JOURNAL OF NUMBER THEORY 23, 169–182 (1986)

Pell's Equations $X^2 - mY^2 = -1, -4$ and Continued Fractions

PIERRE KAPLAN

10 Allée Jacques Offenbach,
54420 Saulxures les Nancy, France

AND

KENNETH S. WILLIAMS*

Department of Mathematics and Statistics,
Carleton University, Ottawa, Ontario, Canada K1S 5B6

Communicated by P. Roquette

Received July 19, 1983; revised June 25, 1984

Let m denote a positive nonsquare integer. It is shown that if Pell's equation $X^2 - mY^2 = -1$ is solvable in integers X and Y then the equation $X^2 - mY^2 = -4$ is solvable in *coprime* integers X and Y if and only if $l(\sqrt{m}) \equiv l(\frac{1}{2}(1+\sqrt{m}))$ (mod 4), where $l(\alpha)$ denotes the length of the period of the continued fraction expansion of the quadratic irrational α.

1. INTRODUCTION

Let m denote a positive nonsquare integer. In the eighteenth century, Lagrange used the continued fraction expansion of $\sqrt{m}$ to give the first complete proof that Pell's equation $x^2 - my^2 = 1$ is always solvable in integers x and y with $y \neq 0$ (see, e.g., [1, p. 358]). Later for the equation

$$x^2 - my^2 = -1 \tag{1.1}$$

the following necessary and sufficient condition for solvability was proved:

$$x^2 - my^2 = -1 \text{ is solvable in integers } x \text{ and } y \text{ if and only if } l(\sqrt{m}) \equiv 1 \pmod 2, \tag{1.2}$$

* Research supported by Natural Sciences and Engineering Research Council Canada Grant A-7233 and the University of Nancy I.

0022-314X/86 $3.00

where $l(\alpha)$ denotes the length of the period of the continued fraction expansion of the quadratic irrational α (see, e.g., [3, Satz 3.18]). (A real irrational number is called a quadratic irrational if it is the root of a quadratic equation with rational coefficients.)

In this paper we shall be concerned with the solvability of the equation

$$X^2 - mY^2 = -4, \qquad (X, Y) = 1. \tag{1.3}$$

We note that if either (1.1) or (1.3) is solvable, m is not divisible by any prime $\equiv -1 \pmod 4$.

Simple congruence arguments show that, if (1.3) is solvable, then either $m \equiv 4$ or $8 \pmod{16}$ or $m \equiv 5 \pmod 8$, and that if (1.1) is solvable then $m \equiv 1$ or $2 \pmod 4$. Thus, when m is even, (1.1) and (1.3) are never simultaneously solvable. Furthermore a straightforward application of (1.2) shows that, if $m \equiv 4$ or $8 \pmod{16}$, (1.3) is solvable if and only if $l(\sqrt{m/4}) \equiv 1 \pmod 2$. Thus we need consider only the case $m \equiv 5 \pmod 8$. The following lemma is easily proved.

LEMMA 1. *Let $m \equiv 5 \pmod 8$ be such that (1.3) is solvable and let (U, V) be the smallest positive solution. Then the relation*

$$u + v\sqrt{m} = (\tfrac{1}{2}(U + V\sqrt{m}))^3$$

defines integers u and v such that (u, v) is the smallest positive solution of (1.1). The solutions (x, y) of (1.1) are given by

$$x + y\sqrt{m} = \pm(\tfrac{1}{2}(U + V\sqrt{m}))^r, \qquad r \equiv 3 \pmod 6,$$

and the solutions X, Y of (1.3) by

$$\tfrac{1}{2}(X + Y\sqrt{m}) = \pm(\tfrac{1}{2}(U + V\sqrt{m}))^r, \qquad r \equiv \pm 1 \pmod 6.$$

However, the solvability of (1.1) does not guarantee that (1.3) is solvable as the example $m = 37$ shows.

