THE DIOPHANTINE EQUATION $X^2 - DY^2 = Z^M$*

BY
MORGAN WARD

I. Introduction

It has been known since the time of Euler and Lagrange† that solutions of the diophantine equation

$$X^2 - DY^2 = Z^M \tag{1.1}$$

may be obtained by setting

$$X + D^{1/2}Y = (a + D^{1/2}b)^M, \qquad Z = a^2 - Db^2,$$

where a and b are any rational integers. In 1891, Pepin‡ claimed to prove that if M is odd, and prime to the class-number of the quadratic field $\mathfrak{R}(D^{1/2})$ while a and b are co-prime, *all* solutions of (1.1) in which X, Y and Z have no common factor—for short, "primitive" solutions of (1.1)—are given by the formulas above. Later, Pepin§ recognized that Z must be restricted to be odd, while Landau‖ has pointed out (for a special case of (1.1)) that if D is positive, the units of the quadratic field $\mathfrak{R}(D^{1/2})$ must be taken into account.

Consider for example the equation $X^2 - 5Y^2 = Z^3$ to which Pepin's procedure should apply, since M is odd and the class-number of $\mathfrak{R}(5^{1/2})$ is unity. This equation has the primitive solution $X = 2$, $Y = 1$, $Z = -1$. It should therefore be possible to choose rational integers a and b such that

$$2 + 5^{1/2} = (a + 5^{1/2}b)^3, \qquad -1 = a^2 - 5b^2.$$

From the second equation, $a + 5^{1/2}b$ is a unit of $\mathfrak{R}(5^{1/2})$ and hence some power of the fundamental unit η multiplied by plus or minus one. But since the fundamental unit is $2 + 5^{1/2}$, the first equation would imply that $2 + 5^{1/2}$ is a root of unity. To obtain this particular solution, it would suffice to multiply $(a + 5^{1/2}b)^3$ by η^{-2}. But it is not at all obvious that such a device will always prove successful.

In the second part of the paper I utilize the theory of ideals to obtain explicit formulas for all the primitive solutions of (1.1) under the restrictions given below.

* Presented to the Society, December 2, 1933; received by the editors December 26, 1933.

† Dickson's *History*, vol. II, chapter XX.

‡ Memorie della Pontificia Accademia dei Nuovi Lincei, vol. 8 (1891), pp. 41–42.

§ Annales de la Société Scientifique de Bruxelles, vol. 27 (1909), pp. 121–170.

‖ L'Intermédiaire des Mathématiciens, vol. 8 (1901), pp. 145–147.

FUNDAMENTAL THEOREM. *Let D be square-free, not equal to -3 or -1,* and incongruent to 1 modulo 8, and let M be any positive integer greater than one, and prime to the class-number h of the quadratic field $\Re(D^{1/2})$, but not necessarily odd.*

Let a and b be rational integers such that $(a, Db)=1$, and of opposite parity unless the contrary is expressly stated. Define A_M and B_M by

$$(a + bD^{1/2})^M = A_M + D^{1/2}B_M. \tag{1.2}$$

Let $1, \omega$ be the canonical basis of the field $\Re(D^{1/2})$, and if D is positive, let

$$\eta = r + \omega s \tag{1.3}$$

be the fundamental unit of the field. Define U_T and V_T $(T=0, 1, \cdots, M)$ by

$$U_T + D^{1/2}V_T = \eta^T, \quad D \equiv 2, 3\ (4) \text{ or } D \equiv 5\ (8), \quad h \equiv 0\ (3);$$
$$U_T + D^{1/2}V_T = 2\eta^T, \quad D \equiv 5\ (8), \quad h \not\equiv 0\ (3).$$

Then all primitive solutions, and only primitive solutions, of the diophantine equation

$$X^2 - DY^2 = Z^M \tag{1.1}$$

are given by the following formulas.

