SOME DIOPHANTINE PROBLEMS

Thesis by

Edward Rosenthall

In Partial Fulfilment of the Requirements

for the Degree of Doctor of Philosophy

California Institute of Technology

Pasadena California

1944

The writer is indebted for constant encouragement and wise counsel at many points to Dr. E.T.Bell, under whose direction this dissertation was written.

Summary of Thesis

This thesis is concerned with the problem of exhibiting all the rational integer solutions satisfying certain diophantine equations. The thesis consists of two sections. The first section indicates how some types of diophantine equations completely reducible in a single quadratic field may be solved completely, and also the complete solution is obtained for an interesting class of cubic diophantine equations. In the past there have been many isolated investigations on the separate equations of the class considered here and at most only partial integral solutions have been given. In this thesis the complete solutions for these equations are deduced from a single multiplicative equation in a quadratic field.

In the second section Diophantine equations completely reducible in two or more different quadratic fields are considered. These equations are solved by operating on multiplicative equations in biquadratic fields.

The success of our method depends fundamentally upon the complete solution of the simple multiplicative equation $xy = zw$.

SECTION ONE

ON SOME CUBIC DIOPHANTINE EQUATIONS.

ON SOME CUBIC DIOPHANTINE EQUATIONS.*

By E. ROSENTHALL.

1. In this paper we shall adhere to the following notation: large capital letters $A, B, \cdots$ (with or without subscripts) will represent integers of the quadratic number field $Ra(\rho)$ where $\rho = \frac{1}{2}(-1 + i\sqrt{3})$; the letter ϵ will be reserved for the units of this field. Small latin letters $a, b, \cdots$ represent rational integers, and the conjugate of a number X is denoted by $\bar{X}$. The symbol $(A, B, C, \cdots)$ signifies the g. c. d. of $A, B, C, \cdots$; $A \mid B$ means A divides B, and $(A, B) = 1$ denotes that A and B are coprime.

The integers of the field $Ra(\rho)$ are of the form $c + d\rho$, or of the form $\frac{1}{2}(a + \sqrt{-3b})$ with a and b of the same parity; also $\epsilon\bar{\epsilon} = 1$.

2. In this paper we solve completely in integers of $Ra(\rho)$ a multiplicative equation of the form

$$wW\bar{W} = nN\bar{N} \tag{2.1}$$

and deduce from this the complete rational integer solution of certain interesting cubic diophantine equations. The method of proof will indicate how some types of diophantine equations reducible in a quadratic field may be solved completely.

Since the integers of $Ra(\rho)$ obey the fundamental law of arithmetic, namely unique decomposition into prime factors, multiplicative equations in this field can be solved completely in parametric form by the method of reciprocal arrays.[1]

To solve (2.1) we require the following fundamental lemma.

LEMMA 1.[1] *All integral solutions of*

$$XY = ZW$$

are given by $X = US$, $Y = VT$, $Z = UT$, $W = VS$; *and it suffices to take* $(S, T) = 1$.

This lemma (as stated in the paper referred to) is for non-zero integers X, Y, Z, W. However the solution given includes all the possible zero solu-

* Received August 19, 1942; Revised February 19, 1943.

[1] E. T. Bell, "Polynomial diophantine systems," *Transactions of the American Mathematical Society*, vol. 35 (1933), pp. 909-910. Also E. T. Bell, "Reciprocal arrays and diophantine analysis," *American Journal of Mathematics*, vol. 35 (1933), pp. 50-66.

tions without violating the conditions on S and T. For example, the solution $X = Z = W = 0$ is obtained by taking $U = S = 0$, $T = 1$, and S, T are coprime.

3. We now solve equation (2.1).

THEOREM 1. *The complete solution in integers w, W, n, N satisfying equation (2.1) is given by*

$$W = SUL, \quad w = tV\bar{V}, \quad N = S\bar{U}\bar{V}, \quad n = t\bar{L}\bar{L} \tag{3.1}$$

and it suffices to take $(UL, \bar{U}\bar{V}) = (V\bar{V}, L\bar{L}) = 1$.

Proof. By Lemma 1 all required values of w, W, n, N are of the form

$$\begin{aligned} W &= R\,A\,F & N &= R\,B\,H \\ W &= S\,B\,G & \bar{N} &= S\,C\,F \\ w &= T\,C\,H & n &= T\,A\,G \end{aligned} \tag{3.2}$$

with the g. c. d. conditions

$$(W, N) = R, \quad (\bar{W}, \bar{N}) = S, \quad (w, n) = T. \tag{3.3}$$

From (3.3) it follows that $R = \epsilon\bar{S}$; substituting this in (3.2) we see that the parameters must be restricted to satisfy

$$\epsilon\,A\,F = \bar{B}\,\bar{G} \quad \text{and} \quad \epsilon\,B\,H = \bar{C}\,\bar{F}. \tag{3.4}$$

Hence (3.2) becomes

$$\begin{aligned} W &= \bar{S}\,\bar{B}\,\bar{G} & N &= \bar{S}\,\bar{C}\,\bar{F} \\ w &= T\,C\,H & n &= T\,A\,G \end{aligned} \tag{3.5}$$

with conditions (3.4). By Lemma 1 all A, F, B, G satisfying $(3.4)_1$ are given by

$$\bar{B} = A_1B_1, \quad \bar{G} = C_1D_1, \quad \epsilon A = A_1D_1, \quad F = C_1B_1.$$

Then $(3.4)_2$ becomes $\epsilon\bar{A}_1H = \bar{C}\bar{C}_1$ and so

$$\epsilon\bar{A}_1 = A_2B_2, \quad H = C_2D_2, \quad \bar{C} = A_2D_2, \quad \bar{C}_1 = C_2B_2.$$

Substituting these values in (3.5) we have

$$\begin{aligned} W &= \epsilon\bar{S}\bar{A}_2\bar{C}_2(\bar{B}_2B_1)(\bar{B}_2D_1), & N &= \bar{S}A_2C_2D_2(B_2\bar{B}_1) \\ w &= T\bar{A}_2C_2(D_2\bar{D}_2), & n &= T\bar{A}_2C_2(\bar{B}_2D_1)(B_2\bar{D}_1). \end{aligned}$$

Since the integers B_2, B_1, D_1 always occur as factors of the products $\bar{B}_2B_1, \bar{B}_2D_1$ we can put $\bar{B}_2B_1 = K$ and $\bar{B}_2D_1 = L$; we also make the reversible substitution $D_2 = \epsilon\bar{V}$ and replace $\epsilon\bar{S}$ by the parameter S. Then we have

$$(3.6)\quad W = S(\bar{A}_2\bar{C}_2K)L,\ w = (T\bar{A}_2C_2)V\bar{V},\ N = S(A_2C_2\bar{K})\bar{V},\ n = (T\bar{A}_2C_2)L\bar{L},$$

where $T\bar{A}_2C_2$ must be restricted to be a rational integer. Thus (3.6) is a complete parametric representation for the indeterminates satisfying (2.1).