Before stating the main result we recall that if $m \equiv 1 \pmod 4$ then $l(\sqrt{m}) \equiv l(\tfrac{1}{2}(1 + \sqrt{m})) \pmod 2$. This congruence can be proved as follows:

$l(\tfrac{1}{2}(1 + \sqrt{m})) \equiv 1 \pmod 2$

$\Leftrightarrow$ $x^2 - xy - \tfrac{1}{4}(m-1)y^2 = -1$ is solvable in integers x and y (see, e.g., [3, Satz 3.35])

$\Leftrightarrow$ $(2x - y)^2 - my^2 = -4$ solvable in integers x and y

$\Leftrightarrow$ $N(\tfrac{1}{2}(2x - y + y\sqrt{m})) = -1$ solvable in integers x and y

$\Leftrightarrow$ N (fund. unit of $Q(\sqrt{m})) = -1$

$\Leftrightarrow$ $x^2 - my^2 = -1$ solvable in integers x and y

$\Leftrightarrow$ $l(\sqrt{m}) \equiv 1 \pmod 2$

(see, e.g., [3, Satz 3.18]).

In Section 3 we prove

THEOREM 1. *Let* $m \equiv 1 \pmod 4$ *be a positive nonsquare integer such that* (1.1) *is solvable. Then* (1.3) *is solvable if and only if* $l(\sqrt{m}) \equiv l(\frac{1}{2}(1+\sqrt{m})) \pmod 4$.

As (1.3) is not solvable for $m \equiv 1 \pmod 8$ we have

COROLLARY. *If* $m \equiv 1 \pmod 8$ *is such that* (1.1) *is solvable then*

$$l(\sqrt{m}) \equiv l(\tfrac{1}{2}(1+\sqrt{m})) + 2 \pmod 4.$$

2. NOTATION AND TWO LEMMAS

Throughout the paper the following notation will be used. If m is a positive nonsquare integer for which $l(\sqrt{m}) \equiv 1 \pmod 2$, say $l(\sqrt{m}) = 2\lambda + 1$, then the continued fraction expansion of $\sqrt{m}$ takes the form (see, e.g., [3, Satz 3.9])

$$\sqrt{m} = [A_0, \overline{A_1, \ldots, A_\lambda, A_\lambda, \ldots, A_1, 2A_0}]. \tag{2.1}$$

Moreover, if $m \equiv 1 \pmod 4$ then $l(\frac{1}{2}(1+\sqrt{m})) \equiv 1 \pmod 2$, say $l(\frac{1}{2}(1+\sqrt{m})) = 2\mu + 1$, and the continued fraction expansion of $\frac{1}{2}(1+\sqrt{m})$ takes the form (see, e.g., [3, Satz 3.30])

$$\tfrac{1}{2}(1+\sqrt{m}) = [B_0, \overline{B_1, \ldots, B_\mu, B_\mu, \ldots, B_1, 2B_0 - 1}]. \tag{2.2}$$

We now prove the following two lemmas which are needed for the proof of Theorem 1.

LEMMA 2. *Let* m *be a positive nonsquare integer such that* $l(\sqrt{m}) \equiv 1 \pmod 2$. *Then there exists exactly one pair of positive integers* (a, b) *with* $m = a^2 + b^2$, $(a, 2b) = 1$, *such that the binary quadratic form* $[a, 2b, -a] = ar^2 + 2brs - as^2$ *lies in the principal class of the group under composition of equivalence classes of primitive binary quadratic forms of discriminant* $4m$. *Moreover, we have*

$$\frac{b+\sqrt{m}}{a} = [\overline{A_\lambda, \ldots, A_1, 2A_0, A_1, \ldots, A_\lambda}]. \tag{2.3}$$

In addition, if $m \equiv 1 \pmod 4$, *we have*

$$\frac{a+\sqrt{m}}{b} = [\overline{B_\mu, \ldots, B_1, 2B_0 - 1, B_1, \ldots, B_\mu}]. \tag{2.4}$$

Proof. For $k = 0, 1, 2, \ldots$, we set

$$[A_k, A_{k+1}, \ldots,] = \frac{P_k + \sqrt{m}}{Q_k},$$

so that P_k and Q_k are integers with

$$P_0 = 0, \qquad Q_0 = 1, \qquad P_k > 0 (k \geqslant 1), \qquad Q_k > 0 (k \geqslant 1),$$

see, for example, [3, Sect. 20]. Next, we set

$$a = Q_{\lambda+1}, \qquad b = P_{\lambda+1},$$

so that a and b are positive integers such that

$$m = a^2 + b^2, \qquad (a, 2b) = 1,$$

see, e.g., [3, Satz 3.12]). Thus we have

$$\frac{b + \sqrt{m}}{a} = [A_{\lambda+1}, A_{\lambda+2}, \ldots,],$$

and so as $A_i = A_{2\lambda+1-i}$ $(1 \leqslant i \leqslant \lambda)$ we obtain

$$\frac{b + \sqrt{m}}{a} = [\overline{A_\lambda, A_{\lambda-1}, \ldots, A_1, 2A_0, A_1, \ldots, A_\lambda}].$$

