ON SOME SPECIAL DIOPHANTINE EQUATIONS

E. ROSENTHALL

1. **Introduction.** The following lemma is fundamental in the algorithm of reciprocal arrays for the solution of multiplicative diophantine equations in certain arithmetics as developed by E. T. Bell.[1]

LEMMA 1. *All sets of integers satisfying the diophantine equation*

$$xy = zw$$

are given by

$$x = ab, \quad y = cd, \quad z = ad, \quad w = cb$$

and it suffices to take b and d coprime.

Rational arithmetic and the theory of ideals in an algebraic number field provide instances of these arithmetics, and in all cases the fundamental theorem of unique decomposition into prime factors is required.

By use of this algorithm Bell has obtained the complete solution of a large class of diophantine equations, and by means of an application of Lemma 1 (and results derived from it) to equations reducible in particular algebraic number fields the present writer has obtained the complete solution of some interesting diophantine equations.

In this paper Lemma 1 is generalized to an arbitrary algebraic field, and the method of proof is then applied to a multiplicative equation from which we immediately obtain a formula exhibiting all the rational integers satisfying $x^2+ay^2=z^{2n+1}$. The procedure is to replace the algebraic indeterminates in the given multiplicative equation by the principal ideals they generate; then solving this equation by the method of arrays we obtain the solution in terms of ideals. In this solution, by a use of properties of equivalent ideals all the ideals are replaced by suitable principal ideals and the complete solution of the given equation is deduced.

2. **Notations.** We shall adhere to the following notations: small letters $a, b, \cdots$ are reserved for the rational integers, the capital letters $A, B, \cdots$ (except E) for integers of the algebraic number field $\mathfrak{F}$; the letter ϵ will be reserved for the units of this field, and all other Greek letters (with or without subscripts) will denote ideals of $\mathfrak{F}$.

Received by the editors March 24, 1944.

[1] E. T. Bell, *Reciprocal arrays and diophantine analysis*, Amer. J. Math. vol. 35 (1933) pp. 50–66.

Parentheses enclosing a letter denote the corresponding principal ideal; thus (X), (e), $\cdots$. The conjugates of the ideal ξ are represented by ξ', ξ'', $\cdots$, $\xi^{(n-1)}$. Two ideals, α and β, are said to be equivalent if an ideal γ exists such that the products $\alpha\gamma$, $\beta\gamma$ are both principal ideals; the equivalence of α and β is expressed by $\alpha\sim\beta$.

3. **Generalization of Lemma 1.** We shall now prove the following result.

THEOREM 1. *All integers X, Y, Z, W satisfying*

$$XY = ZW \tag{3.1}$$

are given by

$$X = ST/e, \qquad Y = UV/e, \qquad Z = SV/e, \qquad W = UT/e,$$

where S, T, U, V are arbitrary and e takes only the finite set of rational integral values each equal to the norm of a representative ideal from each class.

PROOF. By Lemma 1 all solutions of

$$(X)(Y) = (Z)(W) \tag{3.2}$$

are obtainable from

$$(X) = \alpha\beta, \qquad (Y) = \gamma\delta, \qquad (Z) = \alpha\delta, \qquad (W) = \gamma\beta,$$

and the ideals of the right-hand members must be restricted to the values which make the left-hand members principal ideals. Since the products $\alpha\beta$, $\gamma\beta$ are to be principal ideals then $\alpha\sim\gamma$. Let ξ be a representative ideal of each class in which α is a member. Then $\alpha\sim\xi$ and it follows that

$$\alpha\xi'\xi'' \cdots \xi^{(n-1)} \sim \xi\xi' \cdots \xi^{(n-1)} = (e).$$

Hence $\alpha\xi'\xi'' \cdots \xi^{(n-1)}$, and consequently $\gamma\xi'\xi'' \cdots \xi^{(n-1)}$, is equivalent to a principal ideal and must therefore itself be a principal ideal (A). Therefore,

$$(eX) = \alpha\beta\xi\xi' \cdots \xi^{(n-1)} = (A)\xi\beta$$

whence $\xi\beta$ is a principal ideal. Put $\xi\beta = (B)$ and we have $(eX) = (AB)$. Also

$$(eY) = \xi\xi' \cdots \xi^{(n-1)}\gamma\delta = (C)\xi\delta = (C)(D)$$

since $\xi\delta$ must be a principal ideal (D).

