= \frac{t}{3t^2 - 2tu - 3u^2}. \end{aligned}$$

Note that $3t^2 - 2tu - 3u^2 \neq 0$ as t and u are not both zero. As c, d, g, h are integers, we must have

$$3t^2 - 2tu - 3u^2 \mid t, \quad 3t^2 - 2tu - 3u^2 \mid u.$$

Thus there are integers r and s such that

$$t = (3t^2 - 2tu - 3u^2)r, \quad u = (3t^2 - 2tu - 3u^2)s,$$

and so

$$3t^2 - 2tu - 3u^2 = (3t^2 - 2tu - 3u^2)^2(3r^2 - 2rs - 3s^2),$$

giving

$$(3t^2 - 2tu - 3u^2)(3r^2 - 2rs - 3s^2) = 1.$$

Hence we have

$$3t^2 - 2tu - 3u^2 = \pm 1,$$

and so

$$(3t - u)^2 - 10u^2 = \pm 3,$$

which is impossible as $x^2 \equiv \pm 3 \pmod{5}$ is insolvable.

We now begin the proofs of Theorems 1 and 2. We first calculate the relative different $\mathcal{D}(K/k)$. We set

$$\alpha = \sqrt{A(D + B\sqrt{D})}, \quad \beta = \sqrt{A(D - B\sqrt{D})}.$$

LEMMA 1.

$$\mathcal{D}(K/k) = \begin{cases} 2(\alpha, \beta), & \text{if } B \equiv 1 \pmod{2}, \\ (\alpha + \beta, \alpha - \beta), & \text{if } B \equiv 0 \pmod{2}, A + B \equiv 3 \pmod{4}, \\ \left(\frac{\alpha + \beta}{2}, \frac{\alpha - \beta}{2}\right), & \text{if } B \equiv 0 \pmod{2}, A + B \equiv 1 \pmod{4}. \end{cases}$$

PROOF. We just give the details in the case $D \equiv 2 \pmod{8}$ (so that $B \equiv C \equiv 1 \pmod{2}$) as the other cases can be treated similarly. We will obtain $\mathcal{D}(K/k)$ from the relation

$$(4) \quad \mathcal{D}(K/k)\mathcal{D}(k/Q) = \mathcal{D}(K/Q).$$

We first calculate $\mathcal{D}(K/Q)$. An integral basis for K/Q in this case is given by (see [4]) $\{1, \sqrt{D}, \alpha, \beta\}$. For convenience we set $\Omega_1 = 1, \Omega_2 = \sqrt{D}, \Omega_3 = \alpha, \Omega_4 = \beta$, and define ideals X_1, X_2, X_3 of the ring O_K of integers of K by

$$X_j = (\Omega_1 - \theta^j(\Omega_1), \Omega_2 - \theta^j(\Omega_2), \Omega_3 - \theta^j(\Omega_3), \Omega_4 - \theta^j(\Omega_4)),$$

where $\text{Gal}(K/Q) = \langle \theta \rangle$, so that $\mathcal{D}(K/Q) = X_1X_2X_3$. As $\theta(\alpha) = \beta, \theta(\beta) = -\alpha, \theta(\sqrt{D}) = -\sqrt{D}$, we have

$$X_1 = X_3 = (2\sqrt{D}, \alpha - \beta, \alpha + \beta) \quad \text{and} \quad X_2 = 2(\alpha, \beta).$$

Next, making use of

$$\alpha^2 = AD + AB\sqrt{D}, \quad \beta^2 = AD - AB\sqrt{D}, \quad \alpha\beta = AC\sqrt{D},$$

we obtain

$$\begin{aligned} X_1X_3 &= (4D, (\alpha - \beta)^2, (\alpha + \beta)^2, 2\sqrt{D}(\alpha - \beta), 2\sqrt{D}(\alpha + \beta), \alpha^2 - \beta^2) \\ &= 2\sqrt{D}I, \end{aligned}$$

where

$$I = (2\sqrt{D}, AC + A\sqrt{D}, AC - A\sqrt{D}, \alpha - \beta, \alpha + \beta, AB).$$

Now $2D \in I$, $AB \in I$, so as $(A, D) = 1$, $(B, D) = 1$, $A \equiv B \equiv 1 \pmod{2}$, we have $(2D, AB) = (1)$, so that $I = (1)$, and $X_1X_3 = (2\sqrt{D})$. Hence we have

$$(5) \quad \mathcal{D}(K/Q) = (2)^2(\sqrt{D})(\alpha, \beta).$$

Next we calculate $\mathcal{D}(k/Q)$. An integral basis for k in this case is $\{1, \sqrt{D}\}$ and, by the definition of the different, we have

$$\mathcal{D}(k/Q) = (1 - \theta(1), \sqrt{D} - \theta(\sqrt{D}))$$

so that

$$(6) \quad \mathcal{D}(k/Q) = (2\sqrt{D}).$$

Thus, from (4), (5), (6), we obtain

$$\mathcal{D}(K/k) = \frac{(2)^2(\sqrt{D})(\alpha, \beta)}{(2)(\sqrt{D})} = (2)(\alpha, \beta).$$

This completes the proof of Lemma 1 in this case.

