THE STRUCTURE OF THE NUMBER OF REPRESENTATIONS FUNCTION IN A BINARY QUADRATIC FORM*

BY

GORDON PALL

This paper contains, primarily, the extension to any integral, binary quadratic form of the results of a recent article† concerning positive, binary, quadratic forms. With suitable conventions almost all the results carry over without change, though some of the proofs need slight alterations. Incidentally, there are treated automorphs of binary quadratic forms, and (rather fully) properties of sets of representations (representations equivalent through automorphic transformations) in a binary quadratic form.

1. Dirichlet‡ has already in all essentials extended the notion of number of representations to indefinite forms. We shall utilize the following equivalent definition.

Two representations (x,y) and (x',y') of m in the form $f=[a,b,c]$,§ that is, two integral solutions of

$$ax^2+bxy+cy^2=m, \tag{1}$$

will be called *equivalent* if they are transformable one into the other by integral automorphs of f. The class of all representations equivalent to a given one will be called a *set* of representations. The number of sets of representations of m in f will be denoted by $f(m)$. (In MZ, $f(m)$ denoted the number of representations of m in f.)

This definition becomes more interesting when we observe that, if $d(=b^2-4ac)>0$, the number of sets of representations of m in $[a,b,c]$ is equal to the actual number of solutions of (1) together with certain inequalities (cf. Theorem 9). The writer developed the theory of these inequalities before noticing that Dirichlet (§87, loc. cit.) obtains one such system. However, we shall obtain a substantial improvement on Dirichlet's inequalities and give a more complete discussion of the infinitely many alternative systems. The treatment in §3 is fairly comprehensive.

* Presented to the Society, October 29, 1932; received by the editors September 26, 1932.

† Mathematische Zeitschrift, vol. 36 (1933); this article will be referred to here as MZ.

‡ Cf. §§86 and 87 of *Vorlesungen über Zahlentheorie*, 4th edition, 1894.

§ We use Kronecker forms, for simplicity, throughout. Hence $[a,b,c]$ stands for $ax^2+bxy+cy^2$. For the automorphs see §2.

It will then be observed that, once the least positive solution t_1, u_1 of

$$t^2 - du^2 = 4 \tag{2}$$

is known, the labor of representing a number *by trial* in $ax^2+bxy+cy^2$ is, when $d>0$, on a par with the work when $d<0$. For example, for either of the equations

$$x^2 + 2y^2 = n, \quad x^2 - 2y^2 = n,$$

where n is a given positive integer, we need to try only the values y^2 such that $0 \leqq y^2 \leqq n/2$ to obtain a representation in every set. (For $x^2-2y^2=n$ the inequalities of Dirichlet require us to examine $0 \leqq y^2 < 4n$.)

To obtain this improvement it is necessary to introduce a convention whereby solutions on the boundaries of the inequalities count as $\frac{1}{2}$ instead of 1 (cf. Theorem 9). For example, if $d=8$, and $f=[1, 0, -2]$, then $f(n)$ is equal to the number $g(n)$ of integral solutions (x, y) of

$$n = x^2 - 2y^2,\ 0 \leqq y \leqq (n/2)^{1/2} (n > 0),\ (-n/2)^{1/2} \leqq y \leqq (-n)^{1/2} (n < 0), \tag{3}$$

except when $\pm n = k^2$ or $2k^2$ (k integral) in which cases $f(n) = g(n) - 1$. The condition of inequality may be replaced by $|x| \geqq 2y \geqq 0$, or $|y| \geqq x \geqq 0$.

If $d=b^2-4ac$ is negative or is a positive square, the number w of integral automorphs of f is 2, except that w is 4 if $d=-4$ and w is 6 if $d=-3$. Then the number of representations of n in f is $wf(n)$.

Unless otherwise specified each (binary) *form* in the sequel is a *primitive, integral, binary, quadratic form of discriminant d*, where *d is a non-zero integer* $\equiv 0$ *or* 1 (mod 4). For simplicity we do *not* make the usual convention that the forms are positive if $d<0$.

For any d there are a finite number h of (primitive) classes of forms, say $C_0, C_1, \cdots, C_{h-1}$. Representative forms from these classes are denoted, respectively, by $f_0, f_1, \cdots, f_{h-1}$. We shall always take C_0 to be the principal class, which represents $+1$. The system of representative forms will be designated by $S(=S_d)$. The sum of the numbers of sets of representations of n in the h forms will be denoted by $S(n)$, so that

$$S(n) = f_0(n) + f_1(n) + \cdots + f_{h-1}(n). \tag{4}$$

The system of classes C_i constitutes under composition a finite abelian group with C_0 as identity element. We shall assume their behavior in this respect as known, and shall interpret C_iC_j, etc., as the product classes under composition. Further if f is a form belonging to a class F, f^{-1} will denote the opposite form (belonging to the reciprocal class F^{-1}); and if g belongs to G, then f^rg^s will denote any form of the class F^rG^s.

An ambiguous class C is characterized by the equation $C^2=C_0$; or by $C=C^{-1}$; or by containing a form $[a, b, c]$ in which $a \mid b$.

We can now state our principal results.

The function $S(n)$ is a factorable function; for any relative-prime integers n_1 and n_2,

$$S(n_1n_2) = S(n_1)S(n_2). \tag{5}$$

An integer n is *semiprime to* d, by definition, if n is divisible by no prime p such that

$$p>2 \text{ and } p^2 \mid d, \text{ or } p=2 \text{ and } d\equiv 0 \text{ or } 4 \pmod{16}. \tag{6}$$

For any n semiprime to d, we shall prove

$$S(n) = \sum_{\nu \mid n}(d \mid \nu), \tag{7}$$

where ν ranges over the positive divisors of n, and $(d \mid \nu)$ is the Kronecker symbol.

For example in (3), the number $g(n)$ of integral solutions (x, y) is given by $g(n)=\sum(2 \mid \nu)$ unless $\pm n$ is a square or the double of a square, and then $g(n)=1+\sum(2 \mid \nu)$.

The system $\{f_0(n), \cdots, f_{h-1}(n)\}$ is *reducible* in the following sense: for every prime p not satisfying (6) and every integer $a>0$ there exists a matrix of h^2 numbers $\psi_{ij}(p, a)$ $(i, j=0, \cdots, h-1)$ such that, for every integer m prime to p,

$$f_i(p^am) = \sum_{j=0}^{h-1}\psi_{ij}(p, a)f_j(m). \tag{8}$$

More precisely the following formulas hold.

