ON THE DIOPHANTINE EQUATION $Cx^2 + D = y^n$

W. LJUNGGREN

1. Introduction. Let C, D and n denote odd positive integers, $D > 1$ and CD without any squared factor > 1. Let $K = Q(\sqrt{-CD})$, where Q is the field of rational numbers. Let further h denote the number of classes of ideals in K and put $D + (-1)^{(D+1)/2} = 2^m \cdot D_1$, $(D_1, 2) = 1$. In two previous papers [4] and [5] I have proved the following three theorems concerning the diophantine equation $Cx^2 + D = y^n$:

I. The diophantine equation

$$(1) \qquad Cx^2 + D = y^n\,, \qquad n > 1$$

is impossible in rational integers x and y if $h \not\equiv 0 \pmod{n}$, m is odd and either $CD \equiv 1 \pmod{4}$ or $CD \equiv 3 \pmod{8}$ with $n \not\equiv 0 \pmod{3}$.

II. The diophantine equation

$$(2) \qquad Cx^2 + D = y^q\,, \qquad q > 3$$

where q denote an odd prime and $CD \not\equiv 7 \pmod{8}$, is impossible in rational integers x and y if $h \not\equiv 0 \pmod{q}$, m is even and $q \not\equiv CD_1 \pmod{8}$.

III. If $D \equiv 1 \pmod{4}$, $CD \not\equiv 7 \pmod{8}$ and m is even, then the equation (2) has only a finite number of solutions in natural numbers x, y and primes q if $CD_1 \equiv 5 \pmod{8}$ or if $C = 1$ with $D_1 \equiv 3 \pmod{8}$ for given C and D. The possible values of y and an upper limit for the number of primes q may always be determined after a finite number of arithmetical operations.

From the proofs it immediately follows that these theorems also hold good if $CD \equiv 7 \pmod{8}$, *provided y is an odd integer.* This gives a far-reaching extension of results obtained by D. J. Lewis in his paper [2]. Putting $C = 1$, $D = 7$ we find, from 1:

The diophantine equation $x^2 + 7 = y^z$, $z > 1$, is impossible in rational integers x, y and z if y is an odd integer.

Equations of the type (1) have also been studied by T. Nagell [6], [8], [9] and B. Stolt [11].

Received July 2, 1963.

2. The equation $Cx^2 + 4D = y^n$, y odd.

THEOREM 1. *Let n be the power of a prime $q > 3$, and suppose that $h \not\equiv 0 \pmod{n}$. Then the diophantine equation*

$$(3) \qquad Cx^2 + 4D = y^n , \qquad n > 1 , \ y \text{ odd}$$

has no solutions in rational integers x, y if $q \not\equiv 3C(-1)^{(C-1)/2} \pmod{8}$. Likewise, if $D \equiv 0 \pmod{q}$, equation (3) has no integral solution.

Proof. We put $n = q^\alpha$. The principal ideals

$$[Cx + 2\sqrt{-CD}] \quad \text{and} \quad [Cx - 2\sqrt{-CD}]$$

have the greatest common ideal divisor $[C, \sqrt{-CD}]$, because $[C] = [C, \sqrt{-CD}]^2$, y is an odd integer and $(x, y) = 1$. From (3) it then follows

$$[Cx + 2\sqrt{-CD}] = [C, \sqrt{-CD}] \cdot \mathfrak{i}^{q^\alpha} ,$$

where $\mathfrak{i}$ denotes an ideal of the field $Q(\sqrt{-CD})$. Further we get

$$(4) \qquad [Cx + 2\sqrt{-CD}]^2 = [C] \cdot \mathfrak{i}_1^{q^\alpha} (\mathfrak{i}_1 = \mathfrak{i}^2) .$$

