ON THE SOLUTION OF DIOPHANTINE EQUATIONS BY MEANS OF IDEALS*

BY G. E. WAHLIN

1. *Introduction.* In a previous article† I considered the application of the theory of ideals to diophantine analysis. At suggestions from Professors Dickson and Hedrick I have undertaken to make a study of the applications of the theory to problems of less general type than the one considered in that article. In this paper we shall consider diophantine equations in which one member is a binary quadratic form.

Since the publication of the previous article, I have noticed that, with a slight modification in the development, we could have obtained a theory for the solution of equations in which the left hand member is a more general decomposable form. This generalization would not involve any additional difficulty. In the following pages I have made use of this fact and have thus gained the advantage that, in the equations here considered, the only restriction imposed upon the binary quadratic form, used as the left hand member of the equation, is that its discriminant shall not be a perfect square.

In making the modification I have found it necessary to change the definition of a ring ideal from the one previously used in which we had the condition that a ring ideal is always relatively prime to the conductor. This restriction has been removed. Those ring ideals which are relatively prime to the conductor shall be called *regular* ring ideals. Since the properties of ring ideals as developed in Bachmann‡ apply only to regular ring ideals, it has

* Presented to the Society December 26, 1924.

† This BULLETIN, vol. 30, Nos. 3–4 (Mch.–Apr., 1924), p. 140. We shall refer to this article by the symbol (W).

‡ *Allgemeine Arithmetik der Zahlenkörper.*

been found necessary to insert the proof of a property of ring ideals in general. In speaking of equivalent ring ideals and classes of ring ideals, let it be understood that this refers only to regular ring ideals.

The theorems of §§ 2, 3, 4 of (W) refer only to regular ring ideals. Article 2 of the present paper is devoted to a general property of ring ideals. It is a modification of the development on pp. 152–3 of (W), and is used to simplify the following development.* As in (W) $\{\gamma\}$ is a principal field ideal and $[\gamma]$ is a principal ring ideal. Δ is used to denote the index and f the conductor of a ring.

2. *A General Property of Ring Ideals.* In this section I shall give a proof of the following theorem.

THEOREM I. *Let $\mathfrak{M}$ be an ideal of a ring R in an algebraic number field of degree n and γ an integer of $\mathfrak{M}$. Let $\{\gamma\} = T \cdot P_k$ where T is a field ideal relatively prime to $\mathfrak{M} \cdot f$, and P_k a field ideal whose prime ideal divisors are all divisors of $\mathfrak{M} \cdot f$. Then, if c is any rational integer divisible by $\mathfrak{M}$ and I a field ideal relatively prime to $\{c\Delta\}$ and belonging to the class reciprocal to that of T, we have $N(I) \cdot P_k / I = \{\gamma^{(k)}\}$ where $\gamma^{(k)}$ is an integer belonging to $\mathfrak{M}$.*

This theorem is obviously true if P_k is divisible by f, but requires a proof if this condition is not fulfilled. The proof does not, however, preclude this condition.

We shall denote by $\mathfrak{G}$ the unit ideal of the field. Since $\mathfrak{G}\mathfrak{M} \cdot f = \mathfrak{M}\mathfrak{G}f = \mathfrak{M} \cdot f$, $\mathfrak{M}f$ is a field ideal. As stated above let γ be any integer of $\mathfrak{M}$ and $\{\gamma\} = T \cdot P_k$ where T and P_k are field ideals satisfying the given condition. Since T is relatively prime to $\mathfrak{M}f$, it is relatively prime to f and hence there is a corresponding regular ring ideal $T^{(R)}$. From the ring class reciprocal to that of $T^{(R)}$ select an ideal $I^{(R)}$ such that the corresponding field ideal I is relatively prime to $\{c\Delta\}$. The possibility of such a choice

* By making use of the theorem of § 2 below, the development of (W) can be made without the introduction of the ideal I and the rational integer M_2.

of $I^{(R)}$ was shown in § 3, (W). $I^{(R)}$ is then relatively prime to $\mathfrak{M}f$ which is a divisor of $\{c\Delta\}$ and is also a ring ideal.

Denote the norm of I by M. Since M and $c\Delta$ are rational integers and I is relatively prime to $\{c\Delta\}$, M and $c\Delta$ are relatively prime, because if M and $c\Delta$ have a common factor let p be a rational prime which divides both M and $c\Delta$, some ideal prime factor of p must be a dividor of I and hence a common factor of I and $\{c\Delta\}$ contrary to our assumption regarding I. Hence $I_k = \{M\}/I$ is also relatively prime to $\{c\Delta\}$ and hence also to $\mathfrak{M}f$ and the corresponding ring ideal $I_k^{(R)}$ is regular.