Hence there exist integers A, B, C, D with $AD - BC = \pm 1$ such that

$$\frac{b + \sqrt{m}}{a} = \frac{A\sqrt{m} + B}{C\sqrt{m} + D}.$$

If $AD - BC = -1$ we set

$$A' = TA + UB, B' = TB + mUA, C' = TC + UD, D' = TD + mUC,$$

where T and U are integers such that $T^2 - mU^2 = -1$. (Such integers T and U exist as $l(\sqrt{m}) \equiv 1 \pmod 2$.) Then we have

$$A'D' - B'C' = 1$$

and

$$\frac{A'\sqrt{m} + B'}{C'\sqrt{m} + D'} = \frac{A\sqrt{m} + B}{C\sqrt{m} + D}.$$

Hence, without loss of generality, we may assume that $AD-BC=1$. Equating coefficients in $(b+\sqrt{m})/a=(A\sqrt{m}+B)/C\sqrt{m}+D)$, we obtain

$$aA=bC+D,\ aB=mC+bD,$$

so that (as $m=a^2+b^2$)

$$\begin{cases} a=D^2-mC^2=mA^2-B^2, \\ b=BD-mAC, \end{cases}$$

giving

$$ar^2+2brs-as^2=(Dr+Bs)^2-m(Cr+As)^2$$

which shows that the form $[a, 2b, -a]$ is equivalent to $[1, 0, -m]$. Hence the form $[a, 2b, -a]$ lies in the unit (principal) class of the group under composition of equivalence classes of primitive binary quadratic forms of discriminant $4m$.

Now suppose there exists another pair of positive integers (a_1, b_1) with

$$m=a_1^2+b_1^2, \qquad (a_1, 2b_1)=1,$$

such that $[a_1, 2b_1, -a_1]$ lies in the principal class of forms of discriminant $4m$. Then $[a_1, 2b_1, -a_1]$ is equivalent to $[1, 0, -m]$, and so there exist integers A, B, C, D such that $AD-BC=1$ and

$$a_1r^2+2b_1rs-a_1s^2=(Ar+Bs)^2-m(Cr+Ds)^2.$$

Hence we have

$$\begin{cases} a_1=A^2-mC^2=-(B^2-mD^2), \\ b_1=AB-mCD, \end{cases}$$

and so

$$\frac{b_1+\sqrt{m}}{a_1}=\frac{D\sqrt{m}+B}{C\sqrt{m}+A}.$$

This shows that $(b_1+\sqrt{m})/a_1$ and $\sqrt{m}$ are equivalent. As $(b_1+\sqrt{m})/a_1$ is reduced (see [3, p. 73]) we must have [3, Satz 2.24],

$$\frac{b_1+\sqrt{m}}{a_1}=[A_i, A_{i+1},\ldots,] \qquad \text{for some } i\geqslant 1,$$

that is,

$$a_1=Q_i, \qquad b_1=P_i,$$

for some $i \geqslant 1$. Since

$$P_i^2 + Q_i^2 = m \qquad (0 \leqslant i \leqslant 2\lambda + 1)$$

if and only if $i = \lambda + 1$ (see [3, Satz 3.11]) we must have

$$a_1 = Q_{\lambda+1} = a, \qquad b_1 = P_{\lambda+1} = b,$$

establishing the uniqueness of a and b.

If $m \equiv 1 \pmod 4$ then $(a + \sqrt{m})/b$ is a reduced quadratic irrationality corresponding to the form $[b/2,\ a,\ -b/2]$ of discriminant m. As $[a,\ 2b,\ -a]$ represents 1 so does the form $[b/2,\ a,\ -b/2]$. Hence the form $[b/2,\ a,\ -b/2]$ lies in the principal class of forms of discriminant m and so we have

$$\frac{a+\sqrt{m}}{b} = [B_i,\ B_{i+1}, \ldots,] \qquad \text{for some} \quad i \geqslant 1.$$

Proceeding as in the argument given above, we deduce that $i = \mu$. This completes the proof of (2.4).