(I) *D negative.*

$$X = \pm A_M, \qquad Y = \pm B_M, \qquad Z = \pm (a^2 - Db^2).$$

(II) *D positive and either congruent to 2, 3 (4) or congruent to 5 (8) with $h \equiv 0$ (3).*

$$X = \pm (A_M U_T + DB_M V_T), \quad Y = \pm (A_M V_T + B_M U_T), \quad Z = \pm (a^2 - Db^2)$$
$$(T = 0, 1, \cdots, M-1).$$

(III) *D positive, congruent to 5 (8), $h \not\equiv 0$ (3).*

$$2X = \pm (A_M U_{3T} + DB_M V_{3T}), \quad 2Y = \pm (A_M V_{3T} + B_M U_{3T}), \quad Z = \pm (a^2 - Db^2)$$
$$(T = 0, 1, \cdots, [(M-1)/3]).$$

$$2^{M+1}X = \pm (A_M U_T + DB_M V_T), \quad 2^{M+1}Y = \pm (A_M V_T + B_M U_T), \quad 4Z = a^2 - DB^2,$$

a, b both odd. $M + T \equiv 0\ (3)$ if $\dfrac{a+b}{2} + r \equiv 0\ (2)$, and

$$M - T \equiv 0\ (3) \text{ if } \frac{a+b}{2} + r \equiv 1\ (2)$$
$$(T = 0, 1, \cdots, M-1).$$

* The solutions in the cases $D=-1$ or $D=-3$ are well known.

If $M=2$, we have in addition

$$2^M X = \pm (A_M U_T + DB_M V_T), \quad 2^M Y = \pm (A_M V_T + B_M U_T), \quad 2Z = a^2 - Db^2,$$

a, b both odd, $T = 0$ or 1.

In the final part of the paper, these formulas are applied to discuss several allied diophantine equations; notably $X^2+D=Z^M$, $1+DY^2=Z^M$, $X^{2N}-DY^{2N}=Z^N$.

II. The primitive solutions of $X^2-DY^2=Z^M$

1. Let D be a square-free integer not equal to -1 or -3 and incongruent to 1 modulo 8, and let M be an integer $\geqq 2$ and prime to the class-number of the quadratic field $\mathfrak{R}=\mathfrak{R}(D^{1/2})$. A solution $X=A$, $Y=B$, $Z=C$ of the diophantine equation

$$X^2 - DY^2 = Z^M \tag{1.1}$$

will be said to be primitive if A, B, C are rational integers with no common factor save unity. For brevity, we shall speak of "the solution A, B, C."

We shall adhere to the notations of Landau's *Vorlesungen*; italic letters are reserved for rational integers, small Greek letters for integers of the field $\mathfrak{R}$, and small German letters for ideals of $\mathfrak{R}$. A square bracket enclosing a Greek letter denotes the corresponding principal ideal; thus $[\alpha]$, $[\beta]$, $\cdots$. Round parentheses enclosing two or more letters denote greatest common divisors, (a, b), $(\mathfrak{a}, \mathfrak{b})$, $\cdots$; enclosing a single letter, they denote that it is to be used as a modulus. The conjugate of a number α of $\mathfrak{R}$ is denoted by $\bar{\alpha}$.

The following three lemmas are easily proved.

Lemma 1.1. *If A, B, C is a primitive solution of the diophantine equation* (1.1), *then both A, B, C and A, D, C are relatively prime in pairs.*

Lemma 1.2. *If A, B, C is a primitive solution of the diophantine equation* (1.1), *then* (i) *if $M\geqq 3$, C must be odd unless $D\equiv 1$ (8)*; (ii) *if $M=2$, C must be odd unless $D\equiv 1$ or 5 (8). In the latter case, if C is even, $C/2$ must be odd.*

Lemma 1.3. *If M is prime to the class-number of the algebraic field $\mathfrak{R}$, and if $\mathfrak{a}$ is any ideal of $\mathfrak{R}$, then if $\mathfrak{a}^M$ is a principal ideal, $\mathfrak{a}$ is a principal ideal.*