Thus all solutions of (3.2) are obtainable from

$$(eX) = (AB), \qquad (eY) = (CD), \qquad (eZ) = (AD), \qquad (eW) = (CB).$$

This implies that the set of all integers satisfying (3.1) is given by

$$eX = \epsilon_1 AB, \qquad eY = \epsilon_2 CD, \qquad eZ = \epsilon_3 AD, \qquad eW = \epsilon_4 CB,$$

where $\epsilon_1\epsilon_2 = \epsilon_3\epsilon_4$. Make the reversible substitution $A = \epsilon_1^{-1}S$, $B = T$, $D = \epsilon_1\epsilon_3^{-1}V$, $C = \epsilon_4^{-1}U$ and we have the required result.

4. **The equation** $X\overline{X} = z^{2n+1}$. Hereafter the field $\mathfrak{F}$ is an arbitrary quadratic number field and the conjugate of an integer X and an ideal α are denoted by $\overline{X}$ and $\bar{\alpha}$ respectively.

The following theorem will be verified by induction.

THEOREM 2. *All solutions of*

$$\alpha\bar{\alpha} = (z^{2n+1})$$

are given by

$$\alpha = \phi_1^{2n+1}\phi_2^{2n}\bar{\phi}_2\phi_3^{2n-1}\bar{\phi}_3^{2}\cdots\phi_{n+1}^{n+1}\bar{\phi}_{n+1}^{n}, \qquad (z) = \phi_1\bar{\phi}_1\phi_2\bar{\phi}_2\cdots\phi_{n+1}\bar{\phi}_{n+1}.$$

From this we can deduce the following result.[2]

THEOREM 3. *All solutions of*

$$X\,\overline{X} = z^{2n+1} \tag{4.1}$$

are given by

$$\begin{aligned} E^{2n+1}X &= \pm H_1^{2n+1}H_2^{2n}\overline{H}_2\cdots H_{n+1}^{n+1}\overline{H}_{n+1}^{n} \\ E^{2}z &= H_1\overline{H}_1H_2\overline{H}_2\cdots H_{n+1}\overline{H}_{n+1}, \end{aligned} \tag{4.2}$$

where $E = e_1^{n+1}e_2^{n}\cdots e_n^{2}$; $e_1, e_2, \cdots, e_n$ *each being equal to the norm of a representative ideal from each class.*

If we put $X = x + (-a)^{1/2}y$, then (4.1) becomes $x^2 + ay^2 = z^{2n+1}$ and equating rational and irrational parts we obtain from (4.2) an explicit representation for all rational integers satisfying this equation. Although in general the solution appears in rational form, yet for each value of a the indeterminates x, y, z can be expressed by a finite number of polynomials in integral parameters. For, for each value of a the parameter E has only a finite set of integral values and the requirement that the right-hand members of (4.2) be divisible by

[2] For an account of the investigations on equation $x^2 + ay^2 = z^n$ see L. E. Dickson, *History of the theory of numbers*, vol. 2, pp. 534–543; Th. Skolem, *Diophantische Gleichungen*, Berlin, 1938, pp. 64–68; J. V. Uspensky and M. A. Heaslet, *Elementary number theory*, 1939, pp. 389–396.

E^{2n+1}, E^2 respectively may be expressed by congruential conditions upon the coordinates of the integers H_i.

EXAMPLE. From Theorem 3 it follows that all the rational integers satisfying $x^2+47y^2=z^3$ are given by

$$E^3(x+(-47)^{1/2}y) = \pm H_1^3H_2^2\overline{H}_2, \qquad E^2z = H_1\overline{H}_1H_2\overline{H}_2,$$

where $E=e_1^2=1$, 2^2, 3^2 and H_1, H_2 are integers of $Ra(-47)^{1/2}$. It suffices to take H_2 primitive.