LEMMA 3. *Let m be a positive nonsquare integer such that $l(\sqrt{m}) \equiv 1 \pmod 2$, say $l(\sqrt{m}) = 2\lambda + 1$. Let t, u be the smallest solution of $t^2 - mu^2 = -1$ in positive integers. Let the integers a, b be as given in Lemma 2. Then there exist integers α and γ such that*

$$t = 2a\alpha\gamma + b(\alpha^2 - \gamma^2), \tag{2.5}$$

$$u = \alpha^2 + \gamma^2, \tag{2.6}$$

$$(-1)^\lambda = a(\alpha^2 - \gamma^2) - 2b\alpha\gamma, \tag{2.7}$$

and

$$(-1)^\lambda a + tb = m(\alpha^2 - \gamma^2). \tag{2.8}$$

If $m \equiv 1 \pmod 4$ we let T, U be the smallest solution of $T^2 - mU^2 = -4$ in positive integers, so that either $T \equiv U \equiv 0 \pmod 2$ or $T \equiv U \equiv 1 \pmod 2$. Then there exist integers α' and γ' such that

$$T = a(\alpha'^2 - \gamma'^2) + 2b\alpha'\gamma', \tag{2.9}$$

$$U = \alpha'^2 + \gamma'^2, \tag{2.10}$$

$$(-1)^\mu = -a\alpha'\gamma' + \frac{b}{2}(\alpha'^2 - \gamma'^2), \tag{2.11}$$

and

$$Ta + 2(-1)^\mu b = m(\alpha'^2 - \gamma'^2). \tag{2.12}$$

Proof. From (2.1) we have

$$\frac{1}{\sqrt{m}-A_0} = [\overline{A_1,\ldots, A_\lambda, A_\lambda,\ldots, A_1, 2A_0}].$$

As $1/(\sqrt{m}-A_0)$ is a root of $(m-A_0^2)\,x^2-2A_0x-1$ we have, appealing to [2, Satz 114] and [3, Sect. 5],

$$\begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} A_\lambda & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} A_\lambda & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2A_0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} t+A_0u & u \\ (m-A_0^2)\,u & t-A_0u \end{pmatrix}. \tag{2.13}$$

Further, as $(b+\sqrt{m})/a$ is a root of $ax^2-2bx-a$, we have by (2.3)

$$\begin{pmatrix} A_\lambda & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2A_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} A_\lambda & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} t+bu & au \\ au & t-bu \end{pmatrix}. \tag{2.14}$$

Setting

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} A_\lambda & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.15}$$

we obtain from (2.13), (2.14), and (2.15)

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 2A_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} t+A_0u & u \\ (m-A_0^2)\,u & t-A_0u \end{pmatrix} \tag{2.16}$$

and

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 2A_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \begin{pmatrix} t+bu & au \\ au & t-bu \end{pmatrix}. \tag{2.17}$$

Equating appropriate entries in (2.16) and (2.17), we obtain

$$u = \alpha^2+\gamma^2 \tag{2.18}$$
$$t+bu = 2A_0\alpha^2+2\alpha\beta, \tag{2.19}$$
$$t-bu = 2A_0\gamma^2+2\gamma\delta, \tag{2.20}$$
$$au = 2A_0\alpha\gamma+\alpha\delta+\beta\gamma. \tag{2.21}$$

Equation (2.18) is the required equation (2.6). Setting

$$X = A_0\alpha + \beta, \qquad Y = A_0\gamma + \delta, \tag{2.22}$$

from (2.19), (2.20), and (2.21), we obtain

$$t = \alpha X + \gamma Y, \tag{2.23}$$

$$au = \gamma X + \alpha Y, \qquad bu = \alpha X - \gamma Y. \tag{2.24}$$

Solving the equations in (2.24) for X and Y, and making use of (2.18), we obtain

$$X = a\gamma + b\alpha, \qquad Y = a\alpha - b\gamma. \tag{2.25}$$

Substituting these values for X and Y in (2.23), we obtain

$$t = 2a\alpha\gamma + b(\alpha^2 - \gamma^2),$$

which is the required equation (2.5).