Since

$$I_k \cdot I = \{M\}, \qquad I_k^{(R)} \cdot I^{(R)} = [M];$$

and since $I^{(R)}$ and $T^{(R)}$ belong to reciprocal classes in R, $I^{(R)} \cdot T^{(R)} = [\alpha]$, where $[\alpha]$ is regular. Multiplying both members of the last equation by $\mathfrak{G}$, we have $T \cdot I = \{\alpha\}$; and since T and I are both relatively prime to $\mathfrak{M}f$, we have

$$\mathfrak{M}f + \{\alpha\} = \{1\} = \mathfrak{G}.$$

Hence $\mathfrak{M}f + [\alpha]$ is the unit ideal of R. The ideals I_k and T belong to the same class, namely the one reciprocal to that of I; hence I_k and P_k belong to reciprocal classes and $I_k \cdot P_k = \{\gamma^{(k)}\}$.

We shall next see that with I_k as defined, the integer $\gamma^{(k)}$ may be chosen from $\mathfrak{M}$. $T \cdot P_k = \{\gamma\}$ where γ belongs to $\mathfrak{M}$. Since M is a rational integer $M\gamma$ belongs to $\mathfrak{M}$. If we then write

$$I_k P_k = \frac{\{M\}}{I} P_k = \frac{\{M\} T \cdot P_k}{IT} = \left\{\frac{M\gamma}{\alpha}\right\} = \{\gamma^{(k)}\},$$

we may choose $\gamma^{(k)} = M\gamma/a$; hence $\alpha\gamma^{(k)} = M\gamma$, and therefore $\alpha\gamma^{(k)}$ belongs to $\mathfrak{M}$. Therefore if a be any integer from $[\alpha]$, $a\gamma^{(k)}$ belongs to $\mathfrak{M}$. If b be any integer from $\mathfrak{M}f$ then $b\gamma^{(k)}$ belongs to $\mathfrak{M}f$ and hence to $\mathfrak{M}$. From this it follows that $(a+b)\gamma^{(k)}$ belongs to $\mathfrak{M}$. But we have seen that $\mathfrak{M}f + [\alpha] = [1]$; hence a and b may be so chosen that $a + b = 1$ and therefore $\gamma^{(k)}$ belongs to $\mathfrak{M}$.

3. *Preliminary Computations for Rings in a Quadratic Field.* From now on we shall be concerned only with quadratic fields. The development of this article is that corresponding to § 2 of (W).

Let us consider a ring R in a quadratic number field $k(\sqrt{\mu})$. Let $(1, \varrho)$ be a fundamental system of R, so that all its numbers may be written in the form $x+y\varrho$, where x and y are rational integers. As in § 2 of (W), we can then write

$$\varrho^t = C_1^{(t)} + C_2^{(t)}\varrho,$$

and if ϱ is a root of the equation $x^2 - mx - n = 0$ we have

$$\varrho^2 = n + m\varrho. \tag{1}$$

We therefore see that

$$C_1^{(0)} = 1, \qquad C_1^{(1)} = 0, \qquad C_1^{(2)} = n,$$
$$C_2^{(0)} = 0, \qquad C_2^{(1)} = 1, \qquad C_2^{(2)} = m.$$

Multiplying both members of

$$\varrho^{t-1} = C_1^{(t-1)} + C_2^{(t-1)}\varrho$$

by ϱ and substituting for ϱ^2 its value from (1), we have

$$\varrho^t = C_2^{(t-1)} \cdot n + (C_1^{(t-1)} + m \cdot C_2^{(t-1)})\varrho,$$

whence we have the recursion formulas

$$C_1^{(t)} = n \cdot C_2^{(t-1)}, \qquad C_2^{(t)} = C_1^{(t-1)} + m \cdot C_2^{(t-1)}. \tag{2}$$

From this, if $\alpha^{(i)} = a_{1i} + a_{2i}\varrho$, we obtain

$$\begin{aligned}\alpha^{(1)} \cdot \alpha^{(2)} \cdots \alpha^{(k-1)} &= B_0^{(k-1)} + B_1^{(k-1)}\varrho + \cdots + B_{k-1}^{(k-1)}\varrho^{k-1} \\ &= A_1^{(k-1)} + A_2^{(k-1)}\varrho,\end{aligned}$$

where

$$A_1^{(k-1)} = \sum_{i=0}^{k-1} C_1^{(i)} B_i; \qquad A_2^{(k-1)} = \sum_{i=0}^{k-1} C_2^{(i)} B_i.$$

We note also that

$$\begin{aligned}(A_1^{(k-1)} + A_2^{(k-1)}\varrho)(a_{1k}a + a_{2k}\varrho) &= (a_{1k}A_1^{(k-1)} \cdot a + a_{2k}A_2^{(k-1)} \cdot n) \\ &\quad + (a_{1k}A_2^{(k-1)} \cdot a + a_{2k}A_1^{(k-1)} + a_{2k}A_2^{(k-1)} \cdot m)\varrho.\end{aligned}$$

4. *Quadratic Forms.* We shall next consider the binary quadratic form $ax^2+bxy+cy^2$ in which a, b, c are rational integers, $a>0$ and $b^2-4ac = g^2\mu$, where $\mu \neq 0$ or 1 and has no square factor. This form we shall denote by $Q(x, y)$, so that

$$a \cdot Q(x, y) = (ax+\varrho y)(ax+\varrho' y), \tag{3}$$

where $\varrho = (b+g\sqrt{\mu})/2$ and $\varrho' = (b-g\sqrt{\mu})/2$.

