CONDITIONS FOR THE SOLUBILITY OF THE DIOPHANTINE EQUATION $x^2-My^2=-1$[*]

BY

MORGAN WARD

1. In this paper I apply the theory of Lucas' functions[†] to determine conditions[‡] under which the well known diophantine equation

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

is soluble for given integers[§] N and D.

I show first of all that it is sufficient to consider (1) in the case when N is an odd prime P and D is square-free and not divisible by P. Suppose that $N=P$. Clearly, a necessary condition that (1) be soluble is that the equation

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

be soluble. If D is not a quadratic residue of P, this condition is also sufficient for the solubility of (1). However, if D is a quadratic residue of P, the following additional restriction must hold.

Let (u, v) be the least positive integral solution of (2), and suppose that P is of the form $2^{k+1}(2M+1)+1$ with[¶] $(D\,|P)=+1$. Then in order that (1) be soluble it is necessary and sufficient that

$$(u + vD^{1/2})^{(P-1)/2^k} \equiv -1 \pmod{P}. \tag{3}$$

In case P is of the form $8M+5$, (3) may be replaced by the following condition. Let

$$P = (a + bi)(a - bi),\quad u + i = \epsilon\zeta\prod(\alpha + \beta i) \qquad (a,\ \alpha \text{ odd})$$

be the decomposition of P and $u+i$ into primary factors in the field $\mathfrak{F}(i=(-1)^{1/2})$. Here ζ is equal to 1 or $1+i$ according as the norm of $u+i$ is odd or even, and ϵ is a unit chosen so that the integers α are all odd. Then a necessary and sufficient condition that (1) be soluble is that

$$\prod(a + bi\,|\,\alpha + \beta i) = (\epsilon\zeta\,|\,a + bi). \tag{4}$$

[*] Presented to the Society, April 11, 1931; received by the editors March 3, 1931.

[†] A recent paper by D. H. Lehmer, Annals of Mathematics, (2), vol. 31 (1930), pp. 419–448, gives references to the literature on these functions.

[‡] Very few general conditions are known. See Dickson's *History*, vol. 2, chapter XII.

[§] On considering (1) modulo 8, it is obvious that N must be odd and D or $D/2$ odd for a solution to exist. Furthermore, every odd prime factor of N^2D must be of the form $4n+1$.

[¶] $(A\,|B)$ denotes as usual the quadratic character of A with respect to B.

If P is of the form $8M+1$, this condition is necessary, but not sufficient, for the solubility of (1).

For a given value of D, (4) gives an easily applied criterion for the solubility of (1). Its use is illustrated in the closing sections of the paper for the case $D=5$.

2. To prove these statements, consider equations (1) and (2), where we assume that (2) is soluble and that N is odd. If (u, v) is the least positive integral solution of (2), every other solution is given by the formula

$$r_n + D^{1/2}s_n = (u + vD^{1/2})^n \qquad (n = \pm 1, \pm 3, \pm 5, \cdots).$$

Hence a necessary and sufficient condition that (1) be soluble is that there exist an odd n such that

$$s_n \equiv 0 \pmod{N}.$$

Now let $\gamma = u+vD^{1/2}$, $\delta = u-vD^{1/2}$ so that $\gamma+\delta = 2u$, $\gamma-\delta = 2vD^{1/2}$, $\gamma\delta = -1$. Then $r_n+s_nD^{1/2} = \gamma^n$, $r_n-s_nD^{1/2} = \delta^n$ so that $2r_n = V_n$, $s_n = vU_n$ where

$$V_n = \gamma^n + \delta^n, \quad U_n = \frac{\gamma^n - \delta^n}{\gamma - \delta}$$

are the Lucas functions associated with the quadratic equation

$$x^2 - 2ux - 1 = 0.$$

Thus if $N = md$, $v = v'd$, $(m, v') = 1$, $s_n \equiv 0 \pmod{N}$, when and only when $U_n \equiv 0 \pmod{m}$.

