# CLASSES OF EQUATIONS OF THE TYPE  $y^2 = x^3 + k$ HAVING NO RATIONAL SOLUTIONS

# HUGH M. EDGAR

The equation  $y^2 = x^3 + k$ , k an integer, has been discussed by many authors. Mordell [1] has found many classes of *k* values for which the equation has no integral solutions. Fueter [2], Mordell [3] and Chang [4] have found classes of *k* values for which the equation has no rational solutions. The following two theorems exhibit two more sets of conditions which give rise to classes of *k* values for which the corresponding equations have no rational solutions.

**THEOREM** 1. The equation  $y^2 = x^3 + k$  has no rational solutions if k is a square *free positive integer and*

- (1)  $k \equiv 2 \text{ or } 3 \pmod{4}$ ,  $k \equiv -3 \pmod{9}$ , *i.e.,*  $k \equiv 6$  *or* 15(mod 36),
- (2)  $3 \nmid H$ , *H* the class number of  $R(\sqrt{k})$ ,
- (3)  $U = 3$  or 6(mod 9) where  $(T, U)$  is the fundamental solution of the Pellian *equation*

 $Y^2 - kX^2 = 1$ ,

- (4)  $3+h$ , *h* the class number of  $R(\sqrt{1-\frac{1}{2}})$
- (5) the integer solutions of  $p^2 + \frac{\kappa}{2}q^2 = 3^{2h}$  when  $h \equiv 1 \pmod{3}$ , *do not satisfy*  $q \equiv \pm 1 \pmod{9}$ , *and when*  $h \equiv -1 \pmod{3}$ , *do not satisfy*  $q \equiv \pm 2 \left(\frac{k}{3}\right)^2$ (mod 9).

THEOREM 2. The equation  $y^2 = x^3 + k$  has no rational solutions if k is a square *free positive integer and*

- (1')  $k \equiv 5 \pmod{8}$  and  $k \equiv -3 \pmod{9}$ , *i.e.*,  $k \equiv -3 \pmod{72}$ ,
- $(2')$  3 + H, H the class number of  $R(\sqrt{k})$ ,
- (3<sup>*'*)</sup>  $U \equiv 3$  or 6(mod 9), *U* the least positive value of q satisfying the Pellian *equation*

Received November 24, 1965.

 $p^2 - kq^2 = +4$ , (4<sup>t</sup>) 3+*h*, *h* the class number of  $R\left(\sqrt{\frac{1}{2}k}\right)$ . (5')  $\alpha$ ,  $\beta$  and  $\gamma$ ,  $\delta$  the respective integer solutions of the equations  $\frac{1}{\Lambda}$   $\left(\alpha^2 + \frac{1}{\Lambda}\right)$  $\left(\frac{1}{3}k\beta^2\right) = 2^h$ ,  $\frac{1}{4} \left(\gamma^2 + \frac{1}{3}k\delta^2\right) = 3^{2h}$  satisfy the conditions: (a) (i)  $\alpha \not\equiv 0 \pmod{9}$  when h is odd, (ii)  $\beta \not\equiv 0 \pmod{9}$  when h is even: (b) when  $h = 3 n + 1$ ,  $\alpha \pm \beta \frac{1}{3} k^2 (\delta \pm \pm 2 \pmod{9})$ *and*  $\delta \equiv \pm 2 \pmod{9}$ , *when*  $h = 3 n - 1$ ,  $\left\{ \alpha \left( \frac{1}{3} k \right) \pm \beta \right\} \delta \equiv \pm 2 \pmod{9}$ and  $\delta \equiv \pm 4 \left(\frac{k}{3}\right)^2$  (mod 9) were the signs are all independent of *each other.*