Lemma 1.4. *If A, B, C is a primitive solution of the diophantine equation* (1.1) *and if C is odd, then the principal ideals $[A+D^{1/2}B]$ and $[A-D^{1/2}B]$ of the quadratic field $\mathfrak{R}$ are co-prime.*

For otherwise, there exists a prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ such that

$$[A + D^{1/2}B] \equiv 0 \ (\mathfrak{p}), \qquad [A - D^{1/2}B] \equiv 0 \ (\mathfrak{p}).$$

Then $[C^M]=[A+D^{1/2}B]\ [A-D^{1/2}B]\equiv 0\ (\mathfrak{p})$, so that

$$C \equiv 0\ (\mathfrak{p}),\ \text{and}\ ([2],\ \mathfrak{p}) = 1 \text{ since } C \text{ is odd.}$$

Since $\mathfrak{p}$ contains both $A+D^{1/2}B$ and $A-D^{1/2}B$, it contains their sum $2A$ and hence A itself. Therefore the rational prime which $\mathfrak{p}$ divides divides both A and C contrary to Lemma 1.1.

LEMMA 1.5. *If D is congruent to 5 modulo 8, and if $1, \omega$ is the canonical basis for the integers of the field $\mathfrak{R}$, and if $(c+\omega d)^M = c'+\omega d'$, where c and d are rational integers, then if M is prime to three, d' is even when and only when d is even. If M is divisible by three, d' is always even.*

For $5 \equiv D = (2\omega+1)^2 \equiv 4\omega^2+4\omega+1\ (8)$, so that

$$\omega^2 \equiv \omega + 1\ (2).$$

If d is even, d' is obviously even for any value of M. If d is odd, we have either $c+\omega d \equiv 1+\omega\ (2)$ or $c+\omega d \equiv \omega\ (2)$. In the first case, $(c+\omega d)^2 \equiv \omega^2+1 \equiv \omega\ (2)$, $(c+\omega d)^3 \equiv \omega^2+\omega \equiv 1\ (2)$, $(c+\omega d)^4 \equiv c+\omega d\ (2)$. In the second case, $(c+\omega d)^2 \equiv \omega^2 \equiv 1+\omega\ (2)$, $(c+\omega d)^3 \equiv \omega^2+\omega \equiv 1\ (2)$, $(c+\omega d)^4 \equiv c+\omega d\ (2)$. Hence in either case, if $M \equiv N\ (3)$, $N = 0, 1$ or 2, $(c+\omega d)^M \equiv (c+\omega d)^N\ (2)$, from which the rest of the lemma easily follows.

LEMMA 1.6. *If D is congruent to 5 modulo 8, not equal to -3, and negative, the class-number of the quadratic field $\mathfrak{R}$ is always divisible by three.**

LEMMA 1.7. *If D is congruent to 5 modulo 8 and positive, and if*

$$\eta = r + \omega s \tag{1.3}$$

is the fundamental unit of the quadratic field $\mathfrak{R}$, then the class-number of $\mathfrak{R}$ is divisible by three when and only when the rational integer s is even.†

2. Let A, B, C be a primitive solution of (1.1). During the next three sections of the paper, we assume that $M \geqq 3$, so that C is necessarily odd.

If $1, \omega$ is the canonical basis of the field $\mathfrak{R}$, we have

$$\begin{aligned} &\omega^2 = D^{1/2},\quad \bar{\omega} = -\omega \text{ if } D \equiv 2, 3\ (4)\cdot\quad 2\omega + 1 = D^{1/2}, \\ &\bar{\omega} = -1-\omega \text{ if } D \equiv 5\ (8). \end{aligned} \tag{2.1}$$

Let

$$\begin{aligned} &\kappa = A + \omega B, && \lambda = \bar{\kappa} = A - \omega B \quad \text{if } D \equiv 2, 3\ (4), \\ &\kappa = A + B + 2\omega B, && \lambda = \bar{\kappa} = A - B - 2\omega B \text{ if } D \equiv 5\ (8). \end{aligned} \tag{2.2}$$

Then in either case, κ and λ are integers of $\mathfrak{R}$, and $\kappa\lambda = A^2 - DB^2 = C^M$ or

$$[\kappa][\lambda] = [C]^M. \tag{2.3}$$

* Dirichlet-Dedekind, *Zahlentheorie*, 4th edition, 1894, p. 244.