Next we determine the relative discriminant $d(K/k)$.

LEMMA 2.

$$d(K/k) = \begin{cases} (2^3A\sqrt{D}), & \text{if } D \equiv 1 \pmod{4}, B \equiv 1 \pmod{2}, \\ (2^2A\sqrt{D}), & \text{if } D \equiv 2 \pmod{8}, \text{ or} \\ & D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 3 \pmod{4}, \\ (A\sqrt{D}), & \text{if } D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 1 \pmod{4}. \end{cases}$$

PROOF. We just give the details when $D \equiv 2 \pmod{8}$, as the other cases can be treated similarly. We have (appealing to Lemma 1)

$$\begin{aligned} d(K/k) &= N_{K/k}(\mathcal{D}(K/k)) = (2)(\alpha, \beta)(2)(\beta, -\alpha) = (2)^2(\alpha, \beta)^2 \\ &= (2)^2(\alpha^2, \alpha\beta, \beta^2) = (2)^2(AD + AB\sqrt{D}, AC\sqrt{D}, AD - AB\sqrt{D}) \\ &= (2^2A\sqrt{D})(\sqrt{D} + B, \sqrt{D} - B, C). \end{aligned}$$

Now, as $(2B, C) = 1$, we see that $(\sqrt{D} + B, \sqrt{D} - B, C) = (1)$, and so

$$d(K/k) = (2^2A\sqrt{D})$$

as required.

PROOF OF THEOREM 1. Suppose $N_{k/Q}(\varepsilon) = +1$ and K has a RIB over k . Then, by Lemma 2 and Mann's theorem, there exists $\Delta \in O_k$ such that $K = Q(\sqrt{\Delta})$, and $(\Delta) = (2^j A\sqrt{D})$, where

$$j = \begin{cases} 3, & \text{if } D \equiv 1 \pmod{4}, B \equiv 1 \pmod{2}, \\ 2, & \text{if } D \equiv 2 \pmod{8}, \text{ or} \\ & \text{if } D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 3 \pmod{4}, \\ 0, & \text{if } D \equiv 1 \pmod{4}, B \equiv 0 \pmod{2}, A + B \equiv 1 \pmod{4}. \end{cases}$$

Hence there is a unit $\eta \in O_k$ such that

$$\Delta = 2^j A\sqrt{D}\eta.$$

By Dirichlet’s unit theorem we have

$$\eta = \pm \varepsilon^m, \quad \text{for some integer } m,$$

and so

$$Q(\sqrt{A(D + B\sqrt{D})}) = Q(\sqrt{\pm 2^j A\sqrt{D}\varepsilon^m}).$$

Removing squares from under the radical sign on the right-hand side as appropriate and recalling that $Q(\sqrt{A(D + B\sqrt{D})})$ is a cyclic field, we see that

$$Q(\sqrt{A(D + B\sqrt{D})}) = Q(\sqrt{\pm 2^l A\sqrt{D}\varepsilon}),$$

where $l = 0, 1$. Moreover, as $Q(\sqrt{A(D + B\sqrt{D})})$ and $Q(\sqrt{\pm 2^l A\sqrt{D}\varepsilon})$ must both be totally real or both totally imaginary, we have

$$Q(\sqrt{A(D + B\sqrt{D})}) = Q(\sqrt{2^l A\sqrt{D}\varepsilon}).$$

Hence there exist $\alpha, \beta \in k$ such that

$$(7) \quad \sqrt{2^l A\sqrt{D}\varepsilon} = \alpha + \beta\sqrt{A(D + B\sqrt{D})}.$$

From (7) we see that

$$\sqrt{2^l A\sqrt{D}\varepsilon}\sqrt{A(D + B\sqrt{D})} = \frac{1}{2\beta}(2^l A\sqrt{D}\varepsilon + \beta^2 A(D + B\sqrt{D}) - \alpha^2) \in Q(\sqrt{D}).$$

Hence there exist rational numbers e and f such that

$$(8) \quad \sqrt{2^l A\sqrt{D}\varepsilon}\sqrt{A(D + B\sqrt{D})} = e + f\sqrt{D}.$$

Squaring (8) and taking norms, we obtain

$$2^{2l} A^2 (-D) A^2 D C^2 = (e^2 - D f^2)^2,$$

which is impossible. This completes the proof of Theorem 1.