The numbers ϱ and ϱ' are the roots of the equation

$$x^2-bx+ac = 0. \tag{4}$$

Let us consider all numbers of the form $x+y\varrho$, where x and y are rational integers. Since the sum or difference of two such numbers is a number of the same form, they constitute a modul. Moreover it is easily shown that the product of two of these numbers is a number of the same form, and since for $x = 1$, $y = 0$ we get the number 1, we see that the modul is a ring R of which $(1, \varrho)$ is a fundamental system.

If we next consider all numbers of the form $ax+\varrho y$, they also constitute a modul $\mathfrak{M}$ in R and

$$\begin{aligned}(ax_1+\varrho y_1)(x_2+\varrho y_2) &= ax_1x_2+(ax_1y_2+x_2y_1)\varrho+y_1y_2\varrho^2 \\ &= a(x_1x_2-cy_1y_2)+\varrho(ax_1y_2+x_2y_1+by_1y_2).\end{aligned}$$

Hence the product of any number of $\mathfrak{M}$ by a number of R is a number of $\mathfrak{M}$, and $\mathfrak{M}$ is therefore an ideal in R. The ideal $\mathfrak{M}$ has the fundamental system (a, ϱ).

Since

$$a = a\cdot 1+0\cdot\varrho, \qquad \varrho = 0\cdot 1+1\cdot\varrho,$$

$$\begin{vmatrix} a & 0 \\ 0 & 1 \end{vmatrix} = a$$

is the norm of the ideal $\mathfrak{M}$.

We shall next determine the index and conductor of R. Let $(1, \theta)$ be a fundamental system of $k(\sqrt{\mu})$. Then $\theta = \sqrt{\mu}$ if $\mu \equiv 2$ or 3 (mod 4) and $\theta = (1+\sqrt{\mu})/2$ if $\mu \equiv 1$ (mod 4). Let us consider the case when $\mu \equiv 2$ or 3 (mod 4). Then

$$(5) \qquad 1 = 1\cdot 1+0\cdot\theta, \qquad \varrho = \frac{b}{2}\cdot 1+\frac{g}{2}\cdot\theta.$$

Now $g^2\mu \equiv 0$ or $\mu \pmod 4$ and $b^2-4ac \equiv 0$ or $1 \pmod 4$. But $g^2\mu = b^2-4ac$, and hence if $\mu \not\equiv 1 \pmod 4$, $b^2-4ac \not\equiv 1 \pmod 4$, so that $g^2\mu \equiv 0 \pmod 4$ and g is even; hence also b is even and $b/2$ and $g/2$ are integers. From (5) we see that $\Delta = g/2$. In the case where $\mu \equiv 1 \pmod 4$, if $g^2 \equiv 0 \pmod 4$ also $b^2 \equiv 0 \pmod 4$, and if $b^2 \equiv 0 \pmod 4$ also $g^2 \equiv 0 \pmod 4$; hence b and g are simultaneously even or odd. We may then write

$$(6) \qquad 1 = 1\cdot 1+0\cdot\theta, \qquad \varrho = \frac{b-g}{2}+g\theta$$

and see that in this case $\Delta = g$. The conductor f of R is the totality of all integers of $k(\sqrt{\mu})$ such that the product of any integer of $k(\sqrt{\mu})$ by any integer of f belongs to R. Any integer of the field can be written in the form

$$(7) \qquad x+\theta y = x-\frac{b}{g}y+\frac{2y}{g}\varrho = \frac{gx-by}{g}+\frac{2y}{g}\varrho,$$

when $\mu \equiv 2$ or $3 \pmod 4$, and

$$(8) \qquad x+\theta y = x-\frac{b-g}{2g}y+\frac{y}{g}\varrho = \frac{2gx-by+gy}{2g}+\frac{y}{g}\varrho$$

when $\mu \equiv 1 \pmod 4$.

The question then remains to determine the nature of an integer α if $\alpha(x+y\theta) = \xi+\varrho\eta$, where ξ and η are rational integers. Since f is contained in R, α must be of the form $u+v\varrho$; hence when $\mu \equiv 2$ or $3 \pmod 4$, we have

$$\begin{aligned}\alpha(x+y\theta) &= u\cdot\frac{gx-by}{g}+\frac{2uy+gvx-bvy}{g}\varrho+\frac{2vy}{g}\varrho^2 \\ &= \frac{u(gx-by)-2vyac}{g}+\frac{v(gx-by)+2uy+2bvy}{g}\varrho.\end{aligned}$$

It follows that u and v must be such that

$$\begin{aligned} u(gx-by)-2vyac &\equiv 0 \pmod g, \\ v(gx-by)+2uy+2bvy &\equiv 0 \pmod g; \end{aligned}$$

and since b and g are both even, this reduces to

$$(9)\qquad \frac{b}{2}u+acvy \equiv 0, \qquad yu+\frac{b}{2}vy \equiv 0, \qquad (\text{mod } g/2).$$