*Proof of Theorem* 1. The set of conditions used in Theorem 1 arises from a theorem proved by Mordell [3] upon replacing his condition (3), in which he assumes that  $U \not\equiv 0$ ,  $\pm 1 \pmod{9}$ , by the condition (3) as shown in the statement of Theorem 1. Hence it suffices to prove that at that point of the argument where Mordell  $\begin{bmatrix} 3 \end{bmatrix}$  obtains a contradiction by imposing the conditions  $U\neq 0$ ,  $\pm 1 \pmod{9}$  it is possible to obtain a contradiction by imposing instead the conditions  $U \equiv 0 \pmod{3}$  and  $U \not\equiv 0 \pmod{9}$  (i.e.,  $U \equiv 3$  or  $6 \pmod{9}$ ). Upon referring to the paper of Mordell [3] one sees that it is enough to show that the equation

(6) 
$$
Y + \sqrt{k} Z^3 = (T \pm U\sqrt{k})(A + B\sqrt{k})^3
$$

cannot be solved in rational integers *Y*, *Z*, *A* and *B* if  $(Y, k) = 1$  and  $U = 3$ or  $6 \pmod{9}$ .

Upon equating coefficients in (6) one obtains the two equations

(7) 
$$
Z^3 = \pm AU(A^2 + 3kB^2) + TB(3A^2 + kB^2), \text{ and}
$$

(8) 
$$
Y = TA(A^2 + 3kB^2) \pm UkB(3A^2 + kB^2).
$$

Upon taking residues modulo 3 in equation (7) one obtains  $Z = \pm UA \pmod{3}$ . Since it is being assumed that  $U \equiv 0 \pmod{3}$  it follows that  $Z \equiv 0 \pmod{3}$ . Again, taking residues modulo 3 in equation (8) one obtains  $Y \equiv TA \pmod{3}$ . Since  $(F, k) = 1$  it follows that  $A \not\equiv 0 \pmod{3}$  and  $T \not\equiv 0 \pmod{3}$ . Hence  $A^3 \equiv \pm 1$ (mod 9). Next, taking residues modulo 9 in equation (7) one obtains

**CLASSES OF EQUATIONS OF THE TYPE**  $y^2 = x^3 + k$  $+k$  51

(9) 
$$
0 = \pm U + 3TB\left(A^{2} + \frac{k}{3}B^{2}\right) \pmod{9}.
$$

If  $B \equiv 0 \pmod{3}$  then  $3TB(A^2 + \frac{\pi}{2} B^2) \equiv 0 \pmod{9}$ 

which implies  $U \equiv 0 \pmod{9}$  contrary to the assumption on *U*. If  $B \not\equiv 0 \pmod{9}$ 3) then  $B^2 \equiv 1 \pmod{3}$ . Since  $k \equiv -3 \pmod{9}$  it follows that  $\frac{k}{3} \equiv -1 \pmod{3}$ . Since  $A \not\equiv 0 \pmod{3}$  it follows that  $A^2 \equiv 1 \pmod{3}$ . Hence upon assuming (mod 3) one finds that  $A^2 + \frac{R}{2}B^2 \equiv 0 \pmod{3}$  so that once again  $3TB(A^2 + \frac{R}{3})$  $\equiv 0 \pmod{9}$ . Thus one obtains the contradiction  $U \equiv 0 \pmod{9}$  also in this case.

*Proof of Theorem* 2. The set of conditions used in Theorem 2 arises from a theorem proved by Chang  $[4]$  upon replacing his condition (3), in which he assumes that  $U \not\equiv 0 \pmod{3}$  and  $U \not\equiv \pm 2 \pmod{9}$  by the condition (3<sup>t</sup>) as shown in the statement of Theorem 2. The Pellian equation  $p^2 - kq^2 = -4$  need not enter the discussion of the theorem proved by Chang [4] or Theorem 2 since this equation is insoluble whenever  $k \equiv 0 \pmod{3}$ . It suffices to prove that at that point of the argument where Chang  $\left[4\right]$  obtains a contradiction by imposing the conditions  $U \not\equiv 0 \pmod{3}$  and  $U \not\equiv \pm 2 \pmod{9}$  it is possible to obtain a contradiction by imposing instead the conditions

 $U \equiv 0 \pmod{3}$  and  $U \not\equiv 0 \pmod{9}$  (i.e.,  $U \equiv 3$  or 6(mod 9)).