Let f be a form of discriminant d and F its class.

If $p \mid d$ but does not satisfy (6), p is represented by an ambiguous class C of discriminant d. If g belongs to C^aF,

$$f(p^an) = g(n) \text{ for every integer } n. \tag{9}$$

If $(d \mid p)=-1$ (Kronecker symbol),

$$f(pm) = 0, \quad f(p^2n) = f(n), \tag{10}$$

for every m prime to p and every integer n.

If $(d \mid p)=1$ there is a form g of discriminant d representing p. For every integer n,

$$f(pn) + f(n/p) = fg(n) + fg^{-1}(n). \tag{11}$$

Solving this relation as in MZ §6 we obtain

$$f(p^a m) = \sum_{\alpha=0}^{a} f g^{a-2\alpha}(m), \tag{12}$$

which holds for every integer $a \geqq 0$ and m prime to p.

Finally let p satisfy (6). Again $f(pm) = 0$ if p does not divide m. Now there exists a form g, of discriminant $d' = d/p^2$, which may be characterized as representing every number represented by f. For this form,

$$f(p^2 n) = \sigma g(n) \qquad \text{(every } n\text{)}, \tag{13}$$

where σ is partially defined by

$$\begin{cases} \sigma = 1 \text{ if } d' < -4 \text{ or } d' \text{ is a square}, \\ \sigma = 2 \text{ if } d' = -4, \\ \sigma = 3 \text{ if } d' = -3.* \end{cases} \tag{14}$$

If d' is positive but not square, employ the notation t_k, u_k for the successive solutions of

$$t^2 - d'u^2 = 4, \tag{15}$$

t_1, u_1 being the least positive solution (as in §3.4 with d' in place of d). Then σ is the (least) positive index such that

$$u_\sigma \equiv 0, \quad u_k \not\equiv 0 \quad (0 < k < \sigma) \qquad \pmod{p}. \tag{16}$$

To understand these formulas properly we should observe that

(17) If p is a prime, p and $-p$ are each represented in one of the classes of S unless (6) holds or $(d \mid p) = -1$;

(18) Either is represented in at most one class and the reciprocal class.

A class and its reciprocal, being improperly equivalent, represent the same numbers. If $d < 0$ the classes of S will occur in pairs, each class being accompanied by its negative.

The generality of our results as holding even for d square (but $\neq 0$) may be emphasized.

All the results of MZ, with the slight changes obvious from the preceding statements, hold for any integral binary quadratic form with discriminant $d \neq 0$. If $d < 0$ the form $-f_0$ of exponent 2 may be adjoined to the basis of MZ §1, if desired.

It is interesting to obtain a formula for the ψ_{ij} of (8). We can choose

* The reader will note that if $f(n)$ meant the actual number of representations instead of the number of sets we should have $f(p^2 n) = g(n)$ in all the cases in (14).

$\psi_{ik}=\psi_{ij}$ if f_j and f_k belong to reciprocal classes. Then $\psi_{ij}=\frac{1}{2}f_i(p^aq)$, where q is any prime represented in f_j (and f_k). We may choose q so that $q\neq p$ and $(d\,|\,q)=1$. Hence

$$\psi_{ij}(p,\,a)=\tfrac{1}{2}\{f_if_j(p^a)+f_jf_k(p^a)\}\quad(\text{where } f_jf_k=f_0). \tag{19}$$

Suppose $(d\,|\,p)=1$, $g(p)>0$. Then $2\psi_{ij}(p,\,a)$ is the number of the elements of the sequence $g^a, g^{a-2}, \cdots, g^{-a}$ belonging to the class of f_if_j or its reciprocal, plus the number in the class of f_if_k or its reciprocal.

2.1. **Automorphs.** We prove the following theorem.

THEOREM 1. *Let a, b, c be integers of g.c.d. unity, set $d=b^2-4ac$ and suppose $d\neq 0$. Then all integral automorphs (of determinant $+1$) of $[a, b, c]$ are given by*

$$\begin{aligned} x &= \tfrac{1}{2}(t-bu)x_0-cuy_0,\\ y &= aux_0+\tfrac{1}{2}(t+bu)y_0, \end{aligned} \tag{20}$$

as (t, u) ranges over all integral solutions of

$$t^2-du^2=4. \tag{21}$$

Let I denote the identity matrix. If T is a non-singular matrix, $T^{-1}IT=I$. Hence we have the following lemma:

LEMMA 1. *If a form has only the two automorphs with matrices $\pm I$, the same is true of all equivalent forms.*

First let d be a positive square. Set $d=\Delta^2$, $\Delta>0$. Then (21) has only the trivial solutions $(\pm 2, 0)$ (for which (20) has matrices $\pm I$). The theorem will therefore follow if it holds for a form equivalent to $f=[a, b, c]$. Now f is equivalent to one and only one of the $\phi(\Delta)$ forms

$$[k, \Delta, 0],\ 0\leqq k<\Delta,\ k \text{ prime to } \Delta, \tag{22}$$

and it is easy to show that these have only the two trivial automorphs.*

* For a primitive form $(\lambda x+\mu y)$ $(\nu x+\rho y)$ is equivalent to a form $x(\sigma x+\tau y)$, where, by the discriminant, $\tau=\pm\Delta$. Replacing y by $y+\kappa x$ we can alter σ by multiples of Δ. Evidently $[k, \Delta, 0]\sim'$ $[k, -\Delta, 0]$, where $\sim'$ means "is improperly equivalent to". Hence the fact that (22) constitutes a complete representative system of forms will follow once we prove that $[k, \Delta, 0]\sim'[l, \Delta, 0]$ when $kl\equiv 1 \pmod{\Delta}$, and that $[k, \Delta, 0]\sim[l, \Delta, 0]$ only when $k\equiv l \pmod{\Delta}$. To prove both these facts and to obtain all transformations carrying $[k, \Delta, 0]$ into $[l, \Delta, 0]$, compare coefficients in the identity

$$(\alpha x+\beta y)[k(\alpha x+\beta y)+\Delta(\gamma x+\delta y)]=x(lx+\Delta y),$$

where k and l are given prime to Δ, $0\leqq k<\Delta$, $0\leqq l<\Delta$. Then either $\beta=0$ or $k\beta+\Delta\delta=0$. The former case leads to $\alpha\delta=1$, $k\pm\Delta\gamma=l$, whence $k=l$ and $\gamma=0$ and the transformation matrix is $\pm I$. The latter case leads to

$$\alpha\delta-\beta\gamma=-\beta(\alpha k+\Delta\gamma)/\Delta=-1,\ \beta=\pm\Delta,\ \alpha=\pm l,\ \delta=\mp k,\ \gamma=\mp(kl-1)/\Delta.$$

This footnote and formula (22) will be useful to the reader who may wish to verify that properties which he knows to hold for d not square continue to hold when d is a square $\neq 0$.