† Dirichlet-Dedekind, work cited, p. 250.

Since C is odd, the principal ideals $[\kappa]$ and $[\lambda]$ in (2.3) are co-prime by Lemma 1.4. Hence there exist two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{R}$ such that

$$[\kappa] = \mathfrak{a}^M, \qquad [\lambda] = \mathfrak{b}^M, \qquad [C] = \mathfrak{a}\mathfrak{b}, \qquad (\mathfrak{a}, \mathfrak{b}) = 1.$$

Since M is prime to the class-number of the field $\mathfrak{R}$, $\mathfrak{a}$ and $\mathfrak{b}$ are principal ideals of $\mathfrak{R}$ by Lemma 1.3. Denote them by $[\alpha]$ and $[\beta]$ respectively. Then

$$[\kappa] = [\alpha^M], \qquad [\lambda] = [\beta^M], \qquad [C] = [\alpha][\beta], \qquad ([\alpha], [\beta]) = 1.$$

Moreover, since λ is conjugate to κ, β is conjugate to α. Therefore there exist two units ϵ_1 and ϵ_2 of $\mathfrak{R}$ such that

$$\kappa = \epsilon_1\alpha^M, \qquad \lambda = \bar{\epsilon}_1\bar{\alpha}^M, \qquad C = \epsilon_2\alpha\bar{\alpha}, \qquad ([\alpha], [\bar{\alpha}]) = 1.$$

Since $\alpha\bar{\alpha} = N\alpha$ is a rational integer, $\epsilon_2 = \pm 1$. Let η be the fundamental unit of the field $\mathfrak{R}$. Then there exists an integer R such that $\epsilon_1 = \pm\eta^R$.

Divide R by M, and let the quotient and remainder be Q, T: $R = QM + T$, $0 \leqq T \leqq M-1$. Then if we write α' for $\eta^Q\alpha$, we have

$$\kappa = \pm \eta^T\alpha'^M, \quad \lambda = \pm \eta^{-T}\bar{\alpha}'^M, \quad C = \pm \alpha'\bar{\alpha}', \quad 0 \leqq T \leqq M-1, \tag{2.4}$$

$$([\alpha'], [\bar{\alpha}']) = 1. \tag{2.5}$$

If D is negative, the only units in $\mathfrak{R}$ are ± 1, since $D \neq -1, -3$, and (2.4) holds with $T = 0$. Henceforth we retain only the positive signs in (2.4).

3. If $D \equiv 2, 3\ (4)$, α' and $\bar{\alpha}'$ in (2.4) are of the form

$$\alpha' = a + \omega b, \qquad \bar{\alpha}' = a - \omega b, \qquad \omega^2 = D,$$

where a and b are rational integers. Then

$$(a, Db) = 1. \tag{3.1}$$

For otherwise, there exists a prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ such that $\alpha \equiv 0\ (\mathfrak{p})$, $Db = \omega^2 b \equiv 0\ (\mathfrak{p})$, so that $a \equiv \omega b \equiv 0\ (\mathfrak{p})$, $\alpha' \equiv \bar{\alpha}' \equiv 0\ (\mathfrak{p})$ contradicting (2.5).