If the class number h is divisible by q^β $(0 \leqq \beta < \alpha)$ and not by $q^{\beta+1}$, there exist two rational integers f and g such that

$$fq^\alpha - gh = q^\beta .$$

Then by (4) we get the following equivalence

$$\mathfrak{i}_1^{q^\beta} \sim \mathfrak{i}_1^{fq^\alpha} \sim 1 .$$

Hence we obtain the ideal equation

$$(5) \qquad [Cx + 2\sqrt{-CD}]^2 = [C] \cdot \left[\frac{1}{2}(u + v\sqrt{-CD})\right]^{q^{\alpha-\beta}}$$

where u and v are rational integers, $u \equiv v \pmod{2}$. Since $q > 3$ all the units in the field $Q(\sqrt{-CD})$ are q^{th} powers. Then it follows from (5)

$$(6) \quad (Cx + 2\sqrt{-CD})^2 = C\left(\frac{1}{2}(u_1 + v_1\sqrt{-CD})\right)^q , \qquad u_1 \equiv v_1 \pmod{2} .$$

By means of (6) we derive

$$\frac{1}{2}(u_1 + v_1\sqrt{-CD}) = \left(\frac{1}{2}(a_1\sqrt{C} + b_1\sqrt{-D})\right)^2 , \qquad a_1 \equiv b_1 \pmod{2}$$

Inserting this expression in (6) we get

$$(7) \qquad x\sqrt{C} + 2\sqrt{-D} = \left(\frac{1}{2}(a_2\sqrt{C} + b_2\sqrt{-D})\right)^q , \qquad a_2 \equiv b_2 \pmod 2 .$$

Equating the coefficients of $\sqrt{-D}$ we obtain the relation

$$(7') \qquad 2^{q+1} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} a_2^{q-1-2r} b_2^{2r+1} C^{[(q-1)/2]-r} (-D)^r ,$$

whence $b_2 = \pm 2^s$, $0 \leqq s \leqq q+1$.

Equation (7′) gives modulo q

$$b_2^q(-D)^{(q-1)/2} \equiv 2^{q+1} \pmod q ,$$

or

$$b_2\left(\frac{-D}{q}\right) \equiv 4 \pmod q , \qquad \text{i.e.}$$
$$b_2 \equiv \pm 4 \pmod q .$$

For $q > 5$ b_2 and a_2 must be even numbers, so that we have

$$(8) \qquad x\sqrt{C + 2}\sqrt{-D} = (a\sqrt{C + b}\sqrt{-D})^q .$$

If $q = 5$ and $b_2 = \pm 1$ it follows from (7′) that

$$D^2 \pm 8 = 5\left(\frac{1}{2}(Ca^2 - D)\right)^2 ,$$

which is impossible mod 8. Equation (8) is then valid if $q > 3$. Corresponding to (7′) we get

$$(8') \qquad 2 = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (Ca^2)^{[q-1)/2]-r} b^{2r+1} (-D)^r$$

Equation (8′) is impossible if q divides D. If $(D, q) = 1$ it follows from (8′)

$$2 \equiv b^q(-D)^{(q-1)/2} \equiv b\left(\frac{-D}{q}\right) \pmod q ,$$

whence

$$b = 2\left(\frac{-D}{q}\right) .$$

Inserting this expression for b in (8′) we obtain

$$(9) \qquad \left(\frac{-D}{q}\right) = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (Ca^2)^{[(q-1)/2]-r} (-4D)^r .$$

At first we want to prove that (9) *is impossible if* $q \equiv 1 \pmod 4$.

Treating (9) as a congruence mod 4 we find

$$\left(\frac{-D}{q}\right) = 1 .$$

Suppose now that $q-1$ is divisible by 2^{δ}, but not by $2^{\delta+1}$, $\delta \geqq 2$. Equation (9) may be written

$$(10) \quad 1 - q + q(1 - (Ca^2)^{(q-1/2)}) = \sum_{r=1}^{(q-1)/2} \binom{q}{2r+1} (Ca^2)^{[(q-1)/2]-r}(-4D)^r .$$

The general term in the right-hand side in (10) we then prefer to give the following shape

$$(11) \qquad \frac{q(q-1)}{2r(2r+1)} \cdot 2^{2r} \cdot \binom{q-2}{2r-1} (Ca^2)^{[(q-1)/2]-r} \cdot (-D)^r .$$

Here the numerator is divisible by $2^{\delta+2r}$. The denominator is divisible by a power of 2 which is $\leqq 2$. Since for all $r \geqq 1$ $2^{2r} > 2r$, we conclude that the integer (11) is divisible at least by $2^{\delta+1}$. Hence equation (10) is impossible, because $(Ca^2)^{(q-1)/2} - 1$ is divisible at least by $2^{\delta+1}$, while $q-1$ is divisible by 2^{δ} but not by $2^{\delta+1}$.