Second we shall indicate a uniform proof, valid at least when d is not a square, by a modification of Dickson's *Introduction to the Theory of Numbers*, §§60 and 69: By taking $R^2=d$, $R>0$ if $d>0$, $-iR>0$ if $d<0$, we can define first and second roots in §60 for any form with $da\neq 0$. Then Theorems 72 and 73 hold unchanged together with their proofs, at least if d is not square. Also §69 holds for any non-square d.

2.2. **Proper sets of representations.** If (x, y) and (x_0, y_0) are related by (20) we say that (x, y) and (x_0, y_0) are equivalent representations in f. As already defined, all (x, y) equivalent to a given one comprise a *set*.

THEOREM 2. *The g.c.d. of x and y is the same for all (x, y) of a set.*

This is evident on solving (20) for x_0 and y_0. We may now speak of *proper sets*, that is, sets in which the g.c.d. is 1.

2.3. **Proper sets and the congruence $z^2\equiv d \pmod{4m}$.** Let Σ denote the aggregate of solutions z of

$$z^2 \equiv d \pmod{4m},\ 0 \leqq z < 2\,|\,m\,|\,, \tag{23}$$

such that

$$z,\ m, \text{ and } (z^2-d)/(4m) \text{ have g.c.d. } 1. \tag{24}$$

We shall set up a (1, 1) correspondence between the elements z of Σ and the various proper sets of representations of m by the h forms in S.

For any z write $z^2-d=4ml$. Then $\phi=[m, z, l]$ is a primitive form of discriminant d, and hence is equivalent to just one of the forms of S, say to $f=[a, b, c]$. For brevity we shall write

$$T=\begin{pmatrix} x & \xi \\ y & \eta \end{pmatrix},\quad A=\begin{pmatrix} \frac{1}{2}(t-bu) & -cu \\ au & \frac{1}{2}(t+bu) \end{pmatrix}. \tag{25}$$

If T is the matrix of one transformation of determinant $+1$ carrying f into ϕ, then the totality of such matrices is given by AT as t, u range through all integral solutions of (21). But then x and y are relative-prime and $m=ax^2+bxy+cy^2$, that is, (x, y) is a proper representation of m in f. And the class of first columns of the matrices AT is a set of representations of m in f.

Conversely, let (x, y) be a proper representation of m in f. We can choose integers η and ξ so that

$$x\eta - y\xi = 1, \tag{26}$$

and then the general form of such integers is $\xi+tx$, $\eta+ty$, where t is an integer. On applying the transformation with matrix T to f we derive $\phi=[m, n, l]$ where $m=ax^2+bxy+cy^2$ and

$$n = 2ax\xi + b(x\eta + y\xi) + 2cy\eta, \tag{27}$$

while l is determined by the discriminant. If we replace ξ and η in T by $\xi+tx$ and $\eta+ty$, m is unchanged but n is replaced by $n+2tm$. If we replace (x, y) by an equivalent representation, so that T is replaced by AT or a parallel matrix,* we again derive ϕ or a parallel form. Thus the (1, 1) correspondence is established.

THEOREM 3. *Let a, b, c have g.c.d. 1, let $d=b^2-4ac\neq 0$, and let m be an integer $\neq 0$. Let $f'(m)$ denote the number of proper sets of representations of m in $f=[a, b, c]$. Then $f'(m)$ is equal to the number of roots z of (23) such that $[m, z, (z^2-d)/(4m)]$ is equivalent to f.*

2.4. On $S'(n)$ and $S(n)$. Evidently $f(m)=\sum f'(m/q^2)$, where q^2 ranges over the square divisors of m. The number of proper sets of representations of m in S is

$$S'(m) = f_0'(m) + \cdots + f_{k-1}'(m), \tag{28}$$

and is equal to the number of solutions z of (23) and (24). Also,

$$S(m) = \sum S'(m/q^2). \tag{29}$$

Proceeding as in MZ but now allowing n to be negative as well as positive, we see that $S'(n)$ and $S(n)$ are factorable (MZ, §2).† Further we have

$$S'(1) = S'(-1) = S(1) = S(-1) = 1, \tag{30}$$

$$S'(n) = S'(-n), \quad S(n) = S(-n) \quad \text{(every } n\text{)}. \tag{31}$$

For any prime $p\geqq 2$ we have, using the Kronecker symbol $(d\,|\,p)$,

$$S'(p^a) = 1 + (d\,|\,p) \qquad \text{if } p \text{ does not divide } d, \tag{32}$$

$$\begin{aligned} S(p^a) &= a+1 && \text{if } (d\,|\,p)=1,\\ &= \tfrac{1}{2}\{1+(-1)^a\} && \text{if } (d\,|\,p)=-1,\\ &= 1 && \text{if } p\,|\,d \text{ but (6) does not hold.}\end{aligned} \tag{33}$$

If p does not satisfy (6) we have therefore

$$S(p^a) = 1 + (d\,|\,p) + \cdots + (d\,|\,p^a). \tag{34}$$

Hence, if n is semiprime to d,

$$S(n) = \sum (d\,|\,\nu) \tag{35}$$

summed for the positive divisors ν of n. In calculating $S(n)$ it is generally simpler to factor n into primary components, $n=\pm\Pi p^a$, and to employ (33).

* Two matrices like T are called parallel if their first columns are identical and their second columns differ by an integral multiple of their first columns.

† $S(n)$ and $S'(n)$ are used here instead of $r(n)$ and $r'(n)$ in MZ. The value of $S(p^a)$ for all cases may be read from the table of values of $r(p^a)$ in §3 of MZ.