Now let $\mu(m)$ denote the least positive value of n such that $U_n \equiv 0$ (mod m). We shall refer to this number as the rank of apparition of m in $(U)_n$. Its more important properties are as follows:*

I. *U_n is divisible by m when and only when n is divisible by $\mu(m)$.*

II. *If a and b are co-prime, $\mu(ab)$ is the least common multiple of $\mu(a)$ and $\mu(b)$. Consequently*

III. *If $m = p_1^{a_1}, \cdots, p_k^{a_k}$ is the decomposition of m into its prime factors, then $\mu(m)$ is the least common multiple of $\mu(p_1^{a_1}), \cdots, \mu(p_k^{a_k})$.*

IV. *If m is a prime p, and $(D|p)$ denotes the quadratic character of D with respect to p, then $\mu(p)$ divides $p-(D|p)$ and $\mu(p^a) = p^b\mu(p)$, $b \leqq a-1$.*

V. *If m is odd, $\mu(m)$ is odd when and only when all of the V_n are prime to m.*

The first property of $\mu(m)$ gives us immediately the following theorem.

* D. H. Lehmer paper cited.

THEOREM. *If (u, v) is the least positive integral solution of*

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

and $N = md$, $v = v'd$; N odd and $(m, v') = 1$, then a necessary and sufficient condition that the equation

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

be soluble is that the rank of apparition of m in the Lucas function $(U)_n$ associated with the quadratic equation $x^2 - 2ux - 1 = 0$ be odd.

3. The question of the solubility of (1) is thus reduced to the problem of determining the parity of $\mu(m)$ for any odd m. It follows from III and IV that if

$$m = p_1^{a_1} \cdots p_k^{a_k}$$

is the decomposition of m into its prime factors, $\mu(m)$ is odd when and only when $\mu(p_1), \cdots, \mu(p_k)$ are all odd. Since if p divides D, $(D|p) = 0$ and $\mu(p)$ divides p, we can assume that m is prime to D.

Thus it is sufficient to discuss the solubility of (1) when D is square-free, and N is a prime P of the form $4n+1$ not dividing vD. We shall therefore replace (1) by

$$x^2 - P^2Dy^2 = -1, \ (P, vD) = 1, \ P \text{ a prime, } D \text{ square-free,} \tag{5}$$

where

$$P = 2^{k+1}(2M + 1) + 1, \ k \geqq 1. \tag{6}$$

From V we have immediately the following theorem.

THEOREM. *If $x^2 - Dy^2 = -1$ is soluble, and P is an odd prime, then at most one of the equations*

$$x^2 - P^2Dy^2 = -1, \ P^2x^2 - Dy^2 = -1$$

is soluble.

Suppose that $(D|P) = -1$. Since $(P+1)/2$ is odd, we see from IV that $\mu(P)$ is odd when and only when $\mu(P)$ divides $(P+1)/2$; that is, when and only when

$$U_{(P+1)/2} \equiv 0 \pmod{P}. \tag{7}$$

Referring back to the equations in §2 defining U_n, we see that (7) holds when and only when the congruence

$$\gamma^{P+1} \equiv -1 \pmod{P}$$

holds in the Galois field of order P^2 associated with the root γ of $x^2-2ux-1=0$. But

$$\gamma^{P+1} = (u + vD^{1/2})^{P+1} \equiv u^{P+1} + v^{P+1}D^{(P+1)/2} \equiv u^2 - Dv^2 \equiv -1 \pmod{P}.$$

We thus have established the following result:

THEOREM. *If P is a prime of the form $4n+1$ such that $(D|P)=-1$, the diophantine equation $x^2-P^2Dy^2=-1$ is soluble when and only when the diophantine equation $x^2-Dy^2=-1$ is soluble.*

4. The case when $(D|P)=+1$ is considerably more difficult. Since $(P-1)/2^{k+1}$ is odd, $\mu(P)$ is odd when and only when $\mu(P)$ divides $(P-1)/2^{k+1}$. This condition is easily shown to be equivalent to the criterion stated in §1,

$$(3) \qquad (u + vD^{1/2})^{(P-1)/2k} \equiv -1 \pmod{P}.$$

It is now necessary to discuss separately the increasingly more complicated cases* $k=1, 2, 3, 4, \cdots$, corresponding to primes of the form $8n+5$, $16n+9$, $32n+17$, $64n+33$, $\cdots$.

I shall confine myself here to the simplest case $k=1$ where the criterion (3) can be put into a much more manageable form.

