Some remarks on Stolt's Theorems for Pellian Equations

PETER HEICHELHEIM

Toronto, Canada

Abstract

One of the theorems of Bengt Stolt's article »On the Diophantine Equation $u^2 - Dv^2 = 4N$» is not quite correct in its entirety. A counter-example will be given to show this. A modification of the theorem which he was trying to prove will be given for certain special cases.

1. Introduction

Here is a summary of some of the definitions and theorems given in Stolt [1].

All integer solutions (x, y) of

$$x^2 - Dy^2 = 4 \tag{1}$$

for $D > 0$ and not a square are given by

$$\frac{x + \sqrt{D}y}{2} = \pm\left(\frac{x_1 + \sqrt{D}y_1}{2}\right)^i$$

where i is any integer and (x_1, y_1) is the smallest positive solution of (1).

Let (u^*, v^*) be any integer solution of

$$u^2 - Dv^2 = 4N \tag{2}$$

for $D > 0$ and not a square.

Then a *class of solutions* of (2) consists of all solutions (u, v) such that

$$\frac{u + \sqrt{D}v}{2} = \pm\left(\frac{u^* + \sqrt{D}v^*}{2}\right)\left(\frac{x_1 + \sqrt{D}y_1}{2}\right)^i.$$

All solutions of (2) can be divided into a finite number of classes of solutions. Two solutions which belong to the same class of solutions are called associated.

A simple criteria to see if two solutions (u, v) and (u', v') are associated is if $(uv' - u'v)/2N$ is an integer.

In every class of solutions of (2) it is well known that there is at least one solution (u, v) such that

$$0 \leq v \leq \frac{y_1 \sqrt{|N|}}{\sqrt{x_1 + 2N/|N|}} \tag{3}$$

and $0 \leq |u| \leq \sqrt{(x_1 + 2N/|N|)|N|}$.

In [1] Stolt claims to prove that if N is square-free then the number of classes of solutions is a *power of two*. However $u^2 - 79v^2 = 4(3)(5)(7)(13)$ has *six* classes of solutions. The next section will give details of this.

2. Details of counter-example

THEOREM 1. *The equation* $u^2 - 79v^2 = 4(1365) = 4(3)(5)(7)(13)$ *has six classes of solutions.*

Proof. In every class of solutions of $u^2 - 79v^2 = 4(1365)$ there will be at least one solution (u, v) such that

$$0 \leq v \leq 18\sqrt{1365}/\sqrt{160+2} = 2\sqrt{1365/2} = \sqrt{2730} < 53.$$

Table

v	u^2	v	u^2	v	u^2
1	5 539	19	33 979	37	113 611
2	5 776 $= (76)^2$	20	37 060	38	119 536
3	6 171	21	40 299	39	125 619
4	6 724 $= (82)^2$	22	43 696	40	131 860
5	7 435	23	47 251	41	138 259
6	8 304	24	50 964	42	144 816
7	9 331	25	54 835	43	151 531
8	10 516	26	58 864	44	158 404 $= (398)^2$
9	11 859	27	63 051	45	165 435
10	13 360	28	67 396	46	172 624
11	15 019	29	71 899	47	179 971
12	16 836	30	76 560	48	187 476
13	18 811	31	81 379	49	195 139
14	20 944	32	86 356	50	202 960
15	23 235	33	91 491	51	210 939
16	25 684	34	96 784	52	219 076
17	28 291	35	102 235		
18	31 056	36	107 844		

Inspection of the table of squares in Barlow's Tables and the above table show that the only solutions of $u^2 - 79v^2 = 4(1365)$ such that $0 \leq v < 53$ are $(u, v) = (76,2), (-76,2), (82,4), (-82,4), (398,44)$, and $(-398,44)$. As none of these solutions are associated with each other, then the number of classes of solutions is six.

3. Number of classes of solutions in special cases

Details on the theory of ideals and algebraic integers in the quadratic case are given in Stolt [1] and Hancock [2].