2.5. **Representation of p or $-p$.** Let $m=\pm p$ where p is a prime. The number of roots of (23) and (24) is 0 if $(d|p)=-1$ or if (6) holds, 1 if $p|d$ but (6) does not hold, and 2 if $(d|p)=1$. In the second case the root of (23) is $z=0$ if d is even and p is odd, or if $d\equiv 8 \pmod{16}$ and $p=2$; the root is $z=p$ if d is odd, or if $d\equiv 12 \pmod{16}$ and $p=2$; whence the form

$$[\pm p, z, \cdots]$$

associated is ambiguous. In the third case the two roots are of the forms z, $2p-z$, where $0<z<p$, and the classes which represent p are represented by the two forms

$$[\pm p, z, \cdots], [\pm p, 2p-z, \cdots],$$

and are improperly equivalent. These facts prove (17), (18), and the following theorem.

THEOREM 4. *Let $m=\pm p$, p prime. Let f denote a primitive form representing m, and let F be the class of f. Then*

$$(36)\qquad \begin{aligned} f(m)&=2 \text{ if } p \text{ does not divide } d \text{ and } F \text{ is ambiguous};\\ &=1 \text{ if } p|d \text{ or if } p \text{ does not divide } d \text{ and } F \text{ is not ambiguous}. \end{aligned}$$

In case $p|d$, F is necessarily ambiguous.

2.6. **Representation of $\pm p_1p_2$, $(d|p_i)=1$.** As in MZ §4 we may prove the following result.

THEOREM 5. *Let p_1 and p_2 be distinct primes such that $(d|p_1)=(d|p_2)=1$. Let ϵ_1 and ϵ_2 be signs $+$ or $-$. Let g_i represent $\epsilon_i p_i$ $(i=1, 2)$. Let G_i be the class of g_i $(i=1, 2)$. Let f denote any form of the product class G_1G_2. Then f represents $m=\epsilon_1\epsilon_2 p_1p_2$, and*

(37) *$f(m)=4$, 2 or 1 according as G_1G_2 coincides with all, just one, or none of the classes $G_1G_2^{-1}$, $G_1^{-1}G_2$, $G_1^{-1}G_2^{-1}$.**

3. **Some properties of sets of representations.** By definition, (x, y) and (x_0, y_0) are equivalent representations in a form $[a, b, c]$, or belong to the same set of representations in $[a, b, c]$ if solutions of (2) exist satisfying (1). If there is no ambiguity as to the form involved we may write $(x, y)\sim(x_0, y_0)$.

3.1. **Transformation of sets.** We prove the following theorem.

THEOREM 6. *Let $f=[a, b, c]$ and $g=[a', b', c']$ be primitive integral forms of discriminants d and $d\epsilon^2$ respectively, $d\epsilon\neq 0$. If*

$$(38)\qquad x=\alpha x'+\beta y',\ y=\gamma x'+\delta y',\ \alpha, \beta, \gamma, \delta \text{ integers},$$

* I.e., according as all, just one of, or none of G_1, G_2, and G_1G_2 are ambiguous.

where $\alpha\delta-\beta\gamma=\epsilon$, *is a transformation of* f *into* g, *and if* (x', y') *and* (x_0', y_0') *are equivalent representations in* g, *then*

$$(39)\qquad (x, y) = (\alpha x' + \beta y', \gamma x' + \delta y'), (x_0, y_0) = (\alpha x_0' + \beta y_0', \gamma x_0' + \delta y_0')$$

are equivalent representations in f.

For we have

$$(40)\qquad \begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2, \quad b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned}$$

By assumption, integers t', u' exist satisfying

$$(41)\qquad t'^2 - d\epsilon^2u'^2 = 4$$

and such that

$$(42)\qquad \begin{aligned} x' &= \tfrac{1}{2}(t' - b'u')x_0' - c'u'y_0', \\ y' &= a'u'x_0' + \tfrac{1}{2}(t' + b'u')y_0'. \end{aligned}$$

Using (39) and (40) it is easy to verify that (20) holds with

$$(43)\qquad t = t', \ u = u'\epsilon.$$

3.2. **Opposite and ambiguous sets.** It is plain from (20) that either of the relations

$$(44)\qquad a \mid by, \ c \mid bx$$

holds for all or none of the elements (x, y) of a set. We call such a relation an invariant of the set. Another example was the g.c.d. of §2.2.

If $a \mid by$ then with each integral solution (x, y) of

$$(45)\qquad ax^2 + bxy + cy^2 = n$$

is associated a solution (x', y) where $x' = -by/a - x$. It is easy to verify that if (x, y) and (x_0, y_0) are related by (20), then

$$(46)\qquad x' = \tfrac{1}{2}(t + bu)x_0' + cuy_0, \ y = -aux_0' + \tfrac{1}{2}(t - bu)y_0,$$

where $x_0' = -by_0/a - x_0$. Hence (x', y) and (x_0', y_0) are in the same set of solutions in $[a, b, c]$. The set thus associated with a given one in which $a \mid by$ will be called the *x-opposite set.* A set in which $a \mid by$, and which coincides with its *x-opposite set,* will be called *x-ambiguous.* We shall see later that a set is x-ambiguous if and only if it contains an element (x, y) in which dy^2 has one of the values

$$(47)\qquad 0, \ -4an, \ (t_1 - 2)an, \ -(t_1 + 2)an.$$

Similarly, if $c \mid bx$ in a set, there is associated a *y-opposite* set of representations (x, y') in $[a, b, c]$, $y' = -bx/c - y$. A *y-ambiguous* set is one which coincides with its y-opposite set. Later we shall prove that a set is y-ambiguous if and only if it contains an element (x, y) in which dx^2 has the value

$$0, \ -4cn, \ (t_1 - 2)cn, \quad \text{or} \ -(t_1 + 2)cn. \tag{48}$$

Excluding from consideration the trivial set which consists of the single element (0, 0) we have the following theorem.