Since $C = a^2 - Db^2$ is odd, we must have

$$a, b \text{ of opposite parity if } D \text{ is odd, } a \text{ odd if } D \text{ is even.} \tag{3.2}$$

Now $\alpha'^M = A_M + D^{1/2}B_M$, where

$$\begin{aligned} A_M &= a^M + \binom{M}{2} Da^{M-2}b^2 + \binom{M}{4} D^2a^{M-4}b^4 + \cdots; \\ B_M &= \binom{M}{1} a^{M-1}b + \binom{M}{3} Da^{M-3}b^3 + \cdots. \end{aligned} \tag{3.3}$$

If the fundamental unit η is $r + \omega s$ in the case when D is positive, we write $r = u_1$, $s = v_1$, $\omega = D^{1/2}$,

$$\eta^T = (r + \omega s)^T = U_T + D^{1/2}V_T \qquad (T = 0, 1, \cdots, M-1).$$

(2.4) then gives us our final formulas:

$$(3.4) \quad A = U_T A_M + DV_T B_M, \qquad B = U_T B_M + V_T A_M, \qquad C = a^2 - Db^2,$$

where if D is positive, T may have any integral value from 0 to $M-1$, but if D is negative, T is zero.

We have thus shown that in the case $D \equiv 2, 3\ (4)$, *every primitive solution* A, B, C *of* (1.1) *is of the form* (3.4). We shall now show that if a and b are rational integers subject to the conditions (3.1), (3.2), *the formulas* (3.4) *always give a primitive solution of* (1.1).

It is obvious the formulas always give a solution of (1.1), and that for such a solution, C is odd. To show that the solution is primitive, it suffices to prove that $(A, B) = 1$.

If $(A, B) \neq 1$, there exists a prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ such that $A \equiv B \equiv 0\ (\mathfrak{p})$ so that $A \pm D^{1/2}B \equiv 0\ (\mathfrak{p})$. Since $U_T \pm D^{1/2}V_T$ is a unit of $\mathfrak{R}$ and $A \pm D^{1/2}B = (U_T \pm D^{1/2}V_T)(A_M \pm D^{1/2}B_M)$, $A_M \pm D^{1/2}B_M = (a \pm D^{1/2}b)^M \equiv 0\ (\mathfrak{p})$ or $a \pm D^{1/2}b \equiv 0\ (\mathfrak{p})$. Therefore $2a \equiv 2D^{1/2}b \equiv 0\ (\mathfrak{p})$; or since $(a, Db) = 1$, $2 \equiv 0\ (\mathfrak{p})$, and $A \equiv B \equiv 0\ (2)$. But then $C^M = A^2 - DB^2 \equiv 0\ (2)$, so that C would be even.

4. If $D \equiv 5\ (8)$, α' and $\bar{\alpha}'$ in (2.4) are of the form

$$(4.1) \qquad \alpha' = c + \omega d, \qquad \bar{\alpha}' = c - d - \omega d, \qquad (2\omega + 1)^2 = D,$$

where c and d are rational integers which are co-prime by (2.5). There are two cases according as D is negative or positive.

If D is negative, the class-number of $\mathfrak{R}$ is divisible by three by Lemma 1.6. Hence $(M, 3) = 1$. Since 1 is the fundamental unit, we obtain from (2.4) $\alpha'^M = (c + \omega d)^M = \kappa = A + B + 2B\omega$. Therefore, by Lemma 1.5, d is even. If we write $d = 2b$, $c = a - b$, we have $\alpha' = a + D^{1/2}b$. Hence

$$\kappa = A + BD^{1/2} = (a + D^{1/2}b)^M = A_M + D^{1/2}B_M.$$

Thus we obtain as in the previous case D negative and congruent to 2 or 3 (4),

$$(4.2) \qquad A = A_M, \qquad B = B_M, \qquad C = a^2 - Db^2\alpha, \qquad (a, Db) = 1.$$

Since $M \geqq 3$, C is odd by Lemma (1.2). Therefore a and b must be of opposite parity. A_M and B_M are as in (3.3).

Conversely, it may be shown as in §3 that if a and b are rational integers of opposite parity, the formulas (4.2) always give a primitive solution of (1.1).