Since y is arbitrary and hence in general not divisible by a factor of $g/2$, it may be divided out, and we have

$$\frac{b}{2}u+acv \equiv 0, \qquad u+\frac{b}{2}v \equiv 0, \qquad (\text{mod } g/2).$$

Since $b^2/4 \equiv ac \pmod{(g/2)^2}$, we see that the first congruence is obtained from the second by multiplying it by $b/2$ and hence any values of u and v which satisfy the second congruence also satisfy the first. We may therefore write $u = w\cdot g/2 - v\cdot b/2$, and hence

$$u+v\varrho = w\cdot\frac{g}{2}-v\cdot\frac{b}{2}+v\cdot\frac{b}{2}+v\cdot\frac{g}{2}\sqrt{\mu} = \frac{g}{2}(w+v\sqrt{\mu});$$

hence α must be a multiple of $g/2$. Moreover as is easily seen from (7), any integer of the field times $g/2$ is an integer of R. Therefore f is contained in $\{g/2\}$, and $\{g/2\}$ is contained in f, so that $f = \{g/2\}$.

In the case where $\mu \equiv 1 \pmod 4$, (8) shows that g, and hence also $\{g\}$, is contained in f. Again, let $u+v\varrho$ be any integer of f. Then

$$(u+v\varrho)(x+\theta y) = \frac{(2gx-by+gy)u-2acvy}{2g} + \frac{(2gx-by+gy)v+2uy+2bvy}{2g}\varrho,$$

and, as above, this leads to the congruences

$$(b-g)u+2acv \equiv 0, \quad 2u+(b+g)v \equiv 0, \quad (\text{mod } 2g);$$

or, since b and g are simultaneously odd or even,

$$(10)\qquad \frac{b-g}{2}u+acv \equiv 0, \qquad u+\frac{b+g}{2}v \equiv 0, \quad (\text{mod } g).$$

Multiplying the second congruence by $(b-g)/2$, we have

$$\frac{b-g}{2}\cdot u+\frac{b^2-g^2}{4}v \equiv 0 \qquad (\text{mod } g).$$

But $b^2-4ac = g^2\mu$ and hence $b^2-g^2 = 4ac+g^2(\mu-1) \equiv 4ac \pmod{4g^2}$ since $\mu-1 \equiv 0 \pmod 4$; and therefore $(b^2-g^2)/4 \equiv ac \pmod g$. Again we see that any pair of values of u and v which satisfy the second congruence will also satisfy the first, and we may therefore write

$$u = wg - \frac{b+g}{2}\cdot v$$

and

$$u+v\varrho = wg - \frac{b+g}{2}\cdot v + \frac{b}{2}\cdot v + \frac{vg}{2}\sqrt{\mu}$$

$$= g\left(w + v\frac{1+\sqrt{\mu}}{2}\right) = g(w+v\theta).$$

Hence f is contained in $\{g\}$; and, as above, we conclude that $f = \{g\}$.

EXAMPLE. As an example of the foregoing, let us consider the form $Q(x, y) = 11x^2+5xy+2y^2$. The discriminant is -63; hence $g = 3$, $\mu = -7$, $\mu \equiv 1 \pmod 4$, $\Delta = 3$, $f = \{3\}$, $\varrho = (5+3\sqrt{-7})/2$, $R = (1, \varrho)$ and $\mathfrak{M} = (11, (5+3\sqrt{-7})/2)$. The number of classes in $k(\sqrt{-7})$ is one and in R it is four. If we denote the principal class of R by C_0 and the others by C_1, C_2, C_3, the following table gives a representative ideal for each class, the reciprocal class, and a binary quadratic form from the corresponding class of forms. To save space, the computations have been omitted.

Class	Representative ideal	Corresponding form	Reciprocal class	Representative ideal
C_0	$\left[1, \frac{5+3\sqrt{-7}}{2}\right]$	$x^2+5xy+22y^2$	C_0	$\left[1, \frac{5+3\sqrt{-7}}{2}\right]$
C_1	$\left[2, \frac{5+3\sqrt{-7}}{2}\right]$	$2x^2+5xy+11y^2$	C_2	$\left[2, \frac{5-3\sqrt{-7}}{2}\right]$
C_2	$\left[2, \frac{5-3\sqrt{-7}}{2}\right]$	$2x^2+5xy+11y^2$	C_1	$\left[2, \frac{5+3\sqrt{-7}}{2}\right]$
C_3	$\left[7, \frac{7+3\sqrt{-7}}{2}\right]$	$7x^2+7xy+4y^2$	C_3	$\left[7, \frac{7+3\sqrt{-7}}{2}\right]$

5. *Application to Diophantine Equations.* We shall now turn our attention to the study of the diophantine equation

$$Q(x, y) = u_1 u_2 \cdots u_{k-2}, \tag{11}$$

where it is required to determine the rational integral values of $x, y, u_1, u_2, \cdots u_{k-2}$ which satisfy the equation. Obviously the equation may be written in the form

$$N(ax+\varrho y) = a u_1 u_2 \cdots u_{k-2}. \tag{12}$$

Following the procedure in (W), with the modification that $P_1, P_2, \cdots, P_{k-2}$ are constructed from prime ideals relatively prime to $\mathfrak{M}f$, we can show in the same manner that $u_i = \epsilon_i \mu_1' \cdot \mu_i'' F_i(e_1^{(i)}, e_2^{(i)})$.