THEOREM 7. *Let a, b, c be relative-prime integers, $ac \neq 0$, and let both $a \mid by$ and $c \mid bx$ hold for the elements of a set. Then the two opposite sets coincide if and only if $ac \mid b$.*

For in order that they should coincide it is necessary and sufficient that for each (or some) element (x, y) of the set there shall exist integers t, u satisfying (21) and

$$\begin{aligned} -by/a - x &= \tfrac{1}{2}(t - bu)x - cu(-bx/c - y), \\ y &= aux + \tfrac{1}{2}(t + bu)(-bx/c - y). \end{aligned} \tag{49}$$

Multiply (49_1) by $\frac{1}{2}(t+bu)$, (49_2) by cu, and add, obtaining the first of the following equations, the second being a rearrangement of (49_2):

$$\begin{aligned} ax\{1 + \tfrac{1}{2}(t + bu)\} &= y\{acu - \tfrac{1}{2}b(t + bu)\}, \\ cy\{1 + \tfrac{1}{2}(t + bu)\} &= x\{acu - \tfrac{1}{2}b(t + bu)\}. \end{aligned} \tag{50}$$

Now if $ac \mid b$, the integers $t = (b^2 - 2ac)/(ac)$, $u = -b/(ac)$ satisfy (21) and (49). Hence it remains only to show that (50) implies that $ac \mid b$.

If, in (50), $t + bu = -2$, we have

$$y(acu + b) = 0 = x(acu + b),$$

whence $u = -b/(ac)$ is an integer. Suppose $t + bu \neq -2$. Then (50) implies

$$ax^2 = cy^2. \tag{51}$$

If now ac does not divide b, (51) will have to be satisfied by every element (x, y) of the set, which is impossible unless the number of elements in the set is 2 (or the set contains both (x, y) and $(x, -y)$, whence $b = 0$). Finally let the set consist of two elements (x, y) and $(-x, -y)$. If the two opposite sets coincide, either $-x - by/a = x$ and $y = -y - bx/c$, or $-x - by/a = -x$ and $y = y + bx/c$; the first case is impossible and the second implies $b = 0$.

If $a \mid by$ in a set, it is x-ambiguous if and only if for each (or for some) (x, y) of the set there exists a solution (t, u) of (21) such that

$$\begin{aligned} 2ax + by &= \tfrac{1}{2}t(-2ax - by) + \tfrac{1}{2}duy, \\ y &= \tfrac{1}{2}u(-2ax - by) + \tfrac{1}{2}ty. \end{aligned} \tag{52}$$

These may be combined into the single equation (cf. (21))

$$\frac{2ax+by}{y}=\frac{t-2}{u}\left(=\frac{du}{t+2}\right), \tag{53}$$

where $u=0$, $t=2$ is equivalent to $2ax+by=0$, and $u=0$, $t=-2$ is interpreted as $y=0$.

Similarly a set is y-ambiguous if and only if $c \mid bx$ and for each (or some) (x, y) of the set there exists a solution (t, u) of (21) and

$$\frac{2cy+bx}{x}=\frac{t-2}{-u}\left(=\frac{-du}{t+2}\right). \tag{54}$$

Here $(t, u)=(\pm 2, 0)$ corresponds to $2cy+bx=0$ or $x=0$.

3.3. **A congruencial property of sets mod p.** Let a, b, c be relative prime integers, $d=b^2-4ac\neq 0$. Let p be any prime not dividing ad and such that $(d \mid p)=1$ (Kronecker symbol). Then there are just two distinct roots m_1, m_2 of

$$am^2+bm+c\equiv 0 \pmod{p},\quad 0\leqq m<p. \tag{55}$$

For any integer n, each integral solution (x, y) of

$$ax^2+bxy+cy^2=pn \tag{56}$$

satisfies one and only one of the three conditions

$$\begin{aligned} &x\equiv m_1y,\ y\not\equiv 0;\quad x\equiv m_2y,\ y\not\equiv 0;\\ &x\equiv y\equiv 0 \end{aligned} \pmod{p}. \tag{57}$$

It is easy to verify that each of the conditions (57_1), (57_2), (57_3) is an invariant property of any set of solutions (x, y) of (56).

As regards (57_3) this fact is evident from Theorem 2. Assume in (20) that $x_0\equiv m_iy_0 \pmod{p}$. We readily deduce $x\equiv m_iy \pmod{p}$.

3.4. **Concerning the equation $t^2-du^2=4$.** For the remainder of §3 we shall assume that *d is positive but not square.* Accordingly $d\geqq 5$.

All solutions (t, u) of (21) in integers are (t_k, u_k) and $(-t_k, -u_k)$, where $t_0=2$ and $u_0=0$, (t_1, u_1) is the "least positive" solution of (21), while the remaining solutions are linked together by the equations

$$\begin{aligned} 2t_{k+l}&=t_lt_k+du_lu_k,\\ 2u_{k+l}&=u_lt_k+t_lu_k, \end{aligned} \tag{58}$$

valid for all integers k and l.

Hence it is readily proved that

$$
\begin{gathered}
t_{-k} = t_k,\ u_{-k} = -u_k, \\
2 < t_1 < t_2 < \cdots,\ 0 < u_1 < u_2 < \cdots, \\
\frac{t_k}{u_k} > \frac{t_k + t_{k+1}}{u_k + u_{k+1}} > \frac{t_{k+1}}{u_{k+1}},\ \frac{t_k}{u_k} \to d^{1/2} \quad (k = 0, 1, 2, \cdots).
\end{gathered} \tag{59}
$$

Here and later t_0/u_0 is interpreted as $+\infty$.

It will be useful to note the relations

$$
\frac{t_h + t_i}{u_h + u_i} = \frac{t_{h+j} + t_{i-j}}{u_{h+j} + u_{i-j}},\ \frac{t_h - t_i}{u_h - u_i} = \frac{t_{h+j} - t_{i-j}}{u_{h+j} - u_{i-j}} \tag{60}
$$

which hold for all integers h, i, j such that the denominators are different from zero. To prove these formulas, cross-multiply and use (58_2) and (59_1). The second result is related to the first since

$$
\frac{t_h + t_i}{u_h + u_i} \cdot \frac{t_h - t_i}{u_h - u_i} = d. \tag{61}
$$

Since $t_0 = 2$ and $u_0 = 0$, we have, with obvious conventions for the cases where the denominators vanish,

$$
\begin{gathered}
\frac{t_{2k} + 2}{u_{2k}} = \frac{t_k}{u_k},\quad \frac{t_{2k+1} + 2}{u_{2k+1}} = \frac{t_{k+1} + t_k}{u_{k+1} + u_k}, \\
\frac{t_{2k} - 2}{u_{2k}} = \frac{du_k}{t_k},\quad \frac{t_{2k+1} - 2}{u_{2k+1}} = \frac{d(u_{k+1} + u_k)}{t_{k+1} + t_k}.
\end{gathered} \tag{62}
$$