Further, taking determinants in (2.15), we have

$$\alpha\delta - \beta\gamma = (-1)^\lambda. \tag{2.26}$$

Appealing to (2.22) we obtain

$$\alpha Y - \gamma X = (-1)^\lambda, \tag{2.27}$$

which becomes by (2.25)

$$(-1)^\lambda = a(\alpha^2 - \gamma^2) - 2b\alpha\gamma,$$

which is the required equation (2.7).

Equation (2.8) follows easily from (2.5) and (2.7).

We now consider the case $m \equiv 1 \pmod 4$. Similarly to above we have

$$\begin{pmatrix} B_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_\mu & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_\mu & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2B_0 - 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{2}(T + (2B_0 - 1)\,U) & U \\ \frac{1}{4}(m - (2B_0 - 1)^2)\,U & \frac{1}{2}(T - (2B_0 - 1)\,U) \end{pmatrix} \tag{2.28}$$

and

$$\begin{pmatrix} B_\mu & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2B_0 - 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_\mu & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{2}(T + aU) & \frac{1}{2}bU \\ \frac{1}{2}bU & \frac{1}{2}(T - aU) \end{pmatrix}. \tag{2.29}$$

Setting

$$\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} B_\mu & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_1 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.30}$$

we obtain, from (2.28), (2.29) and (2.30),

$$\begin{pmatrix} \alpha' & \gamma' \\ \beta' & \delta' \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \begin{pmatrix} 2B_0 - 1 & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} \frac{1}{2}(T + (2B_0 - 1)\,U) & U \\ \frac{1}{4}(m - (2B_0 - 1)^2\,U & \frac{1}{2}(T - (2B_0 - 1)\,U) \end{pmatrix} \tag{2.31}$$

and

$$\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \begin{pmatrix} 2B_0 - 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha' & \gamma' \\ \beta' & \delta' \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(T + aU) & \frac{1}{2}bU \\ \frac{1}{2}bU & \frac{1}{2}(T - aU) \end{pmatrix}. \tag{2.32}$$

Equating appropriate entries in (2.31) and (2.32) we obtain

$$U = \alpha'^2 + \gamma'^2, \tag{2,33}$$
$$T + aU = 2\alpha'^2(2B_0 - 1) + 4\alpha'\beta', \tag{2.34}$$
$$T - aU = 2\gamma'^2(2B_0 - 1) + 4\gamma'\delta', \tag{2.35}$$
$$bU = 2\alpha'\gamma'(2B_0 - 1) + 2\alpha'\delta' + 2\beta'\gamma'. \tag{2.36}$$

Equation (2.33) is the required equation (2.10). Setting

$$G = \alpha'(2B_0 - 1) + 2\beta', \qquad H = \gamma'(2B_0 - 1) + 2\delta', \tag{2.37}$$

from (2.34), (2.35), (2.36) and (2.37), we obtain

$$T = \alpha' G + \gamma' H, \tag{2.38}$$
$$aU = \alpha' G - \gamma' H, \qquad bU = \gamma' G + \alpha' H. \tag{2.39}$$

Solving the equations in (2.39) for G and H, and making use of (2.33), we obtain

$$G = a\alpha' + b\gamma', \qquad H = -a\gamma' + b\alpha'. \tag{2.40}$$

Substituting these values of G and H into (2.38), we obtain

$$T = a(\alpha'^2 - \delta'^2) + 2b\alpha'\gamma',$$

which is the required equation (2.9). Taking determinants in (2.30), we have

$$\alpha'\delta' - \beta'\gamma' = (-1)^{\mu}. \tag{2.41}$$

Appealing to (2.37) we obtain

$$2(-1)^{\mu} = \alpha' H - \gamma' G,$$

which becomes, by (2.40),

$$2(-1)^{\mu} = -2a\alpha'\gamma' + b(\alpha'^2 - \gamma'^2),$$

from which (2.11) follows. Equation (2.12) follows easily from (2.9) and (2.11). This completes the proof of Lemma 3.