Upon referring to the paper of Chang  $[4]$  one sees that it is enough to show that the equation

(10) 
$$
Y + Z^3 \sqrt{\overline{k}} = \left(\frac{1}{2} T \pm \frac{1}{2} U \sqrt{\overline{k}}\right) \left(\frac{1}{2} A + \frac{1}{2} B \sqrt{\overline{k}}\right)^3
$$

cannot be solved in rational integers Y, Z, A and B if  $(Y, k) = 1$  and  $U = 3$  or 6(mod 9). Here  $(T, U)$  is the fundamental solution of the Pellian equation  $p^2 - kq^2 = +4.$ 

Upon equating coefficients in (10) one obtains the two equations

(11) 
$$
16 Z^3 = \pm A U (A^2 + 3 k B^2) + T B (3 A^2 + k B^2), \text{ and}
$$

(12) 
$$
16 Y = TA(A^2 + 3kB^2) \pm UkB(3A^2 + kB^2).
$$

Upon taking residues modulo 3 in equation (11) one obtains  $Z = \pm UA \pmod{3}$ . Since it is being assumed that  $U=0 \pmod{3}$  it follows that  $Z=0 \pmod{3}$ .

### 52 HUGH M. EDGAR

Again, taking residues modulo 3 in equation (12) one obtains  $Y \equiv TA \pmod{3}$ . Since  $(Y, k) = 1$  it follows that  $A \not\equiv 0 \pmod{3}$  and  $T \not\equiv 0 \pmod{3}$ . Hence  $A^3 \equiv \pm 1$ (mod 9). Next, taking residues modulo 9 in equation (11) one obtains a contradiction in the form  $U \equiv 0 \pmod{9}$ , just as in the proof of Theorem 1.

It seems natural to ask whether it is possible to make any progress when one assumes  $k \equiv 1 \pmod{8}$  and simultaneously  $k \equiv -3 \pmod{9}$  i.e.,  $k \equiv 33 \pmod{9}$ 72). If one parallels the work of Chang [4] it is found that the equation

$$
(13)\qquad \qquad Y^2 - kZ^6 = X^3
$$

can be obtained. The symbols *X<sup>y</sup> Y* and *Z* have the meanings ascribed to them by Chang [4] and the conditions  $(Y, Z) = (X, Z) = 1$  obtain. Upon assuming *k* to be square free one also obtains  $(Y, k) = 1$ . Since  $k \equiv 1 \pmod{8}$ both odd and even values for *X* are conceivable. If  $X \equiv 1 \pmod{2}$  then the argument proceeds exactly as in Chang [4], provided (2) through (5) of Chang [4] (or (2') through (5') of Theorem 2) are assumed. Hence in these two cases one can conclude that there are no solutions of equation (13) with  $X \equiv 1$ (mod 2). It may therefore now be assumed that  $X \equiv 0 \pmod{2}$ . Upon factorizing the lefthand side of equation (13) one obtains the ideal equation

(14) 
$$
\mathbb{E}Y + Z^3 \sqrt{k} \mathbb{E}Y - Z^3 \sqrt{k} \mathbb{E}Y = \mathbb{E}X \mathbb{I}^3.
$$

Let *A* be the greatest common divisor of the two ideals  $[Y + Z^3\sqrt{k}]$  and  $[Y - Z^3 \sqrt{k}]$ . Then it can be shown that  $A/[2]$ . To prove this fact it is enough to show that  $2 \in A$ , since  $A|[2]$  can equivalently be expressed by saying that *A* includes (as a set of algebraic integers from the field  $R(\sqrt{k})$ ) [2]. By the definition of *A* one has

(15) 
$$
A = (\llbracket Y + Z^3 \sqrt{k} \rrbracket, \llbracket Y - Z^3 \sqrt{k} \rrbracket)
$$

$$
= \llbracket Y + Z^3 \sqrt{k} k, \quad Y - Z^3 \sqrt{k} \rrbracket.
$$

It will suffice to prove the existence of rational integers *a, b, c* and *d* having the properties

(16) 
$$
2 = \left(\frac{a+b\sqrt{k}}{2}\right)\left(\frac{Y+Z^3\sqrt{k}}{2}\right) + \left(\frac{c+d\sqrt{k}}{2}\right)\left(\frac{Y-Z^3\sqrt{k}}{2}\right),
$$