It remains to consider the case $q \equiv 3 \pmod 4$. From (9) it then follows

$$\left(\frac{-D}{q}\right) \equiv qC \pmod 4 ,$$

whence

$$(12) \qquad \begin{aligned} \left(\frac{-D}{q}\right) &= -1 \text{ for } C \equiv 1 \pmod 4 , \\ \left(\frac{-D}{q}\right) &= +1 \text{ for } C \equiv 3 \pmod 4 . \end{aligned}$$

Treating (9) as a congruence mod 8, we get

$$(13) \qquad \left(\frac{-D}{q}\right) \equiv qC + 4 \pmod 8$$

Combining (12) and (13) we find

$$q \equiv 3C(-1)^{(C-1)/2} \pmod 8$$

which was to be proved.

REMARK. Theorem 1 remains true if $q = 3$, provided $CD \not\equiv 3 \pmod 8$: All units in $Q(\sqrt{-CD})$ are still q^{th} powers, such that equation (7) also holds good for $q = 3$. Since $b_2 \equiv \pm 4 \pmod q$, we have in addition to consider the cases $b_2 = \pm 1$ and $b_2 = \pm 2$. If $b_2 = \pm 1$

we deduce from (7) that $D = 3Ca_2^2 + 16$, which implies $CD \equiv 3 \pmod 8$, a contradiction. If $b_2 = \pm 2$, a_2 must be even. Putting $a_2 = 2a_3$ we find $D = 3Ca_3^2 + 2$ and $y = 4Ca_3^2 + 2$. But we assumed y to be an odd integer, and then our assertion is proved.

We now proceed to prove two lemmas.

LEMMA 1. *Putting*

$$S_1 = \sum_{r=0}^{[(n-1)/4]} \binom{n}{4r+1} \quad \text{and} \quad S_2 = \sum_{r=0}^{[(n-3)/4]} \binom{n}{4r+3} \tag{15}$$

we have if $n \equiv 3 \pmod 8$

$$S_1 \equiv 0 \pmod 3 , \qquad S_2 \equiv 1 \pmod 3 , \tag{16}$$

and if $n \equiv 7 \pmod 8$

$$S_1 \equiv 1 \pmod 3 , \qquad S_2 \equiv 0 \pmod 3 . \tag{17}$$

Proof. Inserting $x = 1$ and $x = i$ in the identity

$$\frac{1}{2x}((1+x)^n - (1-x)^n) = \binom{n}{1} + \binom{n}{3}x^2 + \binom{n}{5}x^4 + \cdots,$$

we get

$$2^{n-1} = S_1 + S_2 ,$$

and

$$2^{(n-1)/2} \cdot (-1)^{(n-3)/4} = S_1 - S_2 , \qquad n \equiv 3 \pmod 4 ,$$

from which (16) and (17) easily follow.

LEMMA 2. *Equation* (9) *is impossible for* $q > 3$ *if*

$$D \equiv (-1)^{(C+1)/2} \pmod 3 , \tag{18}$$

and besides one of the three following conditions is satisfied:

$$\begin{aligned} &1^\circ \quad C \equiv 0 \pmod 3 \\ &2^\circ \quad C \equiv \pm 1 \pmod 8 \\ &3^\circ \quad C \equiv \pm 3 \pmod 8 \quad \textit{and} \quad C \equiv (-1)^{(C-1)/2} \pmod 3 . \end{aligned} \tag{19}$$

Proof. If $a \equiv 0 \pmod 3$ or if $C \equiv 0 \pmod 3$ it follows from (9) and (12) that

$$(-1)^{(C+1)/2} \equiv -(4D)^{(q-1)/2} \equiv -D \pmod 3 , \quad \text{because } D^2 \equiv 1 \pmod 3 .$$

But this contradicts condition (18).