Next, assume that D is positive, and denote the fundamental unit of the field $\mathfrak{R}$ by

$$\eta = r + \omega s, \tag{1.3}$$

as in Lemma 1.7. Then if the class-number of $\mathfrak{R}$ is divisible by three, s is even. Writing $s=2v$, $r=u-v$,

$$\eta = u + vD^{1/2}, \qquad \eta^T = U_T + V_T D^{1/2} \qquad (T = 0, 1, \cdots, M-1).$$

Then by (2.4), (4.1)

$$\alpha'^M = (c + \omega d)^M = \bar{\eta}^T \kappa = c' + \omega d'$$

where d' is even. Since $(M, 3)=1$, d is therefore even by Lemma 1.5. On writing $d=2b$, $c=a-b$, we obtain therefore

$$A = U_T A_M + DV_T B_M, \qquad B = U_T B_M + V_T A_M, \qquad C = a^2 - Db^2. \tag{4.3}$$

a and b here are of opposite parity, and $(a, Db)=1$. Conversely, we may show as in §3 that (4.3) always gives a primitive solution of (1.1).

If the class-number of $\mathfrak{R}$ is not divisible by three, the integer s in (1.3) is odd. We obtain therefore from (2.4) and (4.1)

$$(r + \omega s)^T (c + \omega d)^M = \kappa = c' + \omega d', \qquad d' \text{ even}.$$

Therefore if d is *even*, T must be divisible by three by Lemma 1.5. On the other hand, if d is *odd*, we have the following restrictions on T and M according to the parity of r in order that d' may be even.

If $r + \omega s \equiv 1 + \omega$ (2) and $c + \omega d \equiv 1 + \omega$ (2), then $T + M \equiv 0$ (3);
if $r + \omega s \equiv 1 + \omega$ (2) and $c + \omega d \equiv \omega$ (2), then $T - M \equiv 0$ (3);
if $r + \omega s \equiv \omega$ (2) and $c + \omega d \equiv \omega$ (2), then $T + M \equiv 0$ (3);
if $r + \omega s \equiv \omega$ (2) and $c + \omega d \equiv 1 + \omega$ (2), then $T - M \equiv 0$ (3).

Let us write

$$2\eta^T = U_T + V_T D^{1/2} \qquad (T = 0, 1, \cdots, M-1).$$

$\alpha' = a + D^{1/2} b$ if d is even; $2\alpha' = a + D^{1/2} b$ if d is odd, where, in the first case, $d=2b$, $c=a-b$, and in the second case, $d=b$, $a=2c-b$, so that a and b are both odd. The four cases above when s is odd may then be stated as follows:

$$\begin{aligned} &T + M \equiv 0 \ (3) \text{ if } r - (a+b)/2 \equiv 0 \ (2), \\ &T - M \equiv 0 \ (3) \text{ if } r - (a+b)/2 \equiv 1 \ (2). \end{aligned} \tag{4.4}$$

The solutions of (1.1) are given by the following formulas:

$$2A = U_{3T} A_M + DV_{3T} B_M, \quad 2B = U_{3T} B_M + V_{3T} A_M, \quad C = a^2 - Db^2, \tag{4.5}$$
$$a, b \text{ of opposite parity}, \ (a, Db) = 1, \ 0 \leqq T \leqq [(M-1)/3)],$$

or

(4.6) $2^{M+1}A = U_T A_M + DV_T B_M$, $2^{M+1}B = U_T B_M + V_T A_M$, $4C = a^2 - Db^2$, a, b both odd, $(a, Db) = 1$, and T restricted by (4.4).

It is easily shown as before that both (4.5) and (4.6) give us primitive solutions of (1.1) with the specified restrictions on a, b and T.

The possibility of primitive solutions of (1.1) of the form (4.6) seems to have been overlooked heretofore. On taking $D=5$, $M=3$, $T=0$, $a=b=1$ in (4.6), we obtain the solution 2, 1, -1 of $X^2-5Y^2=Z^3$ discussed in the introduction.