(17) 
$$
a \equiv b \pmod{2}, \ c \equiv d \pmod{2}.
$$

The form for the general integer of  $R(\sqrt{k})$  follows from the assumption  $k \equiv 1$ (mod 4). Upon equating coefficients on both sides of equation (16) and sim

plifying, one obtains

(18) 
$$
(a + c) Y + (b - d) k Z3 = 4, and
$$

(19)  $(b+d)Y+(a-c)Z^3=0.$ 

Equation (19) can be satisfied by putting  $a = c$  and  $b = -d$ . Then equation  $(18)$  becomes

$$
(20) \t\t aY + bkZ^3 = 2.
$$

Now since  $X \equiv 0 \pmod{2}$  by assumption, it is necessary to have  $Y \equiv Z \equiv 1 \pmod{2}$ 2). Then it follows that  $Y = kZ^3 = 1 \pmod{2}$  from which it follows that if *(a, b*) is to be a solution of equation (20) then  $a \equiv b \pmod{2}$  is necessary. This last condition is in accord with equation (17). Equation (20) is a linear diophantine equation in the two quantities *a* and *b* and has solutions in *a* and *b* since  $(Y, kZ^3) = 1/2$ . Finally, since  $a \equiv b \pmod{2}$  is required by equation (20) the previously imposed conditions  $a = c$  and  $b = -d$  imply that  $b \equiv d \pmod{d}$ 2). Hence it follows that it is possible to find rational integers *a, b, c* and *d* satisfying equations (16) and (17) and so  $A|[2]$  as stipulated.

It will be of use in the sequel to know the canonical decomposition of the ideal [2] in the field  $R(\sqrt{k})$ . Since it is being assumed that  $k \equiv 1 \pmod{4}$  it follows (Theorem 872, page 172, Landau [5]) that the discriminant  $\Delta$  of  $R(\sqrt{k})$ is given by  $\Delta = k \equiv 1 \pmod{8}$ . Hence  $\Delta$  is a quadratic residue modulo 8. From Theorem 879, page 178, Landau [6] with  $p = 2$  it follows that  $[2] = PQ$  where  $P = [2, R + \omega]$  and  $Q = [2, R + \omega']$  for a suitable rational integer *R*. Here  $\omega = \frac{1+\sqrt{R}}{2}$  and  $\omega' = \frac{1-\sqrt{R}}{2}$ . Also since 2 + J it follows from Theorem 880, page 180, Landau [7] that  $P \neq Q$ . *P* and *Q* are prime ideals.

It can be shown that one can choose the prime ideal factors of [2] as *P* = [2,  $\omega$ ] and *Q* = [2,  $\omega'$ ]. Upon writing *PQ* = [2,  $\omega$ ][2,  $\omega'$ ] = [4, 2  $\omega$ ,  $2\omega'$ ,  $\omega\omega'$ ] one sees that 4, 2  $\omega$ , 2  $\omega'$  and  $\omega\omega'$  are integral (algebraic) multiples of 2 and so [2] | PQ. The element  $\omega \omega'$  has the value  $\frac{1-k}{4}$  and since  $k \equiv 1 \pmod{8}$  it follows that  $\omega \omega'$  is an even rational integer. Also  $2 = 2 \omega + 2 \omega'$  so that  $PQ|[2]$ . Hence  $PQ = [2]$ .

The next step is to determine under what conditions *P* and *Q* are principal ideals. In order that *P* and *Q* be principal ideals it is necessary and sufficient that the number 2 have a non-trivial representation of the form

**54 HUGH M. EDGAR**

(21) 
$$
2 = \left(\frac{a+b\sqrt{k}}{2}\right)\left(\frac{u+v\sqrt{k}}{2}\right)
$$

where *a*, *b*, *u* and *v* are rational integers satisfying the conditions  $a \equiv b \pmod{2}$ ,  $u \equiv v \pmod{2}$ . The term non-trivial refers to the requirement that

$$
\frac{a+b\sqrt{k}}{2} \text{ and } \frac{u+v\sqrt{k}}{2} \text{ not be units of } R(\sqrt{k}).
$$