LEMMA 3. *If $N_{k/Q}(\varepsilon) = -1$ then K has a RIB over k if and only if*

$$K = \begin{cases} Q(\sqrt{2A\sqrt{D}(U + V\sqrt{D})}), & \text{if } D \equiv 1 \pmod{4}, B \equiv 1 \pmod{2}, \\ Q(\sqrt{A\sqrt{D}(U + V\sqrt{D})}), & \text{otherwise.} \end{cases}$$

PROOF. We just treat the case $D \equiv 1 \pmod{4}, B \equiv 1 \pmod{2}$, as the other cases can be treated similarly. By Lemma 2 and Mann’s theorem, K has a RIB over k if and only if

$$(9) \quad K = Q(\sqrt{2^3 A\sqrt{D}\lambda}),$$

for some positive unit λ in O_k . The unit λ must be positive for if λ were negative $Q(\sqrt{A(D + B\sqrt{D})})$ and $Q(\sqrt{2^3 A\sqrt{D}\lambda})$ could not both be totally real or both totally imaginary. By Dirichlet’s unit theorem, we have $\lambda = \varepsilon^m$ for some integer m . Recalling that $U + V\sqrt{D} = \varepsilon$ or ε^3 and removing squares from under the radical sign in (9) we see that K has a RIB over k if and only if

$$K = Q(\sqrt{2A\sqrt{D}(U + V\sqrt{D})^j}),$$

where $j = 0$ or 1 . As K is cyclic we must have $j = 1$. This completes the proof of Lemma 3 in this case.

LEMMA 4. *If $N_{k/Q}(\varepsilon) = -1$, then we have*

$$Q(\sqrt{2A\sqrt{D}(U + V\sqrt{D})}) = Q(\sqrt{A(D + N\sqrt{D})}),$$

$$Q(\sqrt{A\sqrt{D}(U + V\sqrt{D})}) = Q(\sqrt{A(D + M\sqrt{D})}).$$

PROOF. This is clear from (3) and the fact

$$Q(\sqrt{2A\sqrt{D}(M + \sqrt{D})}) = Q(\sqrt{A\sqrt{D}(N + \sqrt{D})}).$$

PROOF OF THEOREM 2. Theorem 2 follows immediately from Lemmas 3 and 4 as the representation of K in the form (1) is unique.

PROOF OF THEOREM 3. In each case it is a simple matter to check that the given set of elements has discriminant equal to $d(K/k)$ (the value of which is given in Lemma 2). Appealing to Theorem 2 and Lemma 4, it is easy to check that in each case the elements lie in K . The only element which is not obviously an algebraic integer is

$$\gamma = \frac{1}{2}(1 + \sqrt{A\sqrt{D}(U + V\sqrt{D})}).$$

Since γ satisfies

$$\gamma^2 - \gamma + \frac{1}{4}(1 - AVD - AU\sqrt{D}) = 0$$

it suffices to show that $\frac{1}{4}(1 - AVD - AU\sqrt{D})$ is an integer of k . Since $D \equiv 1 \pmod{4}$ (in this case) and $U^2 - V^2D = -1$, we have $U \equiv 0 \pmod{2}$ and $V \equiv 1 \pmod{2}$. Moreover we have $V \equiv 1 \pmod{4}$ as $U^2 \equiv -1 \pmod{V}$. Hence $1 - AVD$ and AU are both even, and so, it suffices to show that

$$1 - AVD \equiv -AU \pmod{4},$$

or equivalently

$$A(VD - U) \equiv 1 \pmod{4}.$$

We consider two cases according as $U \equiv 0 \pmod{4}$ or $U \equiv 2 \pmod{4}$. If $U \equiv 0 \pmod{4}$ then, from $U^2 - V^2D = -1$, we deduce that $V^2D \equiv 1 \pmod{8}$, so that $D \equiv 1 \pmod{8}$, and thus $B \equiv 0 \pmod{4}$. Hence, as $A + B \equiv 1 \pmod{4}$ (in this case), we obtain $A \equiv 1 \pmod{4}$, giving $A(VD - U) \equiv 1 \pmod{4}$. If $U \equiv 2 \pmod{4}$ then as above we conclude $D \equiv 5 \pmod{8}$, $B \equiv 2 \pmod{4}$, $A \equiv 3 \pmod{4}$ and $A(VD - U) \equiv 1 \pmod{4}$. This completes the proof of Theorem 3.

We conclude by remarking that Xianke [8] has given a less explicit form of Theorems 1, 2, 3. Relative integral bases for bicyclic quartic fields over their quadratic subfields are considered in [1, 2 and 5].

REFERENCES

1. R. H. Bird and C. J. Parry, *Integral bases for bicyclic biquadratic fields over quadratic subfields*, Pacific J. Math. **66** (1976), 29-36.
2. H. M. Edgar, *A number field without any integral basis*, Math. Mag. **52** (1979), 248-251.
3. K. Hardy, R. H. 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, no. 7, 1986.
4. R. H. Hudson and K. S. Williams, *The integers of a cyclic quartic field*, Rocky Mountain J. Math. (to appear).

5. R. MacKenzie and J. Scheuneman, *A number field without a relative integral bases*, Amer. Math. Monthly **78** (1971), 882–883.
6. H. B. Mann, *On integral bases*, Proc. Amer. Math. Soc. **9** (1958), 167–172.
7. I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, 2nd ed., Wiley, 1968.
8. Zhang Xianke, *Cyclic quartic fields and genus theory of their subfields*, J. Number Theory **18** (1984), 350–355.

DEPARTMENT OF MATHEMATICS, OKANAGAN COLLEGE, VERNON, BRITISH COLUMBIA,
CANADA V1T 5R4

DEPARTMENT OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA,
ONTARIO, CANADA K1S 5B6