5. The case when $M=2$, $D\equiv 5$ (8) requires separate discussion, as we see from Lemma 1.2 that primitive solutions of

$$X^2 - DY^2 = Z^2 \tag{5.1}$$

will exist of the form $X=A$, $Y=B$, $Z=C=2E$, where A, B, E are odd and co-prime. The other solutions with C odd may be obtained from our general formulas in §4. In the present case, we write

(5.2) $2\kappa = A + B + 2\omega B$, $2\lambda = A - B - 2\omega B$ where as usual $2\omega + 1 = D^{1/2}$,

or letting $A+B=2G$,

$$\kappa = G + \omega B, \qquad \lambda = \bar{\kappa}, \qquad \kappa\lambda = E^2, \qquad [\kappa][\lambda] = [E]^2.$$

If we now apply the reasoning used in §2 to this ideal equation, we deduce that either

$$\begin{aligned} &\kappa = (c + \omega d)^2, && E = (c + \omega d)(c + \bar{\omega} d), && \text{or} \\ &\kappa = (r + \omega s)(c + \omega d)^2, && E = (c + \omega d)(c + \bar{\omega} d), \end{aligned} \tag{5.3}$$

where $r+\omega s$ is the fundamental unit of the field $\mathfrak{R}$. To agree with our former notation, let $U_0=2$, $V_0=0$, $U_1=2r-s$, $V_1=s$, $2c-d=a$, $d=b$. Then

$$8\kappa = (U_T + D^{1/2}V_T)(a + D^{1/2}b)^2, \qquad 4E = a^2 - Db^2, \qquad T = 0, 1,$$

so that

$$\begin{aligned} &4A = U_T(a^2 + Db^2) + 2abDV_T, && 4B = V_T(a^2 + Db^2) + 2abU_T, \\ &2C = a^2 - Db^2, && T = 0, 1, \end{aligned} \tag{5.4}$$

where a and b are both odd, and $(a, Db)=1$. As before, (5.4) always gives a primitive solution of (5.1) with Z even.

For the case $M=2$, it may be noted, a knowledge of all of the primitive solutions of (1.1) gives us immediately the most general solution of (1.1). On collecting all of our results, we obtain the fundamental theorem stated in the introduction.

III. Applications of the formulas

6. Consider the diophantine equation

$$X^2 - D = Z^M, \tag{6.1}$$

where D is square-free, negative, $\neq -1$ or -3, incongruent to 1 (8), while M is prime to the class-number of the quadratic field $\Re(D^{1/2})$. Then if $X = A$, $Z = C$ is a solution of (6.1), A, ± 1, C is a primitive solution of (1.1). Conversely, any primitive solution of (1.1) with $B = \pm 1$ gives a solution of (6.1). Accordingly, all solutions of (6.1) are obtainable by setting $Y = \pm 1$ in the formulas of case I of the fundamental theorem; thus

$$\pm 1 = \binom{M}{1} a^{M-1}b + \binom{M}{3} Da^{M-3}b^3 + \cdots. \tag{6.2}$$

If M is even, the last term on the right of (6.2) is $\binom{M}{M-1} D^{(M-2)/2} ab^{M-1}$. Since the numbers $\binom{M}{1}, \binom{M}{3}, \cdots, \binom{M}{M-1}$ are all even when M is even, (6.2) is impossible, so that (6.1) *has no solutions if M is even.*

If M is odd, the last term on the right of (6.2) is $D^{(M-1)/2}b^M$. Hence every term is divisible by b, so that $b = \pm 1$, and a must be a root of the equation

$$\binom{M}{1} x^{M-1} + \binom{M}{3} Dx^{M-3} + \cdots + D^{(M-1)/2} \mp 1 = 0. \tag{6.21}$$

For fixed D and M meeting our restrictions, the solution of (6.1) reduces then to finding all the integral roots of (6.2).

Under the same restrictions on D and M, we can obtain information about the diophantine equation

$$1 - DY^2 = Z^M. \tag{6.3}$$

We have in place of (6.2) the condition

$$\pm 1 = a^M + \binom{M}{2} a^{M-2}b^2 + \cdots. \tag{6.4}$$

If M is even, we obtain no direct information. But if M is odd, the right side of (6.4) is divisible by a, so that $a = \pm 1$, and b must be an integral root of the equation*

$$\binom{M}{M-1} D^{(M-3)/2}x^{M-3} + \binom{M}{M-3} D^{(M-5)/2}x^{M-5} + \cdots + \binom{M}{4} Dx^2 + \binom{M}{2} = 0. \tag{6.41}$$

* The conceivable case when $a = \mp 1$ and the left side of (6.4) is ± 1 is easily shown to be impossible.