If $a^2 \equiv 1 \pmod 3$, $C \not\equiv 0 \pmod 3$ we find

$$(-1)^{(\sigma+1)/2} = \binom{q}{1}C - \binom{q}{3}D + \binom{q}{5}C - \binom{q}{7}D + - \cdots,$$

or

$$(-1)^{(\sigma+1)/2} \equiv CS_1 - DS_2 \pmod 3 . \tag{20}$$

The congruence $C \equiv \pm 1 \pmod 8$ may be written $C \equiv (-1)^{(\sigma-1)/2} \pmod 8$. By Theorem 1 we then conclude $q \equiv 3C(-1)^{(\sigma-1)/2} \equiv 3 \pmod 8$. According to Lemma 1 it follows from (20)

$$(-1)^{(\sigma+1)/2} \equiv -D \pmod 3 ,$$

a contradiction.

The congruence $C \equiv \pm 3 \pmod 8$ is equivalent to $C \equiv 3(-1)^{(\sigma+1)/2} \pmod 8$. By means of Theorem 1 we conclude

$$q \equiv 3C(-1)^{(\sigma-1)/2} \equiv 7 \pmod 8 ,$$

and Lemma 1 then gives

$$(-1)^{(\sigma+1)/2} \equiv C \pmod 3 ,$$

which contradicts the second part of the condition 3°.

Our lemma is proved.

THEOREM 2. *Let C, D, n and h be defined as before, $h \not\equiv 0 \pmod n$. If $D \equiv (-1)^{(\sigma+1)/2} \pmod 3$ and if further one of the conditions* (19) *is satisfied, then the diophantine equation*

$$Cx^2 + 4D = y^n , \qquad n > 1,\ y \text{ odd} \tag{21}$$

has no solutions in rational integers x and y, provided $n \not\equiv 0 \pmod 3$ in case $CD \equiv 3 \pmod 8$.

Proof. Suppose that (21) is solvable in integers x, y, where y is odd. There must exist a prime factor q of n with the following property: q^α is a factor of n but not of the class number h. We put $m = q^\alpha$, $n = mr$ and $z = y^r$. Then the equation

$$Cx^2 + 4D = z^m \tag{22}$$

should be solvable in integers x and z. But this is impossible on account of Lemma 2 and the remark to Theorem 1.

EXAMPLE. *The equation $3x^2 + 28 = y^n$, $n \geqq 3$, has no solutions in rational integers x, y with y odd.*

Here is $C = 3$, $D = 7 \equiv 1 \pmod 3$ and $CD \equiv 5 \pmod 8$. Putting $x = 2x_1$, $y = 2y_1$ we get $3x_1^2 + 7 = 2^{n-2}y_1^n$, which implies $n = 3$, because $3x_1^2 + 7 = 2 \pmod 4$. Equation $3x_1^2 + 7 = 2y_1^3$ has at least the solutions $x_1 = \pm 9$, $y_1 = 5$.

3. The equation $x^2 + 4D = y^n$, y odd. In this section we restrict ourselves to the simple case $C = 1$. According to Theorem 1 and the remark attached to this it will be sufficient to deal with the case $q \equiv 3 \pmod 8$, $q = 3$ included. Putting

$$\lambda = a + 2\sqrt{-D} \qquad \text{and} \qquad \lambda' = a - 2\sqrt{-D}$$

it follows from (8), with $b = 2(-D/q) = 2(-1)^{(q+1)/2} = -2$:

$$\frac{\lambda^q - \lambda'^q}{\lambda - \lambda'} = -1 \,. \tag{23}$$

The following identity is easily verified:

$$\frac{\lambda^{(q-1)/2} - \lambda'^{(q-1)/2}}{\lambda - \lambda'}\cdot(\lambda^{(q+1)/2} + \lambda'^{(q+1)/2}) = -(\lambda\lambda')^{(q-1)/2} + \frac{\lambda^q - \lambda'^q}{\lambda - \lambda'} \,. \tag{24}$$

Since $q = 8t + 3$, (24) may be written

$$\frac{\lambda^{4t+1} - \lambda'^{4t+1}}{\lambda - \lambda'}(\lambda^{4t+2} + \lambda'^{4t+2}) = -(a^2 + 4D)^{4t+1} - 1 \,. \tag{25}$$