Suppose then that

$$(8)\ (u + vD^{1/2})^{(P-1)/2} \equiv -1 \pmod{P}, \text{where } P = 8M + 5 \text{ and } (D|\,P) = +1.$$

(8) is equivalent to saying that the congruences

$$(8.1) \qquad x^2 \equiv u + vD^{1/2}, \quad \bar{x}^2 \equiv u - vD^{1/2} \pmod{P}$$

have no solutions. Now let

$$x = \kappa + \lambda D^{1/2}, \quad \bar{x} = \kappa - \lambda D^{1/2}.$$

Then the congruences (8.1) are insoluble when and only when the congruences

$$\kappa^2 + \lambda^2 D \equiv u, \quad 2\kappa\lambda \equiv v, \quad u^2 - v^2 D \equiv -1 \pmod{P}$$

are insoluble. On eliminating λ and v, we obtain

$$(2\kappa^2 - u)^2 + 1 \equiv 0 \pmod{P}.$$

Hence if $w^2 \equiv -1 \pmod{P}$, $4\kappa^2 \equiv 2(u \pm w) \pmod{P}$. On recalling that P is of the form $8M+5$, we see that the congruences (8. 1) are insoluble when and only when the congruence

$$z^2 \equiv u \pm w \pmod{P}$$

* For the case $k=2$, $D=2$, $u=v=1$, see a paper by Perott, *Sur l'équation $t^2-Du^2=-1$*, Crelle's Journal, vol. 102 (1888), pp. 185–223.

is soluble. Since $(u+w)(u-w)\equiv u^2+1\equiv v^2D$ (mod P), $u+w$ and $u-w$ have the same quadratic character modulo P. Hence a necessary and sufficient condition that (8) should hold is that

$$(9)\qquad \left(\frac{u+w}{P}\right)=+1 \text{ where } w^2\equiv -1 \pmod{P}.$$

By passing into the field $\mathfrak{F}(i)$, $i^2=-1$, we can apply the reciprocity law* to simplify the criterion (9). Suppose that

$$P=(a+bi)(a-bi),\ a \text{ odd},$$

is the decomposition of P into primary factors in $\mathfrak{F}(i)$.

Since

$$(u+i\,|\,a-bi)=(u-i\,|\,a+bi) \quad\text{and}\quad (u+i\,|\,a+bi)=(u-i\,|\,a+bi),$$

a necessary and sufficient condition that (9) should hold is that

$$(10)\qquad (u+i\,|\,a+bi)=+1.$$

Let

$$u+i=\epsilon\zeta\prod(\alpha+\beta i)$$

be the decomposition of $u+i$ into primary factors in $\mathfrak{F}(i)$ where $\zeta=1$ or $1+i$ according as the norm of $u+i=v^2D$ is even or odd and ϵ is a unit so chosen that the α are all odd. Then by the reciprocity law in $\mathfrak{F}(i)$,

$$(u+i\,|\,a+bi)=(\epsilon\zeta\,|\,a+bi)\prod(a+bi\,|\,\alpha+\beta i).$$

If P is a prime of the form $8n+1$ and $(D\,|P)=+1$, we see from (3) of the previous theorem that a necessary condition that $x^2-P^2Dy^2=-1$ be soluble is that

$$(u+vD^{1/2})^{(P-1)/2}\equiv 1 \pmod{P}.$$

On proceeding as in the previous case, we find that this condition is again equivalent to the criterion

$$(u+i\,|\,a+bi)=+1.$$

Hence we have the following theorem.

THEOREM. *Let* (u, v) *be the least positive integral solution of the diophantine equation*

$$(2)\qquad x^2-Dy^2=-1$$

and let P *be a prime of the form* $4n+1$ *such that* $(D\,|P)=+1$, $(v, P)=1$.

* Bachmann, *Kreistheilung*, Lecture 13.

Then if

$$P = (a + bi)(a - bi),\ u + i = \epsilon\zeta \prod(\alpha + \beta i)$$

(a, α *odd*; ϵ *a unit*; $\zeta = 1$ *or* $1+i$) ***are the decompositions of*** P ***and*** $u+i$ ***into primary factors in the field*** $\mathfrak{F}(i)$, ***a necessary condition that the diophantine equation***

$$(5) \qquad x^2 - P^2Dy^2 = -1$$

be soluble is that

$$(4) \qquad \prod(a + bi|\alpha + \beta i) = (\epsilon\zeta|a + bi).$$

If P ***is of the form*** $8M+5$, ***this condition is also sufficient for the solubility of*** (5).