Before writing down the expressions for x and y, I shall make some observations regarding μ_i', and μ_i''. $|\mu_i' \cdots \mu_{k-2}'| = N(P_{k-1})$ where P_{k-1} is relatively prime to $\mathfrak{M}f$, but no μ_i' is itself the norm of an ideal. Hence each μ_i' contains only the first powers of such rational primes as are primes in $k(\sqrt{\mu})$ and every such prime must occur in an even number of the μ_i'. But since these primes are relatively prime to f and hence also to Δ, $x+\varrho y$ cannot contain such factors unless the x and y are both divisible by the prime, because with respect to such a prime as a modulus ϱ cannot satisfy a congruence of lower than the second degree. But such a solution can always be obtained from one in which the x and y do not have this common factor by multiplying it into x and y and any two of μ_i'. There is therefore no loss in assuming that $P_{k-1} = \{1\}$ and $I_{k-1} = \{1\}$; and hence $\alpha^{(k-1)} = +1$. This makes it possible to make $\mu_i' = +1$, $(i = 1, 2, \cdots, k-2)$, and in so doing we have in no way restricted the solution.

In accordance with what was stated above $P_1, P_2, \cdots, P_{k-2}$ are all relatively prime to $\mathfrak{M}f$ and P_k contains no ideal prime factors except such as are factors of $\mathfrak{M}f$. In writing the equation in the form (12) the factor a was introduced on the right hand side of the equation and now

$$N(P_k) = |a\mu_1'' \cdot \mu_2'' \cdots \mu_{k-2}''|, \qquad \text{where } a = N_R(\mathfrak{M}).$$

If we now use the method of (W) and the formulas in § 3 above, when we put $\gamma^{(k)} = a_{1k}a + a_{2k}\varrho$, we have the following formulas for the solutions of (11):

$$(13)\quad \begin{cases} x = \dfrac{1}{M}(a_{1k}A_1^{(k-2)} - a_{2k}A_2^{(k-2)} \cdot c), \\ y = \dfrac{1}{M}(a_{1k}A_2^{(k-2)} \cdot a + a_{2k}A_1^{(k-2)} + a_{2k}A_2^{(k-2)} \cdot b), \end{cases}$$

where $M = N(I_1 \cdot I_2 \cdots I_{k-2})$ as in (W);

$$(14)\qquad \mu_i = \varepsilon_i \mu_i'' F_i(e_1^{(i)}, e_2^{(i)}), \quad (i = 1, 2, \cdots, k-2),$$
$$\varepsilon_1 \varepsilon_2 \cdots \varepsilon_{k-2} = +1.$$

In these formulas the upper index on the A_i is $k-2$ in place of $k-1$ due to the fact that $\alpha^{(k-1)}$ was chosen equal to $+1$.

If $(\beta_1^{(i)}, \beta_2^{(i)})$ is a fundamental system of the ring ideal $I_i^{(R)}$ and

$$\beta_1^{(i)} = b_{11}^{(i)} + b_{12}^{(i)}\varrho, \qquad \beta_2^{(i)} = b_{21}^{(i)} + b_{22}^{(i)}\varrho,$$

we have, if $\alpha^{(i)} = a_{1i} + a_{2i}\varrho = e_1^{(i)}\beta_1 + e_2^{(i)}\beta_2$ is any integer of $I_i^{(R)}$,

$$(15)\quad a_{1i} = b_{11}^{(i)}e_1^{(i)} + b_{21}^{(i)}e_2^{(i)}, \qquad a_{2i} = b_{12}^{(i)}e_1^{(i)} + b_{22}^{(i)}e_2^{(i)}.$$

By means of (15) for $i = 1, 2, \cdots, k-2$ the expressions (13) for x and y may be obtained in terms of the parameters $e_1^{(i)}, e_2^{(i)}$, $i = 1, 2, \cdots, k-2$. The a_{1k} and a_{2k} are also parameters which enter into the expressions for the μ_i in the factors μ_i''.

The complete development of the foregoing part of this section is identical with that given in (W) except that here the $P_1, P_2, \cdots, P_{k-2}$ are all relatively prime to $\mathfrak{M}f$ and due to the development of § 2 above, the introduction of the ideal J and the rational integer M_2 is not needed. This is also true for (W) but I did not see it at the time.