From the ideal equation corresponding to equation (21) *it* follows that one can identify P with  $\left\lfloor \frac{a+b\sqrt{k}}{2} \right\rfloor$  and Q with  $\left\lfloor \frac{a+b\sqrt{k}}{2} \right\rfloor$ . Now it is known the  $N(P) = N(Q) = 2$ , and so, using the fact that  $N([\beta]) = |N(\beta)|$  where  $\beta$  is any integer of  $R(\sqrt{k})$ , one sees that the two equations

$$
(22) \qquad |a^2 - kb^2| = 8
$$

$$
(23) \t\t\t |u^2 - kv^2| = 8
$$

must be satisfied. Since  $x^2 - ky^2 = +8$  is insoluble whenever  $k \equiv 0 \pmod{3}$ , equations (22) and (23) become

(24) 
$$
a^2 - kb^2 = -8,
$$

(25) 
$$
u^2 - kv^2 = -8.
$$

Upon equating coefficients on both sides of equation (21) one obtains the two equations

$$
(26) \t\t au + bv = 8
$$

$$
(27) \t av + bu = 0.
$$

If one multiplies equation (26) by  $v$  and substitutes for  $av$  from equation (27) it is found, using equation (25), that  $b = v$ . Hence also  $u = -a$  and thus equation (21) becomes

(28) 
$$
2 = \left(\frac{a+b\sqrt{k}}{2}\right)\left(\frac{-a+b\sqrt{k}}{2}\right).
$$

It is seen that, since  $k \equiv 1 \pmod{4}$ , the parity restrictions on *a*, *b*, *u* and *v* must be met if equations (24) and (25) are to be satisfied.

Since  $k \equiv 1 \pmod{4}$  and since  $Y = Z^3 \equiv 1 \pmod{2}$  it follows that  $\frac{Y + Z \sqrt{R}}{2}$ and  $\frac{Y-Z^3\sqrt{k}}{2}$  are integers of  $R(\sqrt{k})$ . In other words  $[2] | [Y+Z^3\sqrt{k}]$  and  $[2]$  I  $[Y - Z^3\sqrt{k}]$ . Putting this fact together with the previous result that  $A[[2]]$ shows that  $A = [2]$ . From equation (14), using the fact that  $X \equiv 0 \pmod{2}$ 

one obtains the equation

(29) 
$$
\left[\frac{Y+Z^3\sqrt{k}}{2}\right]\left[\frac{Y-Z^3\sqrt{k}}{2}\right] = \left[2\right]\left[\frac{X}{2}\right]^3
$$

where the two ideals on the left-hand side of equation (29) are relatively prime. Upon using the unique factorization of ideals in an algebraic number field, one obtains the two equations

$$
(30) \qquad \qquad \left[\frac{Y+Z^3\sqrt{k}}{2}\right]=I_1D_1^3,
$$

$$
(31) \qquad \qquad \left[\frac{Y - Z^3 \sqrt{k}}{2}\right] = I_2 D_2^3,
$$

Where  $I_1$ ,  $I_2$ ,  $D_1$  and  $D_2$  are ideals in  $R(\sqrt{k})$  which satisfy the conditions  $(I_1, I_2) = [1]$ 

$$
I_1I_2 = [2], (D_1, D_2) = [1]
$$
 and  $D_1D_2 = \left[\frac{X}{2}\right]$ .

If it is now assumed that the Pellian equation  $a^2 - kb^2 = -8$  can be solved, it follows that the ideals  $I_1$  and  $I_2$  are principal ideals in every case, according to remarks made previously. Then from equations (30) and (31) it follows that  $D_1^3$  and  $D_2^3$  are also principal ideals. Finally, the assumption  $3/H$  leads one to conclude that  $D_1$  and  $D_2$  are principal ideals. Thus, in particular, one can write  $I_1 = \left[ \frac{a+b\sqrt{k}}{2} \right]$  and  $D_1 = \left[ \frac{c+d\sqrt{k}}{2} \right]$ . From equation (30) one obtains the equation