However if we put $\bar{A}_2\bar{C}_2K = U$, $T\bar{A}_2C_2 = t$ then all numbers in (3.6) are included in (3.1). But by direct substitution we see that all the numbers (3.1) are solutions of (2.1). Hence (3.1) is the complete solution of (2.1) where S, U, L, V are arbitrary integers in $Ra(\rho)$, and t is any rational integer.

4. From Theorem 1 we can deduce the complete rational integer solution of $x^3 + y^3 = z^3 + w^3$. This equation can be put in the form (2.1), viz.,

$$(4.1)\qquad (X + \bar{X})X\bar{X} = (Y + \bar{Y})Y\bar{Y}$$

where $X = \frac{1}{2}[(x+y) + \sqrt{-3}(x-y)]$, $Y = \frac{1}{2}[(z+w) + \sqrt{-3}(z-w)]$ are integers of $Ra(\rho)$. If $x = y$, we have the trivial solutions with $x = z$.

In **6** we prove the following theorem.

THEOREM 2. *The set of all integers X, Y (with $X \neq Y$) satisfying (4.1) is given by*

$$(4.2)\qquad X = (\sqrt{-3}p/\theta q)(e + f\rho)LU,\quad Y = (\sqrt{-3}p/\theta q)(e + f\rho)\bar{U}\bar{V}$$

where $e + f\rho = UV \cdot V\bar{V} - \bar{U}\bar{L} \cdot \bar{L}L$, and θ is 1 unless $\sqrt{-3} \mid (e + f\rho)$ and then $\theta = 3$; it suffices to take $q = (e, f)$ and $(LU, \bar{U}\bar{V}) = (V\bar{V}, L\bar{L}) = 1$.

5. To obtain the solution of (4.1) in the form (4.2) we require the following three lemmas.

LEMMA 2. *If the product XY is pure imaginary and if $X = aA$ where A is not divisible by a rational integer then $Y = \sqrt{-3}b\bar{A}/\theta$ where θ is 1, or 3 if $\sqrt{-3} \mid A$.*

Proof. Put $X = aA = a(m + n\rho)$ and $Y = b(s + t\rho)$ where $(m, n) = (s, t) = 1$. Then since XY is pure imaginary we must have

$$ns + mt - nt = 2(ms - nt)$$

from which it follows that $m(2s - t) = n(s + t)$; and since $(m, n) = 1$ we have $2s - t = kn$, $s + t = km$. Hence $s = k(n + m)/3$, $t = k(2m - n)/3$ and since $(s, t) = 1$ we can write

$$s = (n + m)/\theta, \qquad t = (2m - n)/\theta,$$

which gives $Y = b\{(m + n) + (2m - n)\rho\}/\theta = b\sqrt{-3}/\theta$.

LEMMA 3. *If $D = (l + m\rho)$ is a g. c. d. of $a + b\rho$ and $c + d\rho$, then $(a, b, c, d) = (l, m)$.*

Proof. We know that if a rational integer t divides $a + b\rho$ then t divides both a and b.

Therefore if $q = (l, m)$, then $q|D$ and q is a divisor of a and b, c and d; and if $s = (a, b, c, d)$ then $q|s$. Also s divides $a + b\rho$, $c + d\rho$, and therefore $s|D$. Then $s|l$ and $s|m$, and therefore $s|q$. Hence $s|q$, $q|s$ and so $s = q$, $(a, b, c, d) = (l, m)$.

LEMMA 4. *If the matrix of the coefficients is of rank 2, then all integral solutions of the simultaneous equations*

$$AX + BY + CZ = 0, \qquad A_1X + B_1Y + C_1Z = 0$$

are given by

$$X = (E/D)(BC_1 - B_1C), Y = (E/D)(A_1C - AC_1), Z = (E/D)(AB_1 - A_1B)$$

where E is an arbitrary integer and it suffices to take $D = (BC_1 - B_1C, A_1C - AC_1, AB_1 - A_1B)$.

For, solving algebraically, X, Y, Z are certainly given by

$$X = \alpha(BC_1 - B_1C), \quad Y = \alpha(A_1C - AC_1), \quad Z = \alpha(AB_1 - A_1B)$$

where α is in the field; writing α in lowest terms E/D, D must be a divisor of $BC_1 - B_1C$, etc. Hence, multiplying up by a suitable factor, it suffices to take D as stated, and E is arbitrary.

The case where the matrix is of rank 0 or 1 will be considered in the application to which the lemma is put.

6. We now prove Theorem 2. Considering each element of (4.1) as independent, then by Theorem 1 all X, Y satisfying (4.1) are of the form

$$(6.1) \qquad X = SUL, \quad X + \bar{X} = tV\bar{V}, \quad Y = S\bar{U}\bar{V}, \quad Y + \bar{Y} = tL\bar{L}$$

with $(UL, \bar{U}\bar{V}) = (V\bar{V}, L\bar{L}) = 1$ and the parameters must be restricted to satisfy

$$SUL + \bar{S}\bar{U}\bar{L} - tV\bar{V} = 0, \qquad S\bar{U}\bar{V} + \bar{S}UV - tL\bar{L} = 0.$$

Considering this system in the indeterminates S, $\bar{S}$, t and taking the matrix of the coefficients to be of rank 2, then by Lemma 4 all S, $\bar{S}$ are given by

$$S = (E/D)(e + f\rho), \qquad \bar{S} = -(E/D)(e + f\rho^2)$$

where E is arbitrary and it suffices to take $D = (e + f\rho, e + f\rho^2)$. From the expressions for S and $\bar{S}$ we get $E\bar{D} + \bar{E}D = 0$, and hence $E\bar{D}$ is pure imaginary; thus by Lemma 2 we can put

$$D = (k + l\rho) = qK, \qquad E = \sqrt{-3}\, pK/\theta \text{ with } q = (k, l),$$

and $\theta = 1$ unless $\sqrt{-3} \mid K$, that is $\sqrt{-3} \mid (e + f\rho)$ and then $\theta = 3$; from Lemma 3 it follows that $q = (e, f)$. Hence

$$E/D = \sqrt{-3}\, p/\theta q$$

where $q = (e, f)$, and Theorem 2 is proved for the case considered.