The results can now be summarized in the following statement of a method for obtaining the solutions of (11). Select any integer γ from $\mathfrak{M} = (a, \varrho)$, and separate $\{\gamma\}$ into the product of two field ideals P_k and T, where T is relatively prime to $\mathfrak{M}f$ and P_k contains no prime factors

except such as are divisors of $\mathfrak{M}f$. Separate T into the product of $k-2$ field ideals $P_1, P_2, \cdots, P_{k-2}$ in any way and let $P_i^{(R)}$ be the ring ideal corresponding to P_i. From the ring class reciprocal to that of $P_i^{(R)}$ select an ideal $I_i^{(R)}$ which is such that the corresponding field ideal I_i is relatively prime to $\{a\Delta\}$ and put $I = I_1 \cdot I_2 \cdots I_{k-2}$. Let $N(I) = M$ and $I_k = \{M\}/I$ and $I_k \cdot P_k = \{\gamma^{(ik)}\} = a_{1k} + a_{2k}\varrho$ by § 2. Let $F_i(x, y)$ be the binary quadratic form corresponding to the base $(\beta_1^{(i)}, \beta_2^{(i)})$ of $I_i^{(R)}$. Then the formulas (13) and (14) by means of relations (15) for $\varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{k-2} = +1$ give solutions for (11) in terms of the parameters $e_1^{(i)}$, $e_2^{(i)}$ with the signs of the μ_i'' so chosen that the sign of their product is the same as that of $N(\gamma^{(ik)})$.

By a variation in the separation of T into factors or by a variation in the choice of γ so that different classes are represented by $P_1^{(R)}, P_2^{(R)}, \cdots, P_{k-2}^{(R)}$ we can obtain all solutions of the equation. The values given to the parameters are rational integral and all solutions so obtained are rational integers.

EXAMPLE. Let us consider the equation

$$11x^2 + 5xy + 2y^2 = u_1 \cdot u_2 \cdot u_3.$$

Here $\mathfrak{M} = (11, (5+3\sqrt{-7})/2)$. Select, from $\mathfrak{M}$, $\gamma = 11 + 2(5+3\sqrt{-7})/2 = 16+3\sqrt{-7}$;

$$\{\gamma\} = \{2-\sqrt{-7}\}\{1+2\sqrt{-7}\}, \quad P_5 = \{2-\sqrt{-7}\}, \quad T = \{1+2\sqrt{-7}\}.$$

T is a prime ideal and hence its separation into $P_1 \cdot P_2 \cdot P_3$ gives $P_1 = \{1+2\sqrt{-7}\}$, $P_2 = \{1\}$, $P_3 = \{1\}$,

$$P_1^{(R)} = \left(29, \frac{13-3\sqrt{-7}}{2}\right), \quad P_2^{(R)} = \left(1, \frac{5+3\sqrt{-7}}{2}\right), \quad P_3^{(R)} = \left(1, \frac{5+3\sqrt{-7}}{2}\right).$$

$P_1^{(R)}$ belongs to the class C_1 (see table in § 4). $P_2^{(R)}$ and $P_3^{(R)}$ belong to class C_0.

$$I_1^{(R)} = \left(2, \frac{5-3\sqrt{-7}}{2}\right), \qquad F_1(x, y) = 2x^2+5xy+11y^2,$$

$$I_2^{(R)} = \left(1, \frac{5+3\sqrt{-7}}{2}\right), \qquad F_2(x, y) = x^2+5xy+22y^2,$$

$$I_3^{(R)} = \left(1, \frac{5+3\sqrt{-7}}{2}\right), \qquad F_3(x, y) = x^2+5xy+22y^2,$$

$$I_1 = \left\{\frac{1+\sqrt{-7}}{2}\right\}, \qquad I_2 = \{1\}, \quad I_3 = \{1\},$$

$$I = I_1 \cdot I_2 \cdot I_3 = I_1, \qquad M = N(I) = 2,$$

$$I_5 = \{M\}/I = I_1' = \frac{1-\sqrt{-7}}{2},$$

$$I_5 \cdot P_5 = \left\{\frac{1-\sqrt{-7}}{2}\right\}\{2-\sqrt{-7}\} = \left\{-\frac{5+3\sqrt{-7}}{2}\right\} = \{\gamma^{(5)}\};$$

$\gamma^{(5)}$ is an integer of $\mathfrak{M}$. The sign may be neglected.

The linear forms used in computing (13) and (14), after application of (15), become

$$\alpha' = 2e_1^{(1)} + \frac{5-3\sqrt{-7}}{2} e_2^{(1)},$$

$$\alpha'' = e_1^{(2)} + \frac{5+3\sqrt{-6}}{2} e_2^{(2)},$$

$$\alpha''' = e_1^{(3)} + \frac{5+3\sqrt{-7}}{2} e_2^{(3)},$$

$$\alpha' \cdot \alpha'' \cdot \alpha''' \gamma^{(5)} = 11 \cdot 2x + \varrho \cdot 2y,$$

from which we have

$$\begin{aligned} x = {} & e_2^{(1)}e_1^{(2)}e_1^{(3)} - 2e_1^{(1)}e_2^{(2)}e_1^{(3)} - 2e_1^{(1)}e_1^{(2)}e_2^{(3)} \\ & - 10e_1^{(1)}e_2^{(2)}e_2^{(3)} - 22e_2^{(1)}e_2^{(2)}e_2^{(3)}, \\ y = {} & e_1^{(1)}e_1^{(2)}e_1^{(3)} + 5e_1^{(1)}e_2^{(2)}e_1^{(3)} + 11e_2^{(1)}e_2^{(2)}e_1^{(3)} + 5e_1^{(1)}e_1^{(2)}e_2^{(3)} \\ & + 11e_2^{(1)}e_1^{(2)}e_2^{(3)} + 3e_1^{(1)}e_2^{(2)}e_2^{(3)} + 55e_2^{(1)}e_2^{(2)}e_2^{(3)}. \end{aligned}$$