The second factor on the left-hand side of (25) is divisible by $(\lambda^2 + \lambda'^2)/2 = a^2 - 4D$. Suppose now $a^2 - 4D > 0$. Since $a^2 - 4D \equiv 5 \pmod 8$, this number contains at least one prime factor $p \equiv 7 \pmod 8$ or $p \equiv 5 \pmod 8$. By means of (25) we derive that the Legendre symbol $((-a^2 - 4D)/p) = -1$, which implies $(-2/p) = 1$, i.e. $p = 8t + 1$ or $8t + 3$, contrary to the assumption. We therefore conclude $a^2 - 4D < 0$, or

$$a^2 < 4D \,. \tag{26}$$

These considerations yield the following theorem:

THEOREM 3. *Let $D > 1$ denote an odd positive integer without any squared factor > 1. If the class number of $Q(\sqrt{-D})$ is indivisible by the odd prime q, then the diophantine equation*

$$x^2 + 4D = y^q \,, \qquad y \text{ odd} \tag{27}$$

has no solutions in rational integers if $q \not\equiv 3 \pmod 8$. If $q \equiv 3 \pmod 8$, then (27) has only a finite number of solutions in rational integers x and y and primes q for given D. The possible values of y and an upper limit for the number of primes q may always *be determined after a finite number of arithmetical operations.*

That an upper limit for the number of primes may be determined, follows as a consequence of a theorem due to Th. Skolem [10]. However, in special cases it will be more convenient to use other methods.

Example 1. $x^2 + 28 = y^q$. We have $h = 1$ and must examine the case $q \equiv 3 \pmod 8$. The inequality (26) gives the possibilities:

$a^2 = 1$, $a^2 = 9$ and $a^2 = 25$. The corresponding values of y^q are 29, 37 and 53 respectively.

We make now use of the formula

$$(x + y)^q - x^q - y^q = qxy(x + y)(x^2 + xy + y^2)^r \cdot Q(u, v) ,$$

where $q > 3$ and

$$u = (x^2 + xy + y^2)^3 , \qquad v = (xy(x + y))^2 ,$$
$$r = 2 \quad \text{for } q \equiv 1 \pmod 3$$

and $r = 1$ for $q \equiv 2 \pmod 3$, and $Q(u, v)$ is a polynomial in u and v with integral coefficients [1]. Putting $x = \lambda$, $y = -\lambda'$, we obtain

$$(\lambda - \lambda')^{q-1} - \frac{\lambda^q - \lambda'^q}{\lambda - \lambda'} = -q\lambda\lambda'(\lambda^2 - \lambda\lambda' + \lambda'^2)^r \cdot Q(u, v) ,$$

or

$$(16D)^{q'} \equiv 1 \pmod{q\cdot(a^2 + 4D)\cdot(a^2 - 12D)} , \qquad q' = \frac{1}{2}(q - 1) . \tag{28}$$

If $a^2 = 1$ we get $112^{q'} \equiv 1 \pmod{29}$, or $2^{q-1} \equiv -1 \pmod{29}$. Since $2^{14} \equiv -1 \pmod{29}$ and $2^s \not\equiv -1 \pmod{14}$ for $0 \leqq s < 14$, we must have $q \equiv 1 \pmod{14}$, which implies $(q/7) = 1$. From (28) we further find $112^{q'} \equiv 1 \pmod q$, i.e.

$$1 = \left(\frac{112}{q}\right) = \left(\frac{7}{q}\right) = -\left(\frac{q}{7}\right) ,$$

a contradiction.

If $a^2 = 9$ we get $112^{q'} \equiv 1 \pmod 5$, or $2^{q'} \equiv 1 \pmod 5$, which is impossible for $q = 8t + 3$.

If $a^2 = 25$ we obtain $112^{q'} \equiv 1 \pmod{53}$, or $6^{q'} \equiv 1 \pmod{53}$. Now 6 belongs to the exponent 26 mod 53, which is impossible since q' is an odd number.

It then remains $q = 3$, where

$$x + 2\sqrt{-7} = (a - 2\sqrt{-7})^3 ,$$

whence $2 = 56 - 6a^2$, i.e. $a^2 = 9$, $x = 225$ and

$$225^2 + 28 = 37^3 .$$

We have then proved:

The diophantine equation $x^2 + 28 = y^z$; $z > 3$ *and odd, has no solutions in integers* x, y *and* z *if* y *is an odd integer. If* $n = 3$ *there are exactly two solutions, namely* $x = \pm 225$ *and* $y = 37$.