To give a numerical example, consider the equation $X^2+42=Z^5$ to which the method is applicable since the class-number of $\mathfrak{R}(42^{1/2}i)$ is 4. If M is a prime,

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

while $\binom{M}{1}, \binom{M}{3}, \cdots, \binom{M}{M-2}$ are all divisible by M. We must therefore choose the ambiguous sign in (6.21) equal to $-\binom{D}{M}$, or $+1$ in this case. On dividing out $M=5$, (6.21) becomes

$$x^4 - 84x^2 + 353 = 0.$$

Since $84^2-4\cdot 353=5644$ is not a square, the initial diophantine equation has no solutions.

7. Consider now the diophantine equation

$$X^2 - 16DY^{2N} = Z^4. \tag{7.1}$$

We assume as before that D is square-free, negative, incongruent to 1 (8), and in addition, that the class-number of the quadratic field $\mathfrak{R}(D^{1/2})$ is *odd*.*

Let A, B, C be a primitive solution of (7.1). Then $A, 4B^N, C$ is a primitive solution of

$$X^2 - DY^2 = Z^4. \tag{7.2}$$

Hence by case I of our fundamental theorem, there exist rational integers a and b such that $(a, Db)=1$, $a+b$ odd, and

$$A = a^4 + 6a^2b^2D + D^2b^4, \qquad 4B^N = 4ab(a^2 + Db^2), \qquad C = a^2 - Db^2.$$

From the expression for $4B^N$, we deduce that a, b, a^2+Db^2 are perfect Nth powers: $a=E^N$, $b=F^N$, $a^2+Db^2=G^N$ so that $X=E$, $Y=F$, $Z=G$ is a primitive solution of

$$X^{2N} + DY^{2N} = Z^N. \tag{7.3}$$

Conversely, a primitive solution of (7.3) gives us a primitive solution of (7.1). But it is easy to see that if (7.3) has any solutions whatever, it has primitive solutions. Therefore: *A necessary and sufficient condition that the diophantine equation* (7.3) *be solvable is that the diophantine equation* (7.1) *have a primitive solution.*

Assume next that D is negative, and congruent to 2 or 3 (4), and that the class-number of $\mathfrak{R}(D^{1/2})$ is prime to 3, while D is divisible by three. Consider

* This always occurs for example if D is a prime, $\equiv 5$ (8). See Dirichlet's Works, vol. I, 1889, pp. 357–370, or Crelle's Journal, vol. 18 (1838), pp. 259–274.

$$X^2 - 9DY^{2N} = Z^3. \tag{7.4}$$

A similar procedure to that given for (7.1) connects (7.4) with the diophantine equation

$$X^N + \frac{DY^N}{3} = Z^N, \tag{7.5}$$

and we have the theorem that *a necessary and sufficient condition that the diophantine equation* (7.5) *be solvable is that the diophantine equation* (7.4) *have a primitive solution.*

For example take $D = -21$. The class number of $\mathfrak{R}(21^{1/2}i)$ is four, and for $N = 7$,

$$X^7 - 7Y^7 = Z^7$$

is known to have no solutions.* Hence

$$X^2 + 189Y^{14} = Z^3$$

has no primitive solutions.

This result generalizes an interesting correspondence recently obtained by Kapferer† between the solutions of Fermat's equation and the primitive solutions of an equation of the form (7.4).

* Maillet, Comptes Rendus, vol. 129 (1899), pp. 189–199.

† Sitzungsberichte, Heidelberg Akademie, 1933, part 2, pp. 32–37.

California Institute of Technology,
Pasadena, Calif.