Since $N(P_5) = a = 11$, we find $\mu_1'' = \mu_2'' = \mu_3'' = 1$; and hence

$$\begin{aligned} u_1 &= \pm 2(e_1^{(1)})^2 + 5(e_1^{(1)}e_2^{(1)}) + 11(e_2^{(1)})^2, \\ u_2 &= \pm (e_1^{(2)})^2 + 5(e_1^{(2)}e_2^{(2)}) + 22(e_2^{(2)})^2, \\ u_3 &= \pm (e_1^{(3)})^2 + 5(e_1^{(3)}e_2^{(3)}) + 22(e_2^{(3)})^2. \end{aligned}$$

For $e_1^{(1)}=2$, $e_2^{(1)}=1$, $e_1^{(2)}=-1$, $e_2^{(2)}=2$, $e_1^{(3)}=-2$, $e_2^{(3)}=-1$, we have $x=98$, $y=-181$, $u_1=\varepsilon_1 29$, $u_2=\varepsilon_2 79$, $u_3=\varepsilon_3 36$, $\varepsilon_1\varepsilon_2\varepsilon_3=+1$. For $e_1^{(1)}=1$, $e_2^{(1)}=1$, $e_1^{(2)}=-1$, $e_2^{(2)}=1$, $e_1^{(3)}=2$, $e_2^{(3)}=-1$, $x=24$, $y=-12$, $u_1=\varepsilon_1 18$, $u_2=\varepsilon_2 18$, $u_3=\varepsilon_3 16$, $\varepsilon_1\varepsilon_2\varepsilon_3=+1$.

For all $e_i^{(i)}=+1$, $x=-35$, $y=91$, $u_1-\varepsilon_1 18$, $u_2=\varepsilon_2 28$, $u_3=\varepsilon_3 28$, $\varepsilon_1\varepsilon_2\varepsilon_3=+1$.

In order to obtain a different class of solutions, it would be necessary to make another choice of γ so that it can be separated into factors representing different classes from C_1, C_0, C_0.

6. *The Case $k=4$.* When the diophantine equation to be solved is $Q(x, y)=u_1\cdot u_2$, the same method as that used above will give a solution which may be easily written down

$$\begin{aligned}\alpha' &= e_1^{(1)}\beta_1^{(2)}+e_2^{(2)}\beta_2^{(2)},\\ \alpha'' &= e_1^{(2)}\beta_1^{(2)}+e_2^{(2)}\beta_2^{(2)},\\ \alpha^{(4)} &= a_{14}a+a_{24}\varrho,\end{aligned}$$

where $(\beta_1^{(1)}, \beta_2^{(1)})$ and $(\beta_1^{(2)}, \beta_2^{(2)})$ are bases of the two ideals I_1 and I_2. Let $F_1(x, y)$ and $F_2(x, y)$ be the corresponding binary quadratic forms. Then the solutions are given by the following relations:

$$(16)\qquad \begin{cases} x = \dfrac{a_{14}A_{12}-a_{24}A_{22}c}{M},\\ y = \dfrac{A_{14}A_2^{(2)}+a_{24}A_1^{(2)}+a_{24}A_2^{(2)}b}{M},\\ u_1 = \varepsilon_1\mu_1'' F_1(e_1^{(1)}, e_2^{(1)}),\\ u_2 = \varepsilon_2\mu_2'' F_2(e_1^{(2)}, e_2^{(2)}),\end{cases}$$

where

$$(17)\qquad A_1^{(2)}=\sum_{i=0}^{2}C_1^{(i)}B_i,\qquad A_2^{(2)}=\sum_{i=0}^{2}C_2^{(i)}B_i,$$

$$(18)\qquad \begin{cases} C_1^{(0)}=1, & C_1^{(1)}=0, & C_1^{(2)}=-ac,\\ C_2^{(1)}=0, & C_2^{(1)}=1, & C_2^{(2)}=b,\end{cases}$$

$$(19)\quad B_0 = a_{11}a_{12},\quad B_1 = a_{11}a_{22}+a_{12}a_{21},\quad B_2 = a_{21}a_{22},$$

$$(20)\quad \begin{cases} a_{11} = b_{11}^{(1)}e_1^{(1)}+b_{21}^{(1)}e_2^{(1)}, \\ a_{21} = b_{12}^{(1)}e_1^{(1)}+b_{22}^{(2)}e_2^{(2)}, \\ a_{12} = b_{11}^{(2)}e_1^{(2)}+b_{21}^{(2)}e_2^{(2)}, \\ a_{22} = b_{12}^{(2)}e_1^{(2)}+b_{22}^{(2)}e_2^{(2)}, \end{cases}$$

where the $b_{ij}^{(k)}$ are constants depending on the ideals I_1 and I_2.