This is a comprehensive generalization of a result obtained by D. J. Lewis [2].

Example 2. $x^2 + 12 = y^q$. Here is $h = 1$, and (26) gives $a^2 = 1$ or $a^2 = 9$. The last possibility must be excluded, giving $y \equiv 0 \pmod 3$. If $q > 3$ it follows from (27)

$$48^{q'} \equiv 1 \pmod{13} ,$$

or

$$2^{q-1} \equiv -1 \pmod{13}$$

implying $q \equiv 1 \pmod 6$, or $(q/3) = 1$. But according to (12) $(-3/q) = -1$, or $(q/3) = 1$, a contradiction. It is further known that $x^2 + 12 = y^3$ has no integral solution. This may be shown in the following manner:

1° y odd. We write our equation in the form

$$x^2 + 4 = (y - 2)(y^2 + 2y + 4)$$

Since $(x, 2) = 1$, all prime factors of $x^2 + 4$ must be of the form $4t + 1$. Consequently, $y \equiv 3 \pmod 4$. But this implies that $y^2 + 2y + 4 \equiv 3 \pmod 4$, which clearly is impossible.

2° y even. Then x must be even, and putting $x = 2x_1$, $y = 2y_1$ we get

$$x_1^2 + 3 = 2^{q-2} y_1^q$$

which is impossible modulo 8, because $q \neq 4$.

Then we have proved:

The diophantine equation $x^2 + 12 = y^n$, $n > 1$ *and odd, has no solutions in rational integers* x *and* y.

4. The equation $Cx^2 + DM^2 = y^n$, y **odd**, $(x, y) = 1$. Let M denote any positive integer, such that $(C, M) = 1$. In order to find criteria for the solvability of the equation

$$Cx^2 + DM^2 = y^n , \quad n > 1, \ y \text{ odd and } (x, y) = 1 , \tag{29}$$

similar to those obtained in the previous sections, we are again led to deal with an expression of the type

$$(30) \qquad x\sqrt{C} + M\sqrt{-D} = \left(\frac{1}{2}(a_2\sqrt{C} + b_2\sqrt{-D})\right)^q , \qquad a_2 \equiv b_2 \pmod 2 ,$$

q denoting an odd prime. From (29) it follows

$$(31) \qquad 2^q \cdot M = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} a_2^{q-1-2r} \cdot b_2^{2r+1} \cdot C^{(q-1)/2} \cdot (-D)^r .$$

It is easily seen that

$$(32) \qquad b_2 \mid M .$$

If $(Db, q) = 1$, we find, treating (31) as a congruence

$$2M \equiv \left(\frac{-D}{q}\right) b_2 \pmod q ,$$

from which we conclude

$$(33) \qquad q \mid 2M \pm b_2 .$$

According to (32) and (33) there are only a finite number of possibilities for b_2 and for the primes q if $b_2 \neq 2M(-D/q)$. It then only remains to consider the case

$$b_2 = 2M\left(\frac{-D}{q}\right) ,$$

where (30) can be written

$$(34) \qquad x\sqrt{C} + \sqrt{-DM^2} = (a\sqrt{C} + b\sqrt{-DM^2})^q ,$$

and

$$b = \left(\frac{-D}{q}\right) .$$

But now we can utilize the results obtained for $M = 1$.

Example.

$$x^2 + 63 = y^n , \quad y \text{ odd}, \ n > 1.$$

If $(x, y) = 1$ we solve

$$x + 3\sqrt{-7} = \left(\frac{a_2 + b_2\sqrt{-7}}{2}\right)^q .$$

Here we have $y = (a_2^2 + 7b_2^2)/4$, i.e. a_2 and b_2 are even integers because y is odd. This gives

$$x + 3\sqrt{-7} = (a + b\sqrt{-7})^q \tag{35}$$

with $b = \pm 1$ or $b = \pm 3$. It is obvious that $q \neq 7$, such that $3 \equiv b(-7/q) \pmod q$. This implies $b^2 = 1$. For $q = 3$ equation (35) is impossible mod 9. Then we must have $b = 3(-7/q)$. Since y is odd, a must be even, and from (34) we conclude $(-7/q) = 1$ and

$$1 = \binom{q}{1}a^{q-1} - \binom{q}{3}a^{q-3}\cdot 7\cdot 3^2 + \cdots + \binom{q}{q}(-7)^{(q-1)/2}\cdot 3^{q-1}\,. \tag{36}$$