If the matrix of the coefficients is of rank 1 then $\bar{\epsilon}V = \epsilon L = \bar{U}$ or $U = 0$ giving in (6.1) the trivial solution $X = Y$; and if the matrix is of rank 0 we get $X = Y = 0$, a solution which is included in (4.2).

7. From Theorem 2 we deduce the following result.

THEOREM 3. *All sets of rational integral values x, y, z, w (except $x = z$) satisfying the equation*

$$x^3 + y^3 = z^3 + w^3 \tag{7.1}$$

are given by

$$x = p(a - 2b)/\theta q,\ y = -p(a + b)/\theta q,\ z = p(c - 2d)/\theta q,\ w = -p(c + d)/\theta q$$

where $a + b\rho = UL(e + f\rho)$, $c + d\rho = \bar{U}\bar{V}(e + f\rho)$, and q, θ, $e + f\rho$, are as defined in Theorem 2.

For from Theorem 2 we have

$$\tfrac{1}{2}[(x + y) + \sqrt{-3}(x - y)] = (\sqrt{-3}p/\theta q)(a + b\rho),$$
$$\tfrac{1}{2}[(z + w) + \sqrt{-3}(z - w)] = (\sqrt{-3}p/\theta q)(c + d\rho).$$

Equating real and imaginary parts and solving for x, y, z, w yields the required results. Further it suffices to take $(UL, \bar{U}\bar{V}) = (V\bar{V}, L\bar{L}) = 1$.

8. The complete solution of the equation $mM\bar{M} = nN\bar{N}$ also yields the complete rational integral solution [2] of

$$x^3 + y^3 + z^3 - 3xyz = u^3 + v^3 + w^3 - 3uvw, \tag{8.1}$$

[2] R. D. Carmichael, *Diophantine Analysis*, New York, 1915, pp. 63-65, discusses this equation and gives a four parameter rational solution.

where

$$m = x + y + z, \quad M = (x - z) + \rho(y - z), \quad n = u + v + w,$$
$$N = (u - w) + \rho(v - w).$$

Then from (3.1) all rational integers satisfying (8.1) are obtainable from

$$(8.2)\quad \begin{aligned} x + y + z &= tV\bar{V} \equiv a, & u + v + w &= tL\bar{L} \equiv a_1, \\ (x - z) + \rho(y - z) &= SUL \equiv b + c\rho, & (u - w) + \rho(v - w) &= S\bar{U}\bar{V} \equiv b_1 + c_1\rho, \end{aligned}$$

and it suffices to take $(L\bar{L}, V\bar{V}) = (UL, \bar{U}\bar{V}) = 1$. Solving (8.2) for x, y, z, u, v, w gives

$$(8.3)\quad \begin{aligned} x &= \tfrac{1}{3}(a + 2b - c), & y &= \tfrac{1}{3}(a - b + 2c), & z &= \tfrac{1}{3}(a - b - c) \\ u &= \tfrac{1}{3}(a_1 + 2b_1 - c_1), & v &= \tfrac{1}{3}(a_1 - b_1 + 2c_1), & w &= \tfrac{1}{3}(a_1 - b_1 - c_1) \end{aligned}$$

for the complete rational integral solution of (8.1).

It is desirable to know how the parameters t, U, L, V are to be selected so that (8.3) always gives integers. These expressions are integers if $a + 2b - c \equiv 0 \pmod 3$ and $a_1 + 2b_1 - c_1 \equiv 0 \pmod 3$. This implies

$$(8.4)\quad \begin{aligned} tV\bar{V} + SUL + \bar{S}\bar{U}\bar{L} &\equiv 0 \pmod 3 \\ tL\bar{L} + S\bar{U}\bar{V} + \bar{S}UV &\equiv 0 \pmod 3. \end{aligned}$$

If both UL and $\bar{U}\bar{V}$ are prime to 3, then it suffices to take S satisfying the linear congruence $AS \equiv B \pmod 3$, where $UL \cdot UV - \bar{U}\bar{L} \cdot \bar{U}\bar{V} = A$, and $-t(V\bar{V}\,\bar{U}\bar{V} - L\bar{L} \cdot UL) = B$. This congruence is solvable if $(3, A) \mid B$. Since A is divisible by $\sqrt{-3}$, B will have to contain the factor $\sqrt{-3}$ or $(\sqrt{-3})^2$ If it happens that U, L, V are selected so that $(V\bar{V} \cdot UV - UL \cdot L\bar{L})$ does not contain this factor then it suffices to select $t \equiv 0 \pmod 3$; otherwise t is arbitrary.

If one of UL, $\bar{U}\bar{V}$ (say UL) is not prime to 3, then it suffices to take $\bar{U}\bar{V}$ prime to 3; whence U must be prime to 3. Thus L must be divisible by $\sqrt{-3}$, and it follows therefore that $L\bar{L} \equiv 0 \pmod 3$ and $SUL + \bar{S}\bar{U}\bar{L} \equiv 0 \pmod 3$. Hence (8.4) becomes

$$(8.5)\qquad tV\bar{V} \equiv 0 \pmod 3, \qquad S\bar{U}\bar{V} + \bar{S}UV \equiv 0 \pmod 3.$$

From $(8.5)_1$ we have $t \equiv 0 \pmod 3$ since $V\bar{V}$, $L\bar{L}$ are coprime; and $(8.5)_2$ holds if and only if $\sqrt{-3}$ divides $S\bar{U}\bar{V}$, whence $\sqrt{-3}$ divides S since $\bar{U}\bar{V}$ is prime to 3. Summing up, we have, in this case, that (8.3) yields integers if and only if S, L (or V) is divisible by $\sqrt{-3}$, and $t \equiv 0 \pmod 3$.

9. As a further illustration of the method used here for solving diophantine equations, we now solve completely in rational integers the equation [3]

$$x^3 + y^3 = z^2. \tag{9.1}$$

For this purpose we require the following lemmas.

LEMMA 5. *If the product XYZ is a rational integer then all values of X, Y, Z are given by*

$$X = aAB, \quad Y = b\bar{A}C, \quad Z = c\bar{B}\bar{C}.$$

Proof. Precisely as in Lemma 2 it follows that if the product RS is a rational integer then all R, S are given by $R = aK$, $S = p\bar{K}$. Hence since $X(YZ)$ is rational we can put $X = aK$, $YZ = p\bar{K}$; whence by Lemma 1, we have

$$Y = FG, \quad Z = HJ, \quad p = FJ, \quad \bar{K} = HG.$$

Again, since FJ is rational it suffices to take $F = bC$, $J = c\bar{C}$; make the change in parameters $H \to \bar{B}$, $G \to \bar{A}$, and the lemma is proved.