In order to select all integers from the above rational forms of x, y, z, it is necessary and sufficient to impose the following congruential conditions upon the coordinates of $H_1=r+sW$, $H_2=m+nW$ where $W=(1+(-47)^{1/2})/2$:

(i) $E=1$. If n even then r, s even; otherwise no restrictions on r, s.

(ii) $E=2^2$. m odd, n even, $s\equiv 2r\equiv 0 \pmod 8$; $m-4n\equiv 2 \pmod 4$, $r\equiv s\equiv 0 \pmod 4$; $m-4n\equiv 4 \pmod 8$, $r\equiv s\equiv 0, 2 \pmod 4$; $m-4n\equiv 8 \pmod{16}$, $r\equiv s\equiv 0, 2 \pmod 4$; $m-4n\equiv 0, \pm 16 \pmod{64}$, $r\equiv s \pmod 2$; $m-4n\equiv 32 \pmod{64}$ requires no restriction on r, s.

m odd, $m+5n\equiv 2 \pmod 4$, $r\equiv s\equiv 0 \pmod 4$; $m+5n\equiv 4 \pmod 8$, $r\equiv s\equiv 0 \pmod 4$; $m+5n\equiv 8 \pmod{16}$, $r\equiv 2s \pmod 4$; $m+5n\equiv 0, \pm 16 \pmod{64}$, r even; $m+5n\equiv 32 \pmod{64}$ requires no restriction on r and s.

(iii) $E=3^2$. $m(m+n)\not\equiv 0 \pmod 3$, $r\equiv s\equiv 0 \pmod 9$; $m-6n\equiv \pm 3 \pmod 9$, $r\equiv s\equiv 0 \pmod 9$; $m-6n\equiv \pm 9 \pmod{27}$, $r+s\equiv 0 \pmod 9$; $m-6n\equiv 0 \pmod{27}$, but $m-114n\not\equiv 0 \pmod{3^6}$, $r+s\equiv 0 \pmod 3$; $m-114n\equiv 0 \pmod{3^6}$ requires no restriction on r and s.

$m+7n\equiv \pm 3 \pmod 9$, $r\equiv s\equiv 0 \pmod 9$; $m+7n\equiv \pm 9 \pmod{27}$, $r\equiv 3s\equiv 0 \pmod 9$; $m+7n\equiv 0 \pmod{27}$ but $m+115n\not\equiv 0 \pmod{3^6}$, $r\equiv 0 \pmod 3$; $m+115n\equiv 0 \pmod{3^6}$ requires no restriction on r and s.

If in addition to the above n is even then r and s must both be even.

The above conditions were obtained by considering in turn the cases according as $H_2\overline{H}_2$ is divisible by $e_1, e_1^2, \cdots, e_1^6$.

For the proof of Theorem 2 we use the following two lemmas.

LEMMA 2. *All solutions of* $\alpha\bar{\alpha}=\gamma\beta\bar{\beta}$ *are given by* $\alpha=\theta_1\theta_2\theta_3$, $\beta=\theta_1\bar{\theta}_2$, $\gamma=\theta_3\bar{\theta}_3$.

LEMMA 3. *All solutions of* $\alpha\bar{\alpha}=\beta\gamma$ *are given by* $\alpha=\theta_1\theta_2\theta_3\theta_4$, $\beta=\theta_1\bar{\theta}_2\theta_3\bar{\theta}_3$, $\gamma=\bar{\theta}_1\theta_2\theta_4\bar{\theta}_4$.

The proof for Lemma 2 is exactly as given in a previous paper[3] where the indeterminates were integers of a unique factorization

[3] E. Rosenthall, *On some cubic diophantine equations*, Amer. J. Math. vol. 65 (1943) pp. 664–665.

quadratic field; Lemma 3 follows immediately by a repeated application of Lemma 1.