3. Proof of Theorem 1

By Lemma 3 we have

$$t \equiv (-1)^{\lambda+1} ab^{-1} \pmod{m}, \quad T \equiv 2(-1)^{\mu+1} a^{-1} b \pmod{m}. \tag{3.1}$$

If (1.3) is insolvable we have $T = 2t$ so that

$$2(-1)^{\lambda+1} ab^{-1} \equiv 2(-1)^{\mu+1} a^{-1} b \pmod{m},$$

which gives, as $(ab^{-1})^2 \equiv -1 \pmod{m}$, $\lambda \equiv \mu + 1 \pmod 2$, that is

$$l(\sqrt{m}) \equiv l(\tfrac{1}{2}(1 + \sqrt{m})) + 2 \pmod 4.$$

If, on the other hand, (1.3) is solvable then $T \equiv U \equiv 1 \pmod 2$ and by Lemma 1 we have $t + u\sqrt{m} = (\tfrac{1}{2}(T + U\sqrt{m}))^3$ so that

$$8t = T^3 + 3mTU^2 \equiv T^3 \pmod{m}.$$

Hence we have

$$8(-1)^{\lambda+1} ab^{-1} \equiv 8(-1)^{\mu+1} a^{-3} b^3 \pmod{m},$$

which implies, as $(ab^{-1})^4 \equiv 1 \pmod{m}$, $\lambda \equiv \mu \pmod 2$, that is,

$$l(\sqrt{m}) \equiv l(\tfrac{1}{2}(1 + \sqrt{m})) \pmod 4.$$

This completes the proof of Theorem 1.

4. Congruences Modulo 4 for $l(\sqrt{m})$ and $l(\frac{1}{2}(1+\sqrt{m}))$ when $m \equiv 5 \pmod 8$

In this section we prove congruences modulo 4 for $l(\sqrt{m})$ and $l(\frac{1}{2}(1+\sqrt{m}))$ when $m \equiv 5 \pmod 8$.

Theorem 2. *If $m \equiv 5 \pmod 8$ and $l(\sqrt{m}) \equiv 1 \pmod 2$ then we have*

$$l(\sqrt{m}) \equiv \tfrac{1}{4}(abt + m - 5) \pmod 4, \tag{4.1}$$

and

$$l(\tfrac{1}{2}(1+\sqrt{m})) \equiv \begin{cases} \tfrac{1}{8}(abT + 2m + 6) \pmod 4, \\ \qquad \text{if} \quad T \equiv U \equiv 0 \pmod 2, \\ \tfrac{1}{8}(ab(T^3 + 3T) + 2m - 10) \pmod 4 \\ \qquad \text{if} \quad T \equiv U \equiv 1 \pmod 2, \end{cases} \tag{4.2}$$

where a, b are given by Lemma 2; and T, U, t, u are as defined in Lemma 3.

Proof. As $m \equiv 5 \pmod 8$ it is easy to see from $t^2 - mu^2 = -1$ that

$$t \equiv 2 \pmod 4, \qquad u \equiv 1 \pmod 4. \tag{4.3}$$

Hence we have

$$t^2 \equiv 4 \pmod{16}, \qquad u^2 \equiv 2u - 1 \pmod{16}, \qquad mu \equiv m - u + 9 \pmod{16}.$$

Using these congruences in $t^2 - mu^2 = -1$ we obtain

$$m \equiv 2u + 3 \pmod{16}$$

so that

$$\tfrac{1}{2}(u-1) \equiv \tfrac{1}{4}(m-5) \pmod 4. \tag{4.4}$$

From (2.6), we see, as u is odd, that exactly one of α and γ is odd and the other is even. As $b \equiv 2 \pmod 4$, (2.7) gives

$$(-1)^{\lambda} \equiv a(\alpha^2 - \gamma^2) \pmod 8,$$

that is,

$$\alpha^2 - \gamma^2 \equiv (-1)^{\lambda} a \pmod 8.$$

Further, appealing to (2.6), we have

$$2\alpha\gamma = (\alpha+\gamma)^2 - (\alpha^2 + \gamma^2) \equiv 1 - u \pmod 8,$$

so that (2.5) gives

$$t \equiv a(1-u) + ab(-1)^{\lambda} \pmod 8.$$

Hence, we have by (4.4),

$$a\frac{t}{2} \equiv -\frac{1}{4}(m-5) + \frac{b}{2}(-1)^{\lambda} \pmod 4,$$

giving

$$(-1)^{\lambda} \equiv \left(\frac{at}{2} + \frac{m-5}{4}\right)\frac{b}{2} \pmod 4,$$

that is,

$$l(\sqrt{m}) = 2\lambda + 1 \equiv (-1)^{\lambda} \equiv \tfrac{1}{4}(abt + m - 5) \pmod 4$$

as required. This completes the proof of (4.1).