We note that it suffices to take A, cC coprime (Lemma 1); further any factor common to a and c can be absorbed into the B and so we can take $(a, c) = 1$. These facts will be required in **10.**

LEMMA 6. *The complete set of integer values X, Y satisfying $X\bar{X} = Y\bar{Y}$ is given by $X = \epsilon ST$, $Y = S\bar{T}$, and it suffices to take T divisible by no rational integer.*

Proof. This equation $X\bar{X} = Y\bar{Y}$ can be considered as a particular case of Theorem 1 by placing $w = n = 1$, from which it follows in (3.1) that $t = 1$, $V = \epsilon_1$, $L = \epsilon_2$. On making the reversible substitution $U = \bar{\epsilon}_1 T$, $\bar{\epsilon}_1\epsilon_2 = \epsilon$ we obtain the required result.

LEMMA 7. *All integers X, z satisfying $X\bar{X} = z^2$ are given by $X = \epsilon aT^2$, $z = aT\bar{T}$.*

For, from Lemma 6 all required X, z are given by $X = \epsilon ST$, $z = S\bar{T}$, where $S\bar{T}$ must be a rational integer; then we can put $S = aT$, since T is divisible by no rational integer.

Lemmas 6 and 7 furnish the complete rational integral solutions of each of the equations [4] $x^2 + my^2 = z^2 + mw^2$ and $x^2 + my^2 = u^2$ for those m in

---

[3] L. E. Dickson, *History of the Theory of Numbers*, vol. 2, pp. 578-581 gives an account of the investigations on (9.1).

[4] If $m \equiv 1\,(4)$ replace form $u^2 + mv^2$ by $u^2 + uv + \frac{1}{4}(1 - m)v^2$.

which the integers of the quadratic field $Ra(\sqrt{-m})$ are uniquely decomposable into prime factors. The complete solutions of these equations for any value of m are readily obtained by other methods,[5] but for our purpose the form of solution given here is desirable since it occurs in multiplicative form.

10. We now return to equation (9.1). Defining the integer X as in **4**, this equation takes the form

$$(X+\bar{X})X\bar{X} = z\cdot z\cdot 1. \tag{10.1}$$

Then from (3.1) it follows that all X, $X+\bar{X}$, z of (10.1) are given by

$$X = SUL, \quad X+\bar{X} = tV\bar{V}, \quad z = S\bar{U}\bar{V}, \tag{10.2}$$

where t and L must satisfy $tL\bar{L}=1$. Thus $t=1$ (since $L\bar{L}>0$), $L=\epsilon$; and with the reversible substitution $U=\bar{\epsilon}K$, $V=\epsilon P$, (10.2) becomes

$$X = SK, \quad X+\bar{X} = P\bar{P}, \quad z = S\bar{K}\bar{P},$$

and it suffices to take K divisible by no rational integer (it can be absorbed into S).

Since $S\bar{K}\bar{P}$ must be a rational integer, then

$$S = aAB, \quad \bar{K} = \bar{A}C, \quad \bar{P} = c\bar{B}\bar{C}$$

and it suffices here to have c prime to a and A (see remarks at the end of Lemma 5), and we have

$$X = aA^2R, \quad X+\bar{X} = c^2R\bar{R}, \quad z = acA\bar{A}R\bar{R} \tag{10.3}$$

in which, since B and C always occur as the product $B\bar{C}$, we have put $B\bar{C}=R$.

Further, the parameters of (10.3) must satisfy $c^2R\bar{R} - aA^2R - a\bar{A}^2\bar{R} = 0$ which is equivalent to

$$(c^2R - a\bar{A}^2)(c^2\bar{R} - aA^2) = (aA\bar{A})^2.$$

Put $c^2R - a\bar{A}^2 = H$, then (10.3) becomes

$$X = aA^2\left(\frac{H+a\bar{A}^2}{c^2}\right), \qquad z = acA\bar{A}\left(\frac{H+a\bar{A}^2}{c^2}\right)\left(\frac{\bar{H}+aA^2}{c^2}\right) \tag{10.4}$$

where $(aA\bar{A})^2 = H\bar{H}$. Whence, by Lemma 1,

$$H = \epsilon bT^2, \quad aA\bar{A} = bT\bar{T}. \tag{10.5}$$

Solving $(10.5)_2$ by Theorem 1 we finally get

[5] L. E. Dickson, *Introduction to the Theory of Numbers*, pp. 40-41; also see Ex. 5, p. 43.

$$H = \epsilon m G\bar{G}(M\bar{F}\bar{E})^2, \quad a = mE\bar{E}, \quad A = MFG. \tag{10.6}$$

Again, since R is an integer we must have c^2 dividing $H + a\bar{A}^2$, that is it must divide $m\bar{G}\bar{F}^2\bar{E}(\epsilon GM^2\bar{E} + E\bar{M}^2\bar{G})$. Since c is prime to a and A, then we have c^2 prime to each of m, E, F, G, M. Hence c^2 must divide $(E\bar{M}^2\bar{G} + \epsilon\bar{E}M^2G)$.

Substituting (10.6) in (10.4) we have

$$X = (mF\bar{F})^2(E\bar{G})(\bar{E}G)^2M^2\left(\frac{E\bar{M}^2\bar{G} + \epsilon\bar{E}M^2G}{c^2}\right),$$

$$z = c(mF\bar{F})^3(\bar{E}G)^2(E\bar{G})^2M\bar{M}\left(\frac{E\bar{M}^2\bar{G} + \epsilon\bar{E}M^2G}{c^2}\right)\left(\frac{\bar{E}M^2G + \bar{\epsilon}E\bar{M}^2\bar{G}}{c^2}\right).$$

Put $mF\bar{F} = k$ and $E\bar{G} = \bar{K}$, and we get

$$\begin{aligned} X &= k^2K^2\bar{K}M^2\left(\frac{\bar{K}\bar{M}^2 + \epsilon KM^2}{c^2}\right) \\ z &= \bar{\epsilon}ck^3(K\bar{K})^2M\bar{M}\left(\frac{\bar{K}\bar{M}^2 + \epsilon KM^2}{c^2}\right), \end{aligned} \tag{10.7}$$

and it suffices to have c prime to each of K, M and k.

All the integer solutions of (10.1), and hence of (9.1), are given by (10.7), and in order to obtain all the integers in (10.7) we can take c, k arbitrary and M any integer prime to c and then select the coördinates of K to make $\left(\frac{\bar{K}\bar{M}^2 + \epsilon KM^2}{c^2}\right)$ integral. This is done in the following way.