3.5. **Distribution of the solutions in a set relative to t_k, u_k.** Let (x_0, y_0) denote any given solution in a set of solutions of (45). Rearranging (20) slightly we see that the aggregate of solutions (x, y) of the set are given by (x_k, y_k) and $(-x_k, -y_k)$ $(k = 0, \pm 1, \pm 2, \cdots)$, where

$$
\begin{aligned}
2ax_k + by_k &= \tfrac{1}{2}(2ax_0 + by_0)t_k + \tfrac{1}{2}dy_0u_k, \\
y_k &= \tfrac{1}{2}(2ax_0 + by_0)u_k + \tfrac{1}{2}y_0t_k.
\end{aligned} \tag{63}
$$

A pair of equations equivalent to (63) is

$$
\begin{aligned}
2cy_k + bx_k &= \tfrac{1}{2}(2cy_0 + bx_0)t_{-k} + \tfrac{1}{2}dx_0u_{-k}, \\
x_k &= \tfrac{1}{2}(2cy_0 + bx_0)u_{-k} + \tfrac{1}{2}x_0t_{-k}.
\end{aligned} \tag{64}
$$

It is convenient to write

$$
X_k = 2ax_k + by_k,\ Y_k = 2cy_k + bx_k. \tag{65}
$$

Hence we have

$$(66)\qquad \begin{aligned} 2y_{-1} &= y_0t_1 - X_0u_1, \quad 2X_{-1} = X_0t_1 - dy_0u_1,\\ 2x_{-1} &= x_0t_1 + Y_0u_1, \quad 2Y_{-1} = Y_0t_1 + dx_0u_1. \end{aligned}$$

Substituting for t_k and u_k from $t_{k+1}=\frac{1}{2}t_1t_k+\frac{1}{2}du_1u_k$ and $u_{k+1}=\frac{1}{2}u_1t_k+\frac{1}{2}t_1u_k$, and employing (66) we obtain the following four systems each equivalent to (63) or (64):

$$(67)\qquad u_1X_k = -y_{-1}t_k + y_0t_{k+1}, \qquad u_1y_k = -y_{-1}u_k + y_0u_{k+1};$$

$$(68)\qquad u_1X_k = -X_{-1}u_k + X_0u_{k+1}, \quad du_1y_k = -X_{-1}t_k + X_0t_{k+1};$$

$$(69)\qquad u_1Y_k = x_{-1}t_k - x_0t_{k+1}, \qquad u_1x_k = -x_{-1}u_k + x_0u_{k+1};$$

$$(70)\qquad u_1Y_k = -Y_{-1}u_k + Y_0u_{k+1}, \quad du_1x_k = Y_{-1}t_k - Y_0t_{k+1}.$$

Since $X_k^2-dy_k^2=4an$, we have $|X_k|>R|y_k|$ if $an>0$, and $R|y_k|>|X_k|$ if $an<0$, where $R=d^{1/2}$. Since also $t_k>Ru_k$ it is evident from (63) that X_k has the same sign as X_0 if $an>0$, and that y_k has the same sign as y_0 if $an<0$. Similarly from (64), Y_k has the same sign as Y_0 if $cn>0$, and x_k has the same sign as x_0 if $cn<0$.

From (67)-(70) with $k=0$ or -1 we have, on performing certain subtractions,

$$\begin{aligned} du_1(y_0 - y_{-1}) &= (t_1 - 2)(X_{-1} + X_0),\\ u_1(X_0 - X_{-1}) &= (t_1 - 2)(y_{-1} + y_0),\\ -u_1(Y_0 - Y_{-1}) &= (t_1 - 2)(x_{-1} + x_0),\\ -du_1(x_0 - x_{-1}) &= (t_1 - 2)(Y_{-1} + Y_0). \end{aligned}$$

But (x_0, y_0) may be any element of the set. Hence, incorporating the preceding result, we have the following:

$$(71)\qquad \begin{aligned} &\text{if } an>0, \text{ every } X_k \text{ and } y_k-y_{k-1} \text{ has the same sign;}\\ &\text{if } an<0, \text{ every } y_k \text{ and } X_k-X_{k-1} \text{ has the same sign;}\\ &\text{if } cn>0, \text{ every } Y_k \text{ and } x_{k-1}-x_k \text{ has the same sign;}\\ &\text{if } cn<0, \text{ every } x_k \text{ and } Y_{k-1}-Y_k \text{ has the same sign.}* \end{aligned}$$

Hence we can choose an element (x_0, y_0) of the set such that (for every integer k)

(72) $X_k>0$ and $y_{-1}<0 \leqq y_0$ if $an>0$; $y_k>0$ and $X_{-1}<0 \leqq X_0$ if $an<0$;

or such that

(73) $Y_k<0$ and $x_{-1}<0 \leqq x_0$ if $cn>0$; $x_k<0$ and $Y_{-1}<0 \leqq Y_0$ if $cn<0$.

* It is easy to deduce from (71), if $a>0$, $b\geqq 0$, $c<0$, that
if $n>0$, every X_k, x_k, y_k-y_{k-1}, $Y_{k-1}-Y_k$ has the same sign as x_0;
if $n<0$, every Y_k, y_k, $x_{k-1}-x_k$, X_k-X_{k-1} has the same sign as y_0.

For this choice of (x_0, y_0) in case (72) we write

$$\lambda = -y_0/y_{-1} \text{ if } an > 0, \quad \lambda = -X_0/X_{-1} \text{ if } an < 0; \tag{74}$$

and in case (73) we write

$$\lambda = -x_0/x_{-1} \text{ if } cn > 0, \quad \lambda = -Y_0/Y_{-1} \text{ if } cn < 0. \tag{75}$$

Thus $\lambda \geqq 0$.