THEOREM 2. *Let*

$$u^2 - Dv^2 = +4\prod_{i=1}^{n} p_i \tag{4}$$

or

$$u^2 - Dv^2 = -4\prod_{i=1}^{n} p_i \tag{5}$$

where D is square-free and the p_i's are distinct primes. At least one of (4) *or* (5) *is solvable in integers.*

Let C_1, C_2 be the number of classes of solutions of (4) *and* (5) *respectively.*

In the field $K(\sqrt{D})$ the ideal (p_i) equals $q_i q_i'$ where q_i and q_i' are prime conjugate ideals for all i. Let $q_i \neq q_i'$ for $i = 1, \ldots, l$ and $q_i = q_i'$ for $i = l+1, \ldots, n$. Choose $r_i = q_i$ or q_i'.

Let S be the number of ways the set $(r_1, r_2, \ldots, r_l)$ can be chosen so that $\prod_{i=1}^{l} r_i$ is a principal ideal.

Then $S = C_1 = C_2$ if $x^2 - Dy^2 = -4$ is solvable,
$S = C_1 + C_2$ otherwise.

Proof. Suppose (α) is a principal ideal such that $(N) = (\alpha)(\alpha')$ where (α') is the conjugate of (α). Then it is easy to see that any class of solutions of (4) will correspond to one and only one principal ideal (α). Also two different classes of solutions of (4) will correspond to two different principal ideals (α). The same is true for (5).

As $(N) = (\alpha)(\alpha') = (\alpha\alpha')$ then $\alpha\alpha' = N$ or $\alpha\alpha' = -N$ where α and α' are algebraic integers which are generators of (α) and (α') respectively. This shows that every (α) corresponds to a class of solutions of (4) or of (5) or of both. But it is easily shown that (α) corresponds to a class of solutions of both (4) and (5) if and only if $x^2 - Dy^2 = -4$ is solvable.

Therefore the theorem is true since (α) equals $\prod_{i=1}^{n} r_i$ uniquely for exactly one set $(r_1, \ldots, r_n)$ and hence for exactly one set $(r_1, \ldots, r_l)$.

Comment. The above theorem shows how the evaluation of the number of classes of solutions becomes a combinatorial problem.

A case where both equations (4) and (5) are solvable while $x^2 - Dy^2 = -4$ is not, is given by $u^2 - 34v^2 = +4(3)(5)$ and $u^2 - 34v^2 = -4(3)(5)$. Now the only values of (u, v) satisfying (3) for $u^2 - 34v^2 = +4(3)(5)$ and $u^2 - 34v^2 = -4(3)(5)$ are (14,2), (— 14,2) and (22,4), (— 22,4) respectively. As neither pair of solutions is associated in this case, $C_1 = 2$ and $C_2 = 2$. This is somewhat different from that indicated in Stolt [1], page 119—120.

4. Evaluation of S for the class-number of $K(\sqrt{D}) \leq 6$

It is well known that all ideals in $K(\sqrt{D})$ can be divided into a finite number of equivalence classes. The set of these equivalence classes is an abelian group under multiplication. If two ideals q_1 and q_2 are in the same equivalence class then $q_1 \sim q_2$.

THEOREM 3. *Suppose S is defined as in Theorem 2 and the class-number h of $K(\sqrt{D}) \leq 6$ where either (4) or (5) is solvable. Then the formulae given in sections A to E below are true.*

Comment. Proofs will be given only for the cases $h \leq 3$.

A. All ideals $q_i \sim q_i'$. (This includes $h = 1, 2$ and $h = 4$ (Non-cyclic group).) Then $S = 2^l$.

Proof. All combinations $(r_1, r_2, \ldots, r_l)$ make $\prod_{i=1}^{l} r_i$ a principal ideal.

B. $h = 3$.

Let $q_i \not\sim q_i'$ for $i = 1, \ldots, l_1$ and $q_i \sim q_i'$ for $i = l_1 + 1, \ldots, l$.

Then $S = 2^{l-l_1}(2^{l_1} + 2(-1)^{l_1})/3$.

Proof. Let S_1 be the number of combinations $(r_1, r_2, \ldots, r_{l_1})$ such that $\prod_{i=1}^{l_1} r_i$ is a principal ideal.

Now $\prod_{i=1}^{l_1} r_i \sim q_1^k q_1'^{l_1-k} \sim q_1^{2l_1-k}$ (where k is the number of r_i equivalent to q_1).

Therefore $\prod_{i=1}^{l_1} r_i$ is a principal ideal if and only if $2l_1 - k \equiv 0 \bmod 3$.

Let b be the smallest non-negative value of k.

Therefore

$$
\begin{aligned}
S_1 &= \binom{l_1}{b} + \binom{l_1}{b+3} + \binom{l_1}{b+6} + \cdots \\
&= \frac{1}{3}\sum_{j=0}^{2}\left(2\cos\frac{j\pi}{3}\right)^{l_1}\cos\left(\frac{(l_1-2b)j\pi}{3}\right)
\end{aligned}
\tag{6}
$$

by Riordan [3].

Since $l_1 - 2b \equiv 2(2l_1 - b) \equiv 0 \bmod 3$,

$$l_1 \equiv l_1 - 2b \bmod 2, \cos \pi/3 = 1/2, \quad \text{and} \quad \cos 2\pi/3 = -1/2$$

then it can be shown by substitution in (6) that $S_1 = (2^{l_1} + 2(-1)^{l_1})/3$.

To complete the proof of the theorem it only remains to be seen that the number of combinations $(r_{l_1+1}, \ldots, r_l)$ such that $\prod_{i=l_1+1}^{l} r_i$ is a principal ideal is 2^{l-l_1}.

C. $h = 4$ *(Cyclic Group)*.
Suppose $q_i \not\sim q_i'$ for $i = 1, \ldots, l_1$ and $q_i \sim q_i'$ for $i = l_1 + 1, \ldots, l$.
Then $S = 2^{l-1}$ if $l_1 > 0$, $= 2^l$ if $l_1 = 0$.

D. $h = 5$.
Suppose $q_i \not\sim q_i'$ and $q_i \sim q_1$ or q_1^4 for $i = 1, \ldots, l_1$, $q_i \sim q_1^2$ or q_1^3 for $i = l_1 + 1, \ldots, l_1 + l_2$, $q_i \sim q_i'$ for $i = l_1 + l_2 + 1, \ldots, l$.
Then

$$S = 25^{-1} 2^{l-l_1-l_2}[5 \cdot 2^{l_1+l_2} + 2(-1)^{l_1+l_2}(2L_{l_1}L_{l_2} - L_{l_1+1}L_{l_2-1} - L_{l_1-1}L_{l_2+1})],$$

where $L_{-1} = -1$, $L_0 = 2$, $L_k = L_{k-1} + L_{k-2}$, $k = 1, 2, \ldots$

E. $h = 6$.
$q_i \not\sim q_i'$ and $q_i^2 \not\sim q_i'$ for $i = 1, \ldots, l_1$,
$q_i \not\sim q_i'$ and $q_i^2 \sim q_i'$ for $i = l_1 + 1, \ldots, l_1 + l_2$,
$q_i \sim q_i'$ for $i = l_1 + l_2 + 1, \ldots, l$.
Then $S = 3^{-1} 2^{l-l_1-l_2}(2^{l_1+l_2} + 2(-1)^{l_1+l_2})$.

Acknowledgement. I wish to thank Professor J. H. H. Chalk for the help he has given me in the preparation of this paper.

References

1. Stolt, B., On the diophantine equation $u^2 - Dv^2 = \pm 4N$, Part III, *Ark. Mat.*, 3 (1954), 117–132.
2. Hancock, *Foundations of the Theory of Algebraic Numbers*, Vol. I, New York, 1931.
3. Riordan, *An Introduction to Combinatorial Analysis*, New York, New York, 1958, page 41.

Received August 1, 1973

Peter Heichelheim
666 Spadina Avenue
Apartment PH9
Toronto, Ontario
Canada