Put $K = u + v\rho$, and let $M^2 = m + n\rho$, (whence m, n, c^2 are coprime). Then if we take $\epsilon = 1$, ρ, ρ^2 in succession the congruence $\bar{K}\bar{M}^2 + \epsilon KM^2 \equiv 0 \pmod{c^2}$ becomes

$$u(2m - n) \equiv (m + n)v \pmod{c^2}, \quad u(m - 2n) \equiv (2m - n)v \pmod{c^2},$$
$$u(m + n) \equiv (2n - m)v \pmod{c^2}$$

respectively; and for $\epsilon = -1$, $-\rho$, $-\rho^2$ respectively we get the congruences

$$un \equiv v(n - m) \pmod{c^2}, \quad um \equiv vn \pmod{c^2}, \quad u(n - m) \equiv vm \pmod{c^2}.$$

Since c^2 is prime to at least one of the coördinates m or n it follows that in the last three congruences either the coefficient of u or of v (at least) must be prime to c^2. If this coefficient is the coefficient of u, then select v arbitrary and solve the congruence for the unique u, and similarly solve for the unique v with arbitrary u if the coefficient of v is prime to c^2.

In the first three congruences, also one of the coefficients (that is, of u or v) must be prime to c^2, and so we can always find a unique u or v. For

example, (considering the first congruence), suppose that $2m - n$, $m + n$, c^2 have the factor $p \not\equiv 3$ in common. Then $p \mid 3m$ and hence divides m, n, c^2, which is impossible since c^2, M^2 are coprime.

Also if 3 is a factor of c^2 then $2m - n$ (and hence $m + n$) is prime to 3, for otherwise $M^2 = \frac{1}{2}(2m - n + \sqrt{-3}n)$ would be divisible by $\sqrt{-3}$, and so M^2 would have a factor in common with c^2.

Thus in all cases either the coefficient of u or v is prime to c^2, and K can be found.

11. The equations which we have solved completely in rational integers, viz. (7.1), (8.1), and (9.1) are merely particular cases of the equation (2.1). By suitably selecting the indeterminates w, W, n, N in (2.1) the complete solution to many other interesting equations can be obtained; for example any of the equations $x^3 + y^3 + z^3 - 3xyz = u^2$, $u^2 + 3v^2$, $u^3 + v^3$; or $(x^3 + y^3)(u^3 + v^3) = (w^3 + z^3)$. Moreover Theorem 1 holds in any normal algebraic field whose integers can be decomposed uniquely into prime factors.

McGILL UNIVERSITY,
MONTREAL, CANADA.

SECTION TWO

DIOPHANTINE EQUATIONS REDUCIBLE IN BIQUADRATIC FIELDS

DIOPHANTINE EQUATIONS REDUCIBLE IN BIQUADRATIC FIELDS

By E. Rosenthall

1. **Introduction.** In an earlier paper [2] the complete rational integer solution was obtained for certain Diophantine equations reducible in a single quadratic field. In this paper we deduce the complete solution in rational integers of some Diophantine equations by operating on multiplicative equations of the form $uN(X) = vN(Y)$ in certain biquadratic fields (for notation see §3). These equations are solved by an extension of the method used earlier [2], and it will be seen from these examples how this method can be used to solve completely Diophantine equations reducible in two or more quadratic fields. The idea is to operate in the field which has as its subfields those fields in which the equation is factorable. Thus, to solve the equation $x^3 + y^3 = u^2 + v^2$ we use the field $Ra(i, 3^{\frac{1}{4}})$. This field is an example of the so-called special Dirichlet biquadratic fields which we use in this paper.

2. **The special Dirichlet biquadratic fields** [1; 47–52]. These are the fields $Ra(i, m^{\frac{1}{4}})$ obtained by adjoining $i = (-1)^{\frac{1}{4}}$ and $m^{\frac{1}{4}}$ to the field of rational numbers, where m is a positive square-free rational integer different from ± 1. The numbers of $Ra(i, m^{\frac{1}{4}})$ are

$$X = a + ib + m^{\frac{1}{4}}c + im^{\frac{1}{4}}d,$$

where a, b, c, d are rational, and the integers [1; 25–26] of the field are of the form

$$X = \tfrac{1}{2}(r + is + m^{\frac{1}{4}}t + im^{\frac{1}{4}}u),$$

where $r \equiv u$, $s \equiv t \pmod 2$ if $m \equiv 3 \pmod 4$, $r \equiv t$, $s \equiv u \pmod 2$ if $m \equiv 1 \pmod 4$, r, s are even and $t \equiv u \pmod 2$ if $m \equiv 2 \pmod 4$.

The conjugates of X are the numbers X_1 , X_2 , X_3 , respectively, obtained by changing in X the sign of i, the sign of $m^{\frac{1}{4}}$, the signs of both i and $m^{\frac{1}{4}}$; it follows then for each type of conjugate that the conjugate of a product is equal to the product of the conjugates of each factor. We also observe that the products XX_1 , XX_2 , XX_3 are numbers in the quadratic subfields $Ra(m^{\frac{1}{4}})$, $Ra(i)$, $Ra(im^{\frac{1}{4}})$, respectively. The norm $N(X)$ of a bi-quadratic number X is defined by $XX_1X_2X_3$, but if X is a quadratic integer, then $N_0(X)$ is the norm in the quadratic field (that is, $N_0(X) = XX_1$ or XX_2). If $N(X) = \pm 1$, then X is called a unit of the field.

3. **Notations.** Hereafter we shall adhere to the following notations. The letters $a, \cdots, g, s, t, \cdots, z$ will represent rational integers, while the remaining italic letters $h, j, \cdots, r$ (except m) will denote integers of $Ra(i)$. The capital letters $A, B, \cdots$ will represent integers of the field $Ra(i, m^{\frac{1}{4}})$; the Greek letters

Received March 15, 1943.

ϵ, θ will be reserved for the units of this field, and all other Greek letters will denote the integers of the quadratic subfield $Ra(im^{\frac{1}{3}})$ unless specified otherwise. For each equation in which it appears X_f will represent any definite one of the conjugates X_1 , X_2 , X_3 of X. The symbol $(R, S) = 1$ means that R and S are coprime.

Also all fields mentioned are those in which the integers possess the property of unique decomposition into primes. The integer parameters given in the solution of the equations are arbitrary unless stated otherwise.

4. **Lemmas.** The success of our method depends on lemmas of types 1 and 6. The remaining lemmas (which are proved by application of Lemmas 1, 6) are required for the particular examples we have selected to illustrate our method.