Let us now suppose that the ring R is the totality of all integers in $k(\sqrt{\mu})$. Then $(1, \varrho)$ is a fundamental system of the field; hence when $\mu \equiv 2$ or $3 \pmod 4$, $b = 0$ and when $\mu \equiv 1 \pmod 4$, $b = 1$. In either case $f = \{1\}$ and $\Delta = \pm 1$. No simplification would occur in the formulas (16) to (20) except that the b would be replaced by its value.

If, however, we make the additional restriction that $\mathfrak{M} = \mathfrak{G} = \{1\}$, we have $a = 1$, $P_k = \{1\}$; hence I_1 and I_2 belong to reciprocal classes, and in this case we may make $I_2 = I_1'$ and $F_1(x, y) = F_2(x, y)$. Moreover, since $P_k = \{1\}$ and $\mathfrak{M} = \{1\}$, we have $\mu_1'' = \mu_2'' = 1$, and the last two formulas of (16) become

$$u_1 = \varepsilon_1 F(e_1^{(1)}, e_2^{(1)}),\quad u_2 = \varepsilon_2 F(e_1^{(2)}, e_2^{(2)}),\qquad \varepsilon_1\varepsilon_2 = +1.$$

Since I_2 is the conjugate of I_1, we have $I_1I_2 = \{e\}$, where $N(I_1) = e$; hence $N(I) = e^2 = M$ and $\{M\}/I = I_4 = \{e\}$. Then $I_4P_4 = \{e\}\{1\} = \{e\}$. Hence $\gamma^{(k)} = e$ and $a_{14} = e_1$, $a_{24} = 0$. The first two of the formulas (16) now become

$$x = A_1^{(2)}/e = \frac{a_{11}a_{12} - a_{21}a_{22}c}{e},$$

$$y = A_2^{(2)}/e = \frac{a_{11}a_{22}+a_{21}a_{12}+a_{21}a_{22}b}{e}.$$

Since I_1 and I_2 are conjugate ideals and their norm is e, we can write the base of I_1 in the form $(e, f+\varrho)$ and that of I_2 in the form $(e, f+\varrho')$, where $f^2+bf+c \equiv 0 \pmod e$. Hence we have

$$b_{11}^{(1)} = e,\quad b_{21}^{(1)} = f,\quad b_{11}^{(2)} = e,\quad b_{12}^{(1)} = 0,\quad b_{22}^{(1)} = 1,\quad b_{12}^{(2)} = 0,$$

for all μ; and

$$b_{21}^{(2)} = f, \qquad b_{22}^{(2)} = -1,$$

when $\mu \equiv 2$ or 3 (mod 4); and

$$b_{21}^{(2)} = f+1, \quad b_{22}^{(2)} = -1,$$

when $\mu \equiv 1 \pmod 4$.

Using these values for the $b_{ij}^{(k)}$ and combining the relations (16) to (20), we have, when $\mu \equiv 2$ or 3 (mod 4),

$$(21) \qquad \begin{cases} x = ee_1^{(1)}e_1^{(2)} + f(e_1^{(1)}e_2^{(2)} + e_2^{(1)}e_1^{(2)}) + ge_2^{(1)}e_2^{(2)}, \\ y = e_1^{(2)}e_2^{(1)} - e_1^{(1)}e_2^{(2)}, \end{cases}$$

where $g = \dfrac{f^2+c}{e}$. When $\mu \equiv 1 \pmod 4$, we have

$$(22) \qquad \begin{cases} x = ee_1^{(1)}e_1^{(2)} + fe_2^{(1)}e_1^{(2)} + (f+1)e_1^{(1)}e_2^{(2)} + ge_2^{(1)}e_2^{(2)}, \\ y = e_1^{(2)}e_2^{(1)} - e_1^{(1)}e_2^{(2)}, \end{cases}$$

where $g = (f^2+f+c)/e$.

The binary quadratic form $F(x, y)$ may be chosen as the form corresponding to the base of I_1 as given above, and hence

$F(x, y) = ex^2 + 2fxy + gy^2$, when $\mu \equiv 2$ or 3 (mod 4);
$F(x, y) = ex^2 + (2f+1)xy + gy^2$, when $\mu \equiv 1 \pmod 4$.

The formulas (16) as thus reduced are those given by Dickson* if we put

$$e_1^{(1)} = e, \quad e_2^{(1)} = g, \quad e_1^{(2)} = u, \quad e_2^{(2)} = -2.$$

A shorter proof of these formulas was published later by Dickson†. The proof as here given is by reduction from the general case by the following specializations: (1) $k = 4$; (2) $R = \mathfrak{G}$, the ring of all integers in $k(\sqrt{\mu})$; and (3) $\mathfrak{M} = \mathfrak{G}$.

THE UNIVERSITY OF MISSOURI

* This BULLETIN, vol. 27, No. 8 (May, 1921), p. 353.
† This BULLETIN, vol. 29, No. 10 (Dec., 1923), p. 464.