5. **Proof of Theorem 2.** We now show independently that Theorem 2 holds for $n=1$ and then complete the proof by mathematical induction. From Lemma 2 it follows that all α, (z) satisfying $\alpha\bar{\alpha}=(z^2)$ are obtainable from

$$\alpha = \theta_1\theta_2\theta_3, \qquad (z) = \theta_1\bar{\theta}_2 = \theta_3\bar{\theta}_3,$$

and applying Lemma 3 it follows that

$$\theta_3 = \lambda_1\lambda_2\lambda_3\lambda_4, \qquad \theta_1 = \lambda_1\bar{\lambda}_2\lambda_3\bar{\lambda}_3, \qquad \bar{\theta}_2 = \bar{\lambda}_1\lambda_2\lambda_4\bar{\lambda}_4.$$

Then

$$\alpha = \phi_1^3\phi_2^2\bar{\phi}_2, \qquad (z) = \phi_1\bar{\phi}_1\phi_2\bar{\phi}_2,$$

where we have put $\lambda_1=\phi_1$, $\bar{\lambda}_2\lambda_3\lambda_4=\phi_2$ since λ_2, λ_3, λ_4 always appear in this product form.

Now consider the induction from $n=s$ to $n=s+1$. Apply Lemma 2 to $\alpha\bar{\alpha}=(z^{2s+3})=(z^{2s+1})(z)(z)$. Then

$$\alpha = \theta_1\theta_2\theta_3, \qquad (z) = \theta_1\bar{\theta}_2, \qquad (z^{2s+1}) = \theta_3\bar{\theta}_3.$$

By hypothesis, Theorem 2 holds for the last equation. Hence

$$\theta_3 = \mu_1^{2s+1}\mu_2^{2s}\bar{\mu}_2\cdots\mu_{s+1}^{s+1}\bar{\mu}_{s+1}^{s}, \qquad (z) = \mu_1\bar{\mu}_1\mu_2\bar{\mu}_2\cdots\mu_{s+1}\bar{\mu}_{s+1};$$

and equating the two parametric representations for (z) we obtain the following equations for all the parameters concerned,

$$\{\mu_1\mu_2\cdots\mu_{s+1}\}\{\bar{\mu}_1\bar{\mu}_2\cdots\bar{\mu}_{s+1}\} = \theta_1\bar{\theta}_2.$$

Applying Lemma 3,

$$\mu_1\mu_2\cdots\mu_{s+1} = \lambda_1\lambda_2\lambda_3\lambda_4, \qquad \theta_1 = \lambda_1\bar{\lambda}_2\lambda_3\bar{\lambda}_3, \qquad \bar{\theta}_2 = \bar{\lambda}_1\lambda_2\lambda_4\bar{\lambda}_4.$$

Substituting these values of the parameters in the preceding formulas for α, (z) gives

$$(5.1) \qquad \alpha = \lambda_1^2\bar{\lambda}_2^2\psi_1\bar{\psi}_1\mu_1^{2s+1}\mu_2^{2s}\bar{\mu}_2\cdots\mu_{s+1}^{s+1}\bar{\mu}_{s+1}^{s}, \qquad (z) = \lambda_1\bar{\lambda}_1\lambda_2\bar{\lambda}_2\psi_1\bar{\psi}_1,$$

where the parameters must satisfy the multiplicative equation

$$(5.2) \qquad \mu_1\mu_2\cdots\mu_{s+1} = \lambda_1\lambda_2\psi_1,$$

where we have put $\lambda_3\lambda_4=\psi_1$.