In order to prove (4.2) we consider two cases.

Case i. $T \equiv U \equiv 1 \pmod 2$.

In this case, by Theorem 1, we have

$$l(\tfrac{1}{2}(1+\sqrt{m})) \equiv l(\sqrt{m}) + 2 \pmod 4.$$

Appealing to (4.1) we obtain

$$l(\tfrac{1}{2}(1+\sqrt{m})) \equiv \tfrac{1}{4}(abt + m + 3) \pmod 4.$$

As $T = 2t$ in this case, the first line of (4.2) follows.

Case ii. $T \equiv U \equiv 1 \pmod 2$.

In this case, by Theorem 1, we have

$$l(\tfrac{1}{2}(1+\sqrt{m})) \equiv l(\sqrt{m}) \pmod 4.$$

Appealing to (4.1) we obtain

$$l(\tfrac{1}{2}(1+\sqrt{m})) \equiv \tfrac{1}{4}(abt + m - 5) \pmod 4.$$

As $t = \frac{1}{8}(T^3 + 3mTU^2) = \frac{1}{2}(T^3 + 3T)$ in this case, the second line of (4.2) follows. This completes the proof of Theorem 2.

5. Two Examples

EXAMPLE 1. $m = 325 = 5^2 \times 13$,

$$\sqrt{325} = [18, \overline{36}], \qquad \tfrac{1}{2}(1+\sqrt{325}) = [9, \overline{1, 1, 17}],$$
$$l(\sqrt{325}) = 1, \qquad l(\tfrac{1}{2}(1+\sqrt{325})) = 3, \quad t = 18,\ u = 1,\ T = 36,\ U = 2$$

a and b are given by

$$\frac{b+\sqrt{325}}{a} = [\overline{36}] = 18 + \sqrt{325}$$

that is,

$$a = 1, \qquad b = 18.$$

Hence by Theorem 2 we have

$$l(\sqrt{325}) \equiv \tfrac{1}{4}(1 \times 18 \times 18 + 325 - 5) \equiv 1 \pmod 4,$$
$$l(\tfrac{1}{2}(1+\sqrt{325})) \equiv \tfrac{1}{8}(1 \times 18 \times 36 + 2 \times 325 + 6) \equiv 3 \pmod 4.$$

EXAMPLE 2. $m = 85 = 5 \times 17$,

$$\sqrt{85} = [9, \overline{4, 1, 1, 4, 18}], \qquad \tfrac{1}{2}(1+\sqrt{85}) = [5, \bar{9}],$$
$$l(\sqrt{85}) = 5, \qquad l(\tfrac{1}{2}(1+\sqrt{85})) = 1, \qquad T = 9,\ U = 1,$$
$$t = \tfrac{1}{8}(T^3 + 3mTU^2) = 378, \qquad u = \tfrac{1}{8}(3T^2U + mU^3) = 41.$$

a and b are given by

$$\frac{b+\sqrt{85}}{a} = [\overline{1, 4, 18, 4, 1}] = \frac{2+\sqrt{85}}{9}$$

or by

$$\frac{a+\sqrt{85}}{b} = [\bar{9}] = \frac{9+\sqrt{85}}{2},$$

so that

$$a = 9, \qquad b = 2.$$

Hence by Theorem 2 we have

$$l(\sqrt{85}) \equiv \tfrac{1}{4}(9 \times 2 \times 378 + 85 - 5) \equiv 1 \pmod 4,$$
$$l(\tfrac{1}{2}(1+\sqrt{85})) \equiv \tfrac{1}{8}(9 \times 2 \times (9^3 + 3 \times 9) + 2 \times 85 - 10) \equiv 1 \pmod 4.$$

ACKNOWLEDGMENT

The authors would like to thank an unknown referee whose suggestions greatly helped to improve the proof of Theorem 1.

REFERENCES

1. L. E. DICKSON, "History of the Theory of Numbers," Vol. 2, Chelsea, New York, 1952.
2. H. LÜNEBURG, "Vorlesungen über Zahlentheorie," Birkhaüser Verlag, Stuttgart, 1978.
3. O. PERRON, "Die Lehre von den Kettenbrüchen," Vol. 1, 3 ed., Teubner, Stuttgart, 1954.