In these respective four cases, we have by (59_1) and (67)-(70) the following results:

$$\begin{aligned} \frac{X_k}{y_k} &= \frac{t_k + \lambda t_{k+1}}{u_k + \lambda u_{k+1}}, & \frac{X_{-1-k}}{-y_{-1-k}} &= \frac{t_{k+1} + \lambda t_k}{u_{k+1} + \lambda u_k}; \\ \frac{X_k}{y_k} &= \frac{d(u_k + \lambda u_{k+1})}{t_k + \lambda t_{k+1}}, & \frac{-X_{-1-k}}{y_{-1-k}} &= \frac{d(u_{k+1} + \lambda u_k)}{t_{k+1} + \lambda t_k}; \end{aligned} \tag{76}$$

$$\begin{aligned} \frac{-Y_k}{x_k} &= \frac{t_k + \lambda t_{k+1}}{u_k + \lambda u_{k+1}}, & \frac{-Y_{-1-k}}{-x_{-1-k}} &= \frac{t_{k+1} + \lambda t_k}{u_{k+1} + \lambda u_k}; \\ \frac{Y_k}{-x_k} &= \frac{d(u_k + \lambda u_{k+1})}{t_k + \lambda t_{k+1}}, & \frac{-Y_{-1-k}}{-x_{-1-k}} &= \frac{d(u_{k+1} + \lambda u_k)}{t_{k+1} + \lambda t_k} \end{aligned} \tag{77}$$

$$(k = 0, 1, 2, 3, \cdots).$$

It is evident from (53), (54), and (62) that an x- or y-ambiguous set is characterized by having $\lambda = 0$ or 1 in (76) or (77) respectively. Write $\epsilon = 1$ or -1 according as $an > 0$ or $an < 0$. Then as (x, y) runs through one half the elements of an x-ambiguous set (the other half consisting of the values $(-x, -y)$) the ratio $(2ax+by)/y$ assumes precisely once each of the values

$$\frac{t_{2h+\lambda} + 2\epsilon}{u_{2h+\lambda}} \qquad (h = 0, \pm 1, \pm 2, \cdots), \tag{78}$$

λ having a fixed value 0 or 1 for the set. (Corresponding to $\lambda = h = 0$ this relation is to be interpreted as $2ax+by=0$ if $\epsilon = -1$ and as $y=0$ if $\epsilon = 1$.) For a y-ambiguous set we interchange a and c, x and y in the preceding. In view of $(2ax+by)^2 - dy^2 = 4an$ we have (47), and similarly (48).

It follows that for an x-ambiguous set one of $4an$, $-4and$, $(t_1+2)an$, or $-(t_1-2)an$ is a square; and similarly for a y-ambiguous set with a replaced by c.

A glance at (76) (where now $0 < \lambda < 1$ or $\lambda > 1$) demonstrates the following theorem.*

* A unification of two types of interval is obtained by means of (62).

THEOREM 8. *Let the discriminant d of the primitive integral form $[a, b, c]$ be positive but not square. If a set of solutions of* (45) *is not x-ambiguous, it contains precisely one pair (x, y) and $(-x, -y)$ satisfying*

$$y \neq 0 \text{ and } \left|\frac{2ax+by}{y}\right| > \frac{t_1+2}{u_1} \text{ if } an > 0, \tag{79}$$

$$0 < \left|\frac{2ax+by}{y}\right| < \frac{t_1-2}{u_1} \text{ if } an < 0. \tag{80}$$

More generally, let k denote any integer $\geqq 0$. In any set which is not x-ambiguous occurs just one (x, y) and $(-x, -y)$ satisfying

$$\frac{t_k+2}{u_k} > \left|\frac{2ax+by}{y}\right| > \frac{t_{k+1}+2}{u_{k+1}} \text{ if } an > 0, \tag{81}$$

$$\frac{t_k-2}{u_k} < \left|\frac{2ax+by}{y}\right| < \frac{t_{k+1}-2}{u_{k+1}} \text{ if } an < 0. \tag{82}$$

We may designate as Theorem 8′ the analogous result for non-y-ambiguous sets, obtained by interchanging x and y, a and c throughout Theorem 8.

Every solution is contained within one of these intervals.

By (21) and (45) the preceding systems of inequalities may be replaced by the following, k denoting any integer $\geqq 0$:

$$\begin{aligned} an(t_k-2) < dy^2 < an(t_{k+1}-2) &\text{ if } an > 0, \\ -an(t_k+2) < dy^2 < -an(t_{k+1}+2) &\text{ if } an < 0, \end{aligned} \tag{83}$$

if the set is not x-ambiguous. In every such set there is precisely one (x, y) and $(-x, -y)$ within each of the intervals (83) for $k=0, 1, 2, \cdots$; for a non-y-ambiguous set the corresponding intervals are

$$\begin{aligned} cn(t_k-2) < dx^2 < cn(t_{k+1}-2) &\text{ if } cn > 0, \\ -cn(t_k+2) < dx^2 < -cn(t_{k+1}+2) &\text{ if } cn < 0. \end{aligned} \tag{83′}$$

It may be noted that, if $b=0$, then y satisfies (83) if and only if x satisfies (83′) for the same k.

THEOREM 9. *Let the discriminant d of the primitive integral form $[a, b, c]$ be positive but not square. Let (t_1, u_1) be the least positive solution of $t^2-du^2=4$. Then the number of sets of solutions of $ax^2+bxy+cy^2=n$ is equal to the number of solutions (x, y) of this equation satisfying*

$$2|an| - 2an \leqq dy^2 \leqq t_1|an| - 2an, \; y \geqq 0, \tag{84}$$

with the convention that solutions with y at an end point of this interval are counted as $\frac{1}{2}$.

In place of (84) we may use

$$2\,|\,cn\,| - 2cn \leqq dx^2 \leqq t_1\,|\,cn\,| - 2cn,\ x \geqq 0; \tag{84'}$$

or indeed any of the infinitely many intervals (79)-(83'), with $\leqq$ in place of $<$, and with the same convention for end points.

4.1. **Reduction formulas for primes p not dividing d.** If $(d\,|\,p) = -1$, (56) requires $x \equiv y \equiv 0 \pmod{p}$, so that (10) is obvious.