LEMMA 1. *All integer solutions of* $XY = ZW$ *are given by* $X = AB$, $Y = CD$, $Z = AD$, $W = CB$; *and it suffices to take* $(B, D) = 1$.

LEMMA 2. *All integer solutions of* $XX_f = YY_f$ *are* $X = ST$, $Y = \epsilon ST_f$, *where* ϵ *is a unit such that* $\epsilon\epsilon_f = 1$, *and it suffices to take* $(T, T_f) = 1$.

LEMMA 3. *All integer solutions of* $KXX_f = MYY_f$ *are* $K = TLL_f$, $X = SUV$, $M = TVV_f$, $Y = SU_fL_f$. *It suffices to take* $(UV, U_fL_f) = (LL_f , VV_f) = 1$.

LEMMA 4. *All integral solutions of* $hh_1 = ab$ *are* $h = ckl$, $a = ckk_1$, $b = cll_1$.

The proofs for these four lemmas are exactly as given in the earlier paper, where the indeterminates are integers of a unique factorization quadratic field.

LEMMA 5. *All integers* K, X, Y *satisfying*

$$KXX_f = YY_f \tag{4.1}$$

are given by $K = LL_f$, $X = SU$, $Y = SU_fL_f$.

Proof. In Lemma 3 we must restrict the parameters so that $TVV_f = 1$. Hence T and V are units. Put $T = \epsilon$, $V = \theta$; then $\epsilon\theta\theta_f = 1$ and all solutions of (4.1) are given by

$$K = \epsilon LL_f , \qquad X = SU\theta, \qquad Y = SU_fL_f .$$

Make the reversible substitution $L = \theta L$, $U_f = \theta_f^{-1}U_f$ and we have the required result. It suffices to take $(U, U_fL_f) = 1$.

LEMMA 6. *If the product* XY *is in* $Ra(im^{\frac{1}{3}})$, *then all* X *and* Y *are given by*

$$X = \eta A, \qquad Y = \nu A_3 .$$

Proof. The following proof applies when $m \equiv 3 \pmod 4$. In this case the integers are of the form $\frac{1}{2}(a + ib + m^{\frac{1}{3}}c + im^{\frac{1}{3}}d)$, where $a \equiv d$, $b \equiv c \pmod 2$. Hence we can put

$$X = \alpha + i\beta, \qquad Y = \gamma + i\delta.$$

Then $XY = (\alpha\gamma - \beta\delta) + i(\beta\gamma + \delta\alpha)$, and since XY is to be in $Ra(im^{\frac{1}{2}})$ we must have

$$\beta\gamma = -\delta\alpha.$$

Hence, by Lemma 1,

$$\beta = \xi\eta, \qquad \gamma = \mu\nu, \qquad \delta = -\xi\nu, \qquad \alpha = \mu\eta,$$

and therefore

$$X = \eta(\mu + i\xi), \qquad Y = \nu(\mu - i\xi).$$

Put $\mu + i\xi = A$; then $\mu - i\xi = A_3$ and we have the required result.

Similarly we have

LEMMA 7. *If the product XY is in $Ra(i)$, then all X and Y are given by $X = hA$, $Y = kA_2$; and if the product is in $Ra(m^{\frac{1}{2}})$, then we must have $X = \psi A$, $Y = \varphi A_1$, where ψ, φ are integers of $Ra(m^{\frac{1}{2}})$.*

LEMMA 8. *If αA is in $Ra(i)$, then $\alpha = a\beta$, $A = h\beta_1$.*

5. **Equations of the form $uN(X) = vN(Y)$.** The complete solutions of these equations in integers of $Ra(i, m^{\frac{1}{2}})$ yield the complete rational integral solution of some interesting Diophantine equations.

THEOREM 1. *All integers a, A, α satisfying the multiplicative equation*

$$a^2N(A) = N_0(\alpha) \tag{5.1}$$

are given by

$$a = g\lambda\lambda_1, \qquad A = \sigma ML, \qquad \alpha = \epsilon g\sigma\sigma_1\lambda^2 M_1M_2LL_3. \tag{5.2}$$

Proof. The given equation (5.1) can be written as

$$(aAA_3)(aAA_3)_1 = \alpha\alpha_1,$$

whence, by Lemma 2,

$$aAA_3 = \beta\gamma, \qquad \alpha = \epsilon\beta\gamma_1 \tag{5.3}$$

and it suffices to take $(\gamma, \gamma_1) = 1$, and ϵ is a unit of $Ra(im^{\frac{1}{2}})$. Solving the first equation of (5.3) by Lemma 1 we get

$$a = \psi\pi, \qquad AA_3 = \xi\zeta, \qquad \beta = \psi\zeta, \qquad \gamma = \xi\pi.$$

Since the product $\psi\pi$ must be a rational integer, then [2] (much as in Lemma 6) we must have

$$\psi = c\lambda, \qquad \pi = d\lambda_1.$$

Hence

$$a = cd\lambda\lambda_1, \qquad \alpha = \epsilon cd\lambda^2\xi_1\zeta, \qquad AA_3 = \xi\zeta$$

and it remains only to solve the equation

$$AA_3 = \xi\zeta.$$

From Lemma 1 it follows that

$$A = BC, \qquad A_3 = DE, \qquad \xi = BE, \qquad \zeta = DC,$$

where the parameters must be restricted so that the products BE, DC are in $Ra(im^{\frac{1}{2}})$. Hence, by Lemma 6,

$$B = \tau F, \qquad E = \mu F_3\,, \qquad D = \varphi G, \qquad C = \nu G_3\,.$$

Thus, $A = \tau\nu FG_3$, $A_3 = \varphi\mu GF_3$, from which it follows that $\tau\nu = \varphi\mu$ and so we must have

$$\tau = \omega\rho, \qquad \nu = \eta\kappa, \qquad \varphi = \omega\kappa, \qquad \mu = \eta\rho.$$

Hence all solutions of (5.1) are given by (5.2) where we have put $cd = g$, $\omega\eta = \sigma$, $\rho F = \epsilon M$, $\kappa G_3 = \epsilon_1 L$, since these parameters always occur in these product forms.

Remark. When $m = 3$, then in (5.2) it suffices to take $\epsilon = \pm 1$. Also since $(\gamma, \gamma_1) = 1$ then the g.c.d. of the coördinates of $\alpha + aA_1A_2 = \lambda_1(\beta_1 + \epsilon\beta)$ is equal to the g.c.d. of the coördinates of $g(\pm\lambda\sigma LL_3 + \lambda_1\sigma_1 L_1L_2)$. (The coördinates of a quadratic integer are the coefficients of the basis elements.) This remark will be required in the proof of Theorem 4.