(32) 
$$
\left[\frac{Y+Z^3\sqrt{k}}{2}\right]=\left[\frac{a+b\sqrt{k}}{2}\right]\left[\frac{c+d\sqrt{k}}{2}\right]^3.
$$

From equation (32) one obtains the equation

(33) 
$$
\frac{Y + Z^3 \sqrt{k}}{2} = \varepsilon \left( \frac{a + b\sqrt{k}}{2} \right) \left( \frac{c + d\sqrt{k}}{2} \right)^3
$$

 $Y - Z^3 \sqrt{k}$ where  $\varepsilon$  is a unit of the field  $\mathbf{\Lambda}(\mathbf{\gamma}\kappa)$ . It follows that one can write  $\frac{\gamma}{2}$ in the form

(34) 
$$
\frac{Y - Z^3 \sqrt{k}}{2} = \epsilon \left( \frac{a - b\sqrt{k}}{2} \right) \left( \frac{c - d\sqrt{k}}{2} \right)^3
$$

and a corresponding equation in ideals would be

$$
(35) \qquad \qquad \left[\frac{Y - Z^3 \sqrt{k}}{2}\right] = \left[\frac{a - b\sqrt{k}}{2}\right] \left[\frac{c - d\sqrt{k}}{2}\right]^3.
$$

From equations (31) and (35) one obtains the equation

(36) 
$$
I_2 D_2^3 = \left[ \frac{a - b\sqrt{k}}{2} \right] \left[ \frac{c - d\sqrt{k}}{2} \right]^3.
$$

From equation (36) one has  $\left[\frac{c-d\sqrt{k}}{2}\right]$   $D_2$  for if there were a prime ideal R with the properties  $R\left|\frac{c-d\sqrt{k}}{2}\right|$  and  $R+D_2$  then one would necessarily have  $R^3 | I_2$ , which is impossible since  $I_2 | [2]$ . In the same way, one finds that  $D_2\left[\frac{c-a\sqrt{\kappa}}{2}\right]$  since the conditions on  $\left[\frac{a-v\sqrt{\kappa}}{2}\right]$  make it impossible to have the cube of a prime ideal dividing  $\left[\frac{a-b\sqrt{k}}{2}\right]$ . Hence  $D_2 = \left[\frac{c-d\sqrt{k}}{2}\right]$  and  $\left[\frac{-b\sqrt{k}}{2}\right]$ . Since one now has  $I_1I_2 = \left[\frac{a+b\sqrt{k}}{2}\right] \left[\frac{a-b\sqrt{k}}{2}\right] = [2]$ , the two possibilities  $I_1 = [1]$  and  $I_1 = [2]$  cannot arise.

If one parallels the treatment of Mordeli [3] the following equations result in those cases where the unit cannot be totally absorbed

(37) 
$$
\frac{Y+Z^3\sqrt{k}}{2} = \left(\frac{T \pm U\sqrt{k}}{2}\right)\left(\frac{a+b\sqrt{k}}{2}\right)\left(\frac{C+D\sqrt{k}}{2}\right)^3,
$$

$$
(38) \tC2 - kD2 = -2 X.
$$

In those situations where total absorption of the unit factor is possible, equation (38) still applies but equation (37) is replaced *by* the equation

(39) 
$$
\frac{X+Z^3\sqrt{k}}{2} = \left(\frac{a+b\sqrt{k}}{2}\right)\left(\frac{C+D\sqrt{k}}{2}\right)^3.
$$

From equation (39) one obtains, upon equating coefficients, the equation

(40) 
$$
8 Y = aC(C^2 + 3 kD^2) + b k D(3 C^2 + kD^2).
$$

Upon taking residues modulo 9 in equation (40) it is found, using the fact that  $C \neq 0 \pmod{3}$ , that  $Y = \pm a \pmod{9}$ . Now if it is assumed that  $b \equiv 0 \pmod{3}$ then the equation  $a^2 - kb^2 = -8$  forces the condition  $a^2 \equiv 1 \pmod{9}$ . Thus  $Y^2$  $\equiv$  1(mod 9) and upon referring back to equation (13) it can be seen that  $Z \equiv 0$ (mod 3) is necessary. Upon equating coefficients of  $\sqrt{k}$  in equation (39) one obtains the equation

(41) 
$$
8 Z^3 = aD(3 C^2 + kD^2) + bC(C^2 + 3 kD^2).
$$

Upon taking residues modulo 9 in equation (41) it is found that  $b \equiv 0 \pmod{9}$ is required. Thus one cannot find rational integers F, Z, *C* and *D* whicfi

satisfy equation (39) if it is assumed that  $b \equiv 0 \pmod{3}$  and simultaneously  $b \not\equiv 0 \pmod{9}$ .

From equation (37) one obtains, upon equating coefficients of *k,* the equation

(42) 
$$
16 Z^3 = (Ta \pm Ubk) (3 C^2 + kD^2) D + (Tb \pm Ua) (C^2 + 3kD^2) C.
$$

In equation (42) it is enough to consider the positive sign, upon replacing *b* by  $-b$ , D by  $-D$  and leaving a and C unchanged. This replacement has the effect of changing  $Y$  to  $-Y$ . Hence one can replace equation (42) by the equation

(43) 
$$
16 Z^3 = (Ta + Ubk) (3 C^2 + kD^2) D + (Tb + Ua) (C^2 + 3 kD^2) C.
$$

Upon taking residues modulo 9 in equation (43) one obtains the relation

(44) 
$$
-2 Z^3 \equiv \pm (Tb + Ua) \pmod{9}.
$$

With the assumptions on U and b it follows that  $Z \equiv 0 \pmod{3}$  so that one would require  $Tb + Ua \equiv 0 \pmod{9}$ .

The following result has been established:

**THEOREM** 3. The equation  $y^2 = x^3 + k$  has no rational solutions if k is a square *free positive integer and if the following conditions obtain:*

(a)  $k \equiv 1 \pmod{8}$  *and*  $k \equiv -3 \pmod{9}$ ,

*i.e.*,  $k \equiv 33 \pmod{72}$ ,

(b) the conditions (2<sup>t</sup>) through (5<sup>t</sup>) of Theorem 2,

(c) the Pellian equation  $X^2 - kY^2 = -8$  is soluble and possesses a solution  $(a, b)$  for which  $b \equiv 0 \pmod{3}$  and  $b \not\equiv 0 \pmod{9}$ ,

*i.e.,*  $b \equiv 3$  *or* 6(mod 9).

(d)  $Tb + Ua \not\equiv 0 \pmod{9}$ .

# **REFERENCES**

- [1] Mordell, L. J., Proc. London Math. Soc, Hodgson, London, 1914, Volume 13, The Dio phantine equation  $y^2 - k = x^3$ , Pages 60-80.
- [2] Fueter, R., Commentarii Mathematici Helvetici, Societate Mathematica Helvetica, Zurich, 1930, Volume 2, Ueber kubische diophantische Gleichungen, Pages 69-89.
- [3] Mordell, L. J., Archiv fur Mathematik og Naturvidenskab B.I.L., NR 6, Oslo, 1947, On some diophantine equations  $y^2 = x^3 + k$  with no rational solutions, Pages 143-150.
- [4] Chang, K. L., The Quarterly Journal of Mathematics, Oxford University Press, Oxford,

#### **58 HUGH M. EDGAR**

1948, Volume 19. On some diophantine equations  $y^2 = x^3 + k$  with no rational solutions, **Pages 181-188.**  $\mathcal{A}$ 

- **[5] Landau, E. G. H., Vorlesungen ίiber Zahlentheorie, Chelsea Publishing Company, New York, 1947, Page 172, Theorem 872.**
- **[6] Landau, E. G. H., Vorlesungen iiber Zahlentheorie, Chelsea Publishing Company, New York, 1947, Page 178, Theorem 879.**
- **[7] Landau, E. G. H., Vorlesungen iiber Zahlentheorie, Chelsea Publishing Company, New York, 1947, Page 180, Theorem 880.**

*San Jose State College, San Jose 14, Calif., U.S.A.*