Hence let $(d\,|\,p) = 1$ and employ the notations and hypotheses of §3.3. Then (56) requires

$$x = m_i y + pX, \tag{85}$$

X integral ($i = 1$ or 2). The equation (85) defines a (1, 1) correspondence between the integral solutions (x, y) of (56) satisfying $x \equiv m_i y \pmod{p}$ and the integral solutions (X, y) of

$$n = apX^2 + (2am_i + b)Xy + p^{-1}(am_i^2 + bm_i + c)y^2. \tag{86}$$

Here $g_i = [ap, 2am_i + b, \cdots]$ is a primitive integral form of discriminant d. The solutions (X, y) of (86) in which $p\,|\,y$ correspond to solutions (X, Y) of

$$n/p = aX^2 + (2am_i + b)XY + (am_i^2 + bm_i + c)Y^2, \tag{87}$$

under the transformation $y = pY$. The form in (87) is equivalent to $f = [a, b, c]$. Hence to conclude for every integer n that

$$f(pn) = f(n/p) + \{g_1(n) - f(n/p)\} + \{g_2(n) - f(n/p)\},$$

that is,

$$f(pn) + f(n/p) = g_1(n) + g_2(n), \tag{88}$$

we have to prove that if (x, y) and (x_0, y_0) are equivalent solutions of (56), then (X, y) and (X_0, y_0), where

$$x = m_i y + pX, \quad x_0 = m_i y_0 + pX_0, \tag{89}$$

are equivalent solutions of (86), and conversely. The converse holds by Theorem 6. Assume that (20) holds. Then by (89),

$$X = p^{-1}(x - m_i y) = \tfrac{1}{2}[t - (2am_i + b)u]X_0 - p^{-1}(am_i^2 + bm_i + c)uy_0,$$
$$y = apuX_0 + \tfrac{1}{2}y_0[t + (2am_i + b)u], \text{ as required.}$$

The remaining developments of §6, MZ, may now be carried through, if we use Theorems 4 and 5.

4.2. **Reduction formulas for primes dividing d.** First, let $p > 2$, $d = b^2 - 4ac$, $p\,|\,d$, where a, b, c are relative-prime integers. Then p does not divide a or c, say p does not divide a. We can choose integers A and Q such that

$$2Aa + Qp = 1. \tag{90}$$

Then the equation

$$ax^2 + bxy + cy^2 = pn, \tag{91}$$

being equivalent to $(2ax+by)^2 - dy^2 = 4apn$, implies

$$x = -Aby + pX, \quad X \text{ integral}. \tag{92}$$

Second, let $p=2$, $4 \mid d$. Then a or c is odd, say a. Then (91) implies $x \equiv cy \pmod 2$, so that in place of (92) we have

$$x = 2X \text{ if } c \text{ is even}, \quad x = 2X + y \text{ if } c \text{ is odd}. \tag{93}$$

Thus (92) or (93) sets up a (1, 1) correspondence between the integral solutions (x, y) of (91) and the integral solutions (X, y) of

$$apX^2 + b'Xy + c'y^2 = n, \tag{94}$$

where, in the respective cases (92), (93_1), and (93_2),

$$\begin{aligned} &b' = bQp, && c' = (aA^2b^2 - Ab^2 + c)/p && (p > 2);\\ &b' = b, && c' = \tfrac{1}{2}c && (p = 2, c \text{ even});\\ &b' = 2a + b, && c' = \tfrac{1}{2}(a + b + c) && (p = 2, c \text{ odd}). \end{aligned} \tag{95}$$

It is plain that c' is an integer in all cases, and that the form

$$g = [ap, b', c'] \tag{96}$$

is of discriminant d. Hence, in case (95_1), $p \mid c'$ if and only if $p^2 \mid d$, so that g is primitive if and only if p^2 does not divide d. In either of cases (95_2) or (95_3), the divisor of g is seen to be 1 if $d \equiv 8$ or 12, but 2 if $d \equiv 0$ or 4 (mod 16).

In the respective three cases, write

$$\begin{aligned} &X = (x + Aby)/p, && X_0 = (x_0 + Aby_0)/p; && X = \tfrac{1}{2}x, && X_0 = \tfrac{1}{2}x_0;\\ &X = (x - y)/2, && X_0 = (x_0 - y_0)/2. \end{aligned} \tag{97}$$

We find, by (90) and the values of b' and c', that the relations (20) are equivalent to

$$\begin{aligned} X &= \tfrac{1}{2}(t - b'u)X_0 - c'uy_0,\\ y &= apuX_0 + \tfrac{1}{2}(t + b'u)y_0. \end{aligned} \tag{98}$$

Thus, *if g is primitive*, that is, if (6) does not hold, the (1, 1) correspondence between representations set up by (92) or (93) carries over to sets of representations. Hence, if $f = [a, b, c]$,

$$f(pn) = g(n). \tag{99}$$

4.3. Finally let (6) hold. Now (92) or (93) still sets up a (1, 1) correspondence between the solutions (x, y) of (91) and the solutions (X, y) of

$$aX^2 + (b'/p)Xy + (c'/p)y^2 = n/p. \tag{100}$$

But now, while $(x, y)\sim(x_0, y_0)$ implies $(X, y)\sim(X_0, y_0)$, the converse is no longer true. The former fact is evident from (98) on replacing ap by a, b' by b'/p, u by pu, c' by c'/p, and on noticing that $t^2-(d/p^2)(pu)^2=4$.

In the cases where $T=\pm 2$, $U=0$ are the only solutions of

$$T^2 - (d/p^2)U^2 = 4, \tag{101}$$

we evidently have conversely that

$$(X, y) \sim (X_0, y_0) \text{ implies } (x, y) \sim (x_0, y_0), \tag{102}$$

the first equivalence relating to (100), the second to (91). If $d=-3p^2$ or $-4p^2$, the values of σ in (14) are evident from the relative numbers of solutions of (20) and (101) (which are the numbers of solutions in a set).

There remains only the case where d is positive but not square. Then $(X, y)\sim(X_0, y_0)$ may be written as

$$\begin{aligned} 2aX + (b'/p)y &= \tfrac{1}{2}T(2aX_0 + (b'/p)y_0) + \tfrac{1}{2}(d/p^2)Uy_0, \\ y &= \tfrac{1}{2}U(2aX_0 + (b'/p)y_0) + \tfrac{1}{2}Ty_0, \end{aligned} \tag{103}$$

where (T, U) denotes some solution of (101).

Our remaining problem may now be stated precisely. We are given a pair of integers x_0, y_0 such that X_0, as defined in (97), is an integer. Let K denote the aggregate of all (integer) pairs x, y defined by (103), and (97), as T, U range over all the solutions of (101). Each such pair x, y is a solution of (91). Evidently K is the sum of a certain number of sets of such solutions. The problem is to determine that number.

Let then x', y' be another pair, defined by

$$\begin{aligned} 2aX' + (b'/