Applying the method of arrays[4] to (5.2) we obtain

[4] See E. T. Bell, *loc. cit.*, p. 62.

$$\mu_1 = \xi_1\eta_1\zeta_1, \qquad \lambda_1 = \xi_1\xi_2 \cdots \xi_{s+1},$$
$$\mu_2 = \xi_2\eta_2\zeta_2, \qquad \lambda_2 = \eta_1\eta_2 \cdots \eta_{s+1},$$
$$\cdots\cdots\cdots, \qquad \psi_1 = \zeta_1\zeta_2 \cdots \zeta_{s+1}.$$
$$\cdots\cdots\cdots,$$
$$\mu_{s+1} = \xi_{s+1}\eta_{s+1}\zeta_{s+1}.$$

Finally, substituting in (5.1) gives

$$\alpha = \phi_1^{2s+3}\phi_2^{2s+2}\bar{\phi}_2 \cdots \phi_{s+1}^{s+3}\bar{\phi}_{s+1}^{s}\phi_{s+2}^{s+2}\bar{\phi}_{s+2}^{s+1}, \qquad (z) = \phi_1\bar{\phi}_1\phi_2\bar{\phi}_2 \cdots \phi_{s+2}\bar{\phi}_{s+2},$$

where we have put $\xi_1=\phi_1$, $\xi_2\zeta_1=\phi_2$, $\zeta_{s+1}\eta_s\bar{\eta}_{s+1}=\phi_{s+2}$, and $\xi_i\zeta_{i-1}\eta_{i-2}=\phi_i$ for $i=3, 4, \cdots, s+1$, since the parameters always occur in these product forms. This completes the induction.

6. **Proof of Theorem 3.** All solutions of

$$(X)(\overline{X}) = (z^{2n+1}) \tag{6.1}$$

are obtainable from

$$(X) = \phi_1^{2n+1}\phi_2^{2n}\bar{\phi}_2 \cdots \phi_{n+1}^{n+1}\bar{\phi}_{n+1}^{n}, \quad (z) = \phi_1\bar{\phi}_1\phi_2\bar{\phi}_2 \cdots \phi_{n+1}\bar{\phi}_{n+1}, \tag{6.2}$$

and the ideals of the right-hand members must be restricted to those values which make the left-hand members principal ideals. From $(6.2)_1$ it follows that $\phi_1^{2n+1}\phi_2^{2n-1} \cdots \phi_{n+1} \sim (1)$. Let ξ_i $(i=1, 2, \cdots, n)$ be a representative ideal from each of the classes in which ϕ_i is a member. Then we can put $\phi_i\bar{\xi}_i=(H_i)$ and $\xi_1^{2n+1}\xi_2^{2n-1} \cdots \xi_n^3\phi_{n+1}=(H_{n+1})$. Multiplying both sides of $(6.2)_1$ by $[\{\xi_1\bar{\xi}_1\}^{n+1}\{\xi_2\bar{\xi}_2\}^{n} \cdots \{\xi_n\bar{\xi}_n\}^{2}]^{2n+1}$ and $(6.2)_2$ by $[\{\xi_1\bar{\xi}_1\}^{n+1}\{\xi_2\bar{\xi}_2\}^{n} \cdots \{\xi_n\bar{\xi}_n\}^{2}]^{2}$ and also putting $\xi_i\bar{\xi}_i=(e_i)$ we obtain

$$(E^{2n+1}X) = (H_1^{2n+1}H_2^{2n}\overline{H}_2 \cdots H_{n+1}^{n+1}\overline{H}_{n+1}^{n}),$$
$$(E^{2}z) = (H_1\overline{H}_1H_2\overline{H}_2 \cdots H_{n+1}\overline{H}_{n+1})$$

for all solutions of (6.1). This implies that all solutions of (4.1) are given by

$$E^{2n+1}X = \epsilon_1H_1^{2n+1}H_2^{2n}\overline{H}_2 \cdots H_{n+1}^{n+1}\overline{H}_{n+1}^{n}, \qquad E^{2}z = \epsilon_2H_1\overline{H}_1 \cdots H_{n+1}\overline{H}_{n+1}.$$

Make the reversible substitution $H_{n+1}=\bar{\epsilon}_1H_{n+1}$, and then observe that $\epsilon_2\epsilon_1\bar{\epsilon}_1$ must be unity. Hence Theorem 3 is proved.

McGILL UNIVERSITY