Similarly we have

THEOREM 2. *All integers a, h, X satisfying $a^2N(X) = N_0(h)$ are given by $a = grr_1$, $h = \epsilon g^2 kk_1LL_2M_1M_3$, $X = kML$, where ϵ is a unit of $Ra(i)$.*

COROLLARY 1. *All X, h satisfying $N(X) = N_0(h)$ are $X = kML$, $h = \epsilon kk_1LL_2M_1M_3$.*

THEOREM 3. *All integers X, Y satisfying*

$$N(X) = N(Y) \tag{5.4}$$

are given by

$$X = \theta KPQR, \qquad Y = KP_1Q_2R_3\,. \tag{5.5}$$

This result can be deduced from Theorem 2 and the following lemma.

LEMMA 9. *All integral θ, V and primitive r satisfying $\theta rr_1 = VV_2$ are included in the solutions $\theta = \psi\psi_2$, $r = \epsilon SS_2UU_2$, $V = \psi SS_3UU_1$, where ψ, ϵ are units of $Ra(i, m^{\frac{1}{2}})$, $Ra(i)$, respectively.*

Proof. By Lemma 1 we have

$$\theta r = AB, \qquad r_1 = CD, \qquad V = AD, \qquad V_2 = CB; \qquad (B, D) = 1.$$

Then $(r, V) = A$, $(r, V_2) = A_2$ and so $B \mid A_2$; similarly $D \mid C_2$. Put $A_2 = KB$, $C_2 = LD$ and it follows from the expressions for V, V_2 that $K = L_2$. Thus

$$\theta r = LBB_2\,, \qquad r_1 = L_2DD_2\,, \qquad V = LB_2D$$

and from the expression for θr we must have L in $Ra(i)$ and so $L = L_2$. Hence $L_2 = \epsilon_1$, a unit, since r is primitive. It remains only that the parameters must satisfy $\theta D_1 D_3 = \pm BB_2$, and from Lemma 5 it follows that

$$\theta = \pm\psi\psi_2, \qquad D = S_3U_1, \qquad B = S_2U_2\psi_2; \qquad \psi = \text{a unit of } Ra(i, m^{\frac{1}{3}}).$$

Replacing ψ by $\epsilon\psi$ and noting that $\pm\epsilon^2 = 1$ we have the required result.

We can now give the proof of Theorem 3. By the corollary to Theorem 2, all X, Y satisfying (5.4) must satisfy

$$X = kML, \qquad YY_2 = (\theta kk_1)(LM_1)(LM_1)_2.$$

Therefore, by Lemma 5,

$$Y = SUV, \qquad \theta kk_1 = VV_2, \qquad LM_1 = SU_2$$

and thus, by Lemma 9,

$$\theta = \psi\psi_2, \qquad k = \epsilon ABA_2B_2, \qquad V = \psi ABA_3B_1.$$

From $LM_1 = SU_2$ we have

$$L = CD, \qquad M_1 = EF, \qquad S = CF, \qquad U_2 = ED.$$

Thus all X, Y satisfying (5.4) are

$$X = \epsilon(ABC)(F_1A_2)DE_1B_2, \qquad Y = \psi(ABC)(F_1A_2)_1D_2(E_1B_2)_3. \tag{5.6}$$

Put $\psi ABC = K$, $F_1A_2 = P$, $D = Q$, $B_2E_1 = R$ and all numbers of (5.6) are included in (5.5), but all numbers of (5.5) are solutions of (5.4) and hence (5.5) gives all solutions of (5.4).

6. **Complete rational integer solution of two interesting equations.** In the following theorem ρ denotes the integer $\frac{1}{2}(-1 + 3^{\frac{1}{2}}i)$.

THEOREM 4. *All rational integers x, y, u, v satisfying*

$$x^3 + y^3 = u^2 + v^2 \tag{6.1}$$

are given by

$$\begin{aligned} u + iv &= c^2nr(rr_1)(\pi\pi_1)^2KK_2\theta\theta_1, \\ x + \rho(x - y) &= c(rr_1)(\pi\pi_1)\pi KK_3\theta, \end{aligned} \tag{6.2}$$

where

$$\pi_1K_1K_2 \pm \pi KK_3 = cnn_1\theta, \tag{6.3}$$

and $\theta = 1, 3^{\frac{1}{2}}i$ according as the $+$ or $-$ sign is taken.

Remark. To obtain all the integers in (6.3) we can select K, n, r arbitrarily. Then if $KK_3 = a + b\rho$ and if we put $\pi = s + t\rho$, (6.3) becomes (taking the $+$ sign)

$$s(2a - b) - t(a + b) = cnn_1 . \tag{6.4}$$

Selecting c so that $(2a - b, a + b) \mid cnn_1$ we can solve (6.4) for s, t and hence obtain π; similarly for the $-$ sign.

Proof. Equation (6.1) can be put in the form

$$(\alpha + \alpha_1)\alpha\alpha_1 = hh_1 , \tag{6.5}$$

where $\alpha = x + \rho(x - y)$ and $h = u + iv$. The class number for $Ra(i, 3^{\frac{1}{2}})$ is 1, see [1; 51]. Then all α and h satisfying (6.5) must also satisfy

$$\alpha + \alpha_1 = LL_1 , \qquad \alpha = SU, \qquad h = SU_1L_1 ,$$

by Lemma 5; and we must make LL_1 rational and have SU, SU_1L_1 integers of $Ra(3^{\frac{1}{2}}i)$ $Ra(i)$ respectively. Since SU is in $Ra(3^{\frac{1}{2}}i)$ we can put $S = \beta A$, $U = \gamma A_3$, and then the expression for h becomes $h = \beta AA_2\gamma_1L_1$ from which it follows, since AA_2 is in $Ra(i)$, that $\beta\gamma_1L_1$ must be in $Ra(i)$. Hence we have

$$\beta\gamma_1 = a\delta, \qquad L_1 = k\delta_1 , \tag{6.6}$$

by Lemma 8; and it suffices to take $(\delta, \delta_1) = 1$.