5. We shall now apply our results to the case $D=5$. Here $u=2$, $v=1$ so that the norm of $u+i=5$, and $\alpha=1$, $\beta=-2$, $\zeta=1$, $\epsilon=i$. (4) becomes simply

$$(a + bi|\,1 - 2i) = (i|\,a + bi)\begin{cases} = -1,\ P \equiv 5 & (\text{mod } 8), \\ = +1,\ P \equiv 1 & (\text{mod } 8). \end{cases}$$

We easily find that the square of any integer in $\mathfrak{F}(i)$ is congruent modulo $1-2i$ to 0, ± 1 or $\pm 2i$; morever since $P=a^2+b^2$ is a quadratic residue of 5, we must have either $a\equiv 0$ or $b\equiv 0$ (mod 5). Hence

$$(a + bi|\,1 - 2i) = +1\begin{cases} b \equiv 0,\ a \equiv \pm 1,\ P \equiv 1 & (\text{mod } 5), \\ a \equiv 0,\ b \equiv \pm 2,\ P \equiv 4 & (\text{mod } 5), \end{cases}$$

$$(a + bi|\,1 - 2i) = -1\begin{cases} b \equiv 0,\ a \equiv \pm 2,\ P \equiv 4 & (\text{mod } 5), \\ a \equiv 0,\ b \equiv \pm 1,\ P \equiv 1 & (\text{mod } 5). \end{cases}$$

Now every odd prime save 5 must belong to one of the forms

$$40n + 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.$$

Hence if P is of the form

$$40n + 3, 7, 11, 19, 23, 27, 31, 39,$$

the diophantine equation

$$(11) \qquad x^2 - 5P^2y^2 = -1$$

is insoluble, since $P\equiv 3$ (mod 4), while if P is of the form

$$40n + 13, 17, 33, 37,$$

(11) is soluble since P is then a non-residue of 5.

There are left primes of the forms

$$40n + 21,\ 40n + 29 \text{ and } 40n + 1,\ 40n + 9$$

congruent to 5 and 1 modulo 8 respectively. For such primes, we have from the results just given the following remarkable theorem:

THEOREM. *Let $P=a^2+b^2$ be the representation of any prime of the forms* $40n+1$, 9, 21, 29 *as the sum of two squares, where a is assumed to be odd. Then a necessary condition that the diophantine equation*

$$x^2-5P^2y^2=-1 \tag{11}$$

be soluble is given by the following table:

Residue of P (mod 40)	*Criterion for solubility*
1	$b\equiv 0 \pmod 5$
9	$a\equiv 0 \pmod 5$
21	$a\equiv 0 \pmod 5$
29	$b\equiv 0 \pmod 5$.

In the last two cases, this criterion is also sufficient for the solubility of (11).

In the concluding table, we apply this theorem to all the primes of the four forms considered less than 1000. Soluble cases are marked with S, insoluble with I and doubtful with ?. In conjunction with our previous results, we see that for the 168 primes <1000, we are left in doubt as to the solubility of (11) only in the six cases $P=89$, 401, 521, 761, 769 and 809.

Table of Primes of the Form $40n+1$, 9, 21, 29 Less than a Thousand

$P=40n+1$	a^2+b^2, a odd	$5P^2$		$P=40n+9$	a^2+b^2, a odd	$5P^2$	
41	5^2+4^2	8405	I	89	5^2+8^2	39605	?
241	15^2+4^2	290405	I	409	3^2+20^2	836405	I
281	25^2+4^2	394805	I	449	7^2+20^2	1008005	I
401	1^2+20^2	804005	?	569	13^2+20^2	1618805	I
521	11^2+20^2	1357205	?	769	25^2+12^2	2956805	?
601	5^2+24^2	1806005	I	809	5^2+28^2	3272405	?
641	25^2+4^2	2054405	I	929	23^2+20^2	4315205	I
761	19^2+20^2	2895605	?				
881	25^2+16^2	3880805	I				
$P=40n+21$				$P=40n+29$			
61	5^2+6^2	18605	S	29	5^2+2^2	4205	I
101	1^2+10^2	51005	I	109	3^2+10^2	59405	S
181	9^2+10^2	163805	I	149	7^2+10^2	111005	S
421	15^2+14^2	886205	S	229	15^2+2^2	262205	I
461	19^2+10^2	1062605	I	269	13^2+10^2	361805	S
541	21^2+10^2	1463405	I	349	5^2+18^2	609005	I
661	25^2+6^2	2184605	S	389	17^2+10^2	756605	S
701	5^2+26^2	2457005	S	509	5^2+22^2	1294055	I
821	25^2+14^2	3370205	S	709	15^2+22^2	2513405	I
941	21^2+20^2	4427405	I	829	27^2+10^2	3436205	S

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.