Since $q \equiv 1 \pmod 3$ and $a^2 \equiv 1 \pmod 3$, it can be shown that (36) is impossible, exactly in the same way as we earlier proved the impossiblity of (10), exchanging only the prime 2 by the prime 3. Our equation is then impossible if $(x, y) = 1$. If $(x, y) = 3$ we get, putting $x = 3x_1$, $y = 3y_1$

$$x_1^2 + 7 \equiv 3^{n-2}y^n \equiv 0 \pmod 3\,,$$

which is impossible. Then we have proved:

The diophantine equation $x^2 + 63 = y^n$ is impossible in integers x, y if y is odd and $n > 1$ is an odd number.

5. Remark on earlier results. The diophantine equation

$$ax^2 + bx + c = dy^n\,, \tag{37}$$

where the left-hand side is an irreducible polynomial of the second degree, having integral coefficients and d is an integer $\neq 0$, has only a finite number of solutions in rational integers x, y when $n \geqq 3$. This was first shown by A. Thue and later on by Laundau and Ostrowski. See for instance [7]. However, no general method is known for determining all integral solutions x and y for a given equation of the form (37).

Equation (1) was solved completely by T. Nagell in case y odd, C arbitrary and $D = 1, 2$ or 4 [9]. Nagell has also examined equation 1 when $C = 1$ and D a square-free integer congruent to 1 or 2 modulo 4, but the results obtained are far from being complete [6]. He has further found interesting theorems concerning the equation $x^2 + 8D = y^n$, $(D, 2) = 1$ [8]. The first complete solution of the equation $x^2 + 2 = y^n$ was given by Ljunggren [3]. An upper bound for the number of solutions of (1), in terms of D and n, was derived by Stolt [11]. It must be emphasized that we in this note have deduced *bounds which are independent of n*. For other equations of the type (1) see [9].

If y is odd, but the classnumber h is divisible by n, we have to deal with *irreducible* binary forms of degree $n \geqq 3$. This occurs also if y is even. The problem of representation of rational integers by such forms is not solved. For the determination of an upper bound for the number of solutions of our equations in these cases compare [2], p. 1075.

REFERENCES

1. L. E. Dickson, *History of the theory of numbers*, Vol. II, N. Y. (1952), p. 748.

2. D. J. Lewis, *Two classes of diophantine equations*, Pacific J. Math., **11** (1961), 1063-1076.

3. W. Ljunggren, *Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen*, Arkiv för Mat., Astronomi och Fysik, v. 29 A, N : o 13, Stockholm (1943), 1-11.

4. ———, *On a diophantine equation*, Kong. Norske Videnskabers Selskab Forhandl. v. 18, Nr. 32, Trondheim (1945), 125-128.

5. ———, *New theorems concerning the diophantine equation* $Cx^2 + D = y^n$, Kong. Norske Videnskabers Selskab Forhandl., v. 29, Nr. 1, Trondheim (1956), 1-4.

6. T. Nagell, *Sur l'impossibilité de quelques équations à deux indeterminées*, Norsk Mat. Forenings Skrifter, Ser. I. Nr. 13, Oslo (1923).

7. ———, *L'analyse indeterminée à degré superieure*, Mem. Sci. Math., Fasc 39, Paris 1929.

8. ———, *On the diophantine equation* $x^2 + 8D = y^n$, Arkiv för Mat., v. 3, nr. 6, Stockholm (1955), 103-112.

9. ———, *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*, Nova Acta Reg. Soc. Upsal. IV Ser. 16, Uppsala 1955, p. 1-38.

10. Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8de Skand. Mat. Kongr. Förh., Stockholm (1934), 163-188.

11. B. Stolt, *Über einen verallgemeinerten Fermatschen Satz*, Acta aritmetica, **5** (1959), 267-276.