From the first equation in (6.6) we get $\beta = b\gamma\delta$ since from U, U_1L_1 being coprime it follows that γ, $\delta_1\gamma_1$ are coprime; hence we have

$$\alpha + \alpha_1 = kk_1\delta\delta_1 , \qquad \alpha = b\delta BB_3 , \qquad h = bk\delta\delta_1BB_2 ,$$

where we have put the product $\gamma A = B$. Finally the parameters must satisfy $(kk_1)\delta\delta_1 - (bBB_3)\delta - (bB_1B_2)\delta_1 = 0$, which is equivalent to

$$(kk_1\delta - bB_1B_2)(kk_1\delta_1 - bBB_3) = b^2BB_1B_2B_3 .$$

(If $k = 0$, we get the solution $u = v = 0$, which is included in (6.2).) Put $kk_1\delta - bB_1B_2 = \psi$; then $\delta = (\psi + bB_1B_2)/kk_1$ (whence it suffices to select the parameters so that kk_1 is the g.c.d. of the coördinates of $\psi + bB_1B_2$, since we can have the coördinate of δ coprime) and we have

$$\alpha = bBB_3\left(\frac{\psi + bB_1B_2}{kk_1}\right), \qquad h = bkBB_2\left(\frac{\psi + bB_1B_2}{kk_1}\right)\left(\frac{\psi_1 + bBB_3}{kk_1}\right), \tag{6.7}$$

where $\psi\psi_1 = b^2N(B)$; then by Theorem 1 the last equation yields

$$\psi = \pm g\sigma\sigma_1\lambda^2M_1M_2KK_3 , \qquad b = g\lambda\lambda_1 , \qquad B = \sigma MK \tag{6.8}$$

and the g.c.d. of the coördinates of $\psi + bB_1B_2$ is the g.c.d. of the coördinates of $g(\lambda_1\sigma_1K_1K_2 \pm \lambda\sigma KK_3)$. Substituting (6.8) in (6.7) we get

$$h = kgl^2l_1KK_2(\pi\pi_1)^2\theta\theta_1 , \qquad \alpha = g(ll_1)KK_3\pi^2\pi_1\theta \tag{6.9}$$

with

$$\theta kk_1 = g(\pi_1K_1K_2 \pm \pi KK_3) \tag{6.10}$$

in which the products $\lambda\sigma$, MM_2 have been replaced by the single parameters π, l. From (6.10) we get

$$k = cnp, \qquad g = cpp_1 , \qquad \pi_1 K_1 K_2 \pm \pi K K_3 = \theta c n n_1 ,$$

by Lemma 4; and writing these values in (6.9) and putting $pl = r$ we have the required result.

THEOREM 5. *All sets of rational integers x, y, u, v satisfying*

$$x^4 + y^4 = u^2 + v^2 \tag{6.11}$$

are given by

$$u + iv = \epsilon k k_1 M_1 M_3 L L_2 ,$$

$$x = as - bt - dz - (c + 2d)w, \qquad y = cs - t(c + 2d) + z(a - b) - 2wb,$$

where we first select arbitrary k, M giving $kM = \frac{1}{2}(2a + i\cdot 2b + 2^{\frac{1}{2}}c + 2^{\frac{1}{2}}i(c + 2d))$ and then solve for the indeterminates s, t, w, z of $L = \frac{1}{2}(2s + i\cdot 2t + 2^{\frac{1}{2}}z + 2^{\frac{1}{2}}i(z + 2w))$ from the homogeneous linear equations

$$bs + at + (d + c)z + wc = 0,$$

$$ds + (c - d)t + bz + (a - b)w = 0.$$

Proof. Equation (6.11) can be written as

$$N(X) = N_0(h), \tag{6.12}$$

where $X = x + \frac{1}{2}(2^{\frac{1}{2}}y + 2^{\frac{1}{2}}yi)$, $h = u + iv$.

Therefore, by Theorem 2, all X, h are given by

$$X = kML, \qquad h = \epsilon k k_1 L L_2 M_1 M_3 ,$$

where M, L are integers of $Ra(i, 2^{\frac{1}{2}})$ and we must restrict the product kML to have the form $x + \frac{1}{2}(2^{\frac{1}{2}}y + 2^{\frac{1}{2}}iy)$. To do this we may put

$$kM = \tfrac{1}{2}(2a + 2bi + 2^{\frac{1}{2}}c + 2^{\frac{1}{2}}i(c + 2d)), \qquad L = \tfrac{1}{2}(2s + i\cdot 2t + 2^{\frac{1}{2}}z + 2^{\frac{1}{2}}i(w + 2z))$$

since kM, L are integers of $Ra(i, 2^{\frac{1}{2}})$. If we select arbitrary k, M, then a, b, c, d are known and on equating the corresponding coördinates of kML and X we have the required result.

7. **Other equations.** Using Lemma 3 we can deduce that all integers X, Y satisfying

$$(X + X_2)XX_2 = (Y + Y_2)YY_2 \tag{7.1}$$

are given by

$$X = 3^{\frac{1}{2}}ipSUL/\theta q, \qquad Y = 3^{\frac{1}{2}}ipSU_2V_2/\theta q, \tag{7.2}$$

where $S = UV \cdot VV_2 - U_2L_2 \cdot LL_2 = \frac{1}{2}(l + 3^{\frac{1}{2}}ij)$ and it suffices to take $q = (l, j)$; θ is 1 or 3 if $3^{\frac{1}{2}}i \mid S$. The proof is similar to that given in [2]; here however we operate in the field $Ra(i, 3^{\frac{1}{2}})$ instead of the quadratic field $Ra(3^{\frac{1}{2}}i)$.

If we put $2X = (h + k) + 3^{\frac{1}{2}}i(h - k)$, $2Y = (r + n) + 3^{\frac{1}{2}}i(r - n)$, then (7.1) becomes $h^3 + k^3 = r^3 + n^3$, and we obtain from (7.2) an explicit representation for all Gaussian integers satisfying this equation.

Also by operating in the biquadratic field $Ra(a^{\frac{1}{2}}, b^{\frac{1}{2}})$ we can obtain all integral solutions of $x^2 - ay^2 = z^2 - bw^2$ in all cases in which these fields have unique factorization. For, proceeding much as in Lemma 9, we obtain the complete solution

$$x + a^{\frac{1}{2}}y = \epsilon c Y Y_2 , \qquad z + b^{\frac{1}{2}}w = \theta c Y Y_1 ,$$

where Y is an integer of $Ra(a^{\frac{1}{2}}, b^{\frac{1}{2}})$ and Y_1 , Y_2 are respectively obtained from Y by changing sign of $a^{\frac{1}{2}}$, $b^{\frac{1}{2}}$; ϵ and θ are units of $Ra(a^{\frac{1}{2}})$ and $Ra(b^{\frac{1}{2}})$, respectively.

Bibliography

1. D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Berlin, 1932.
2. E. Rosenthall, *On some cubic Diophantine equations*, American Journal of Mathematics, vol. 65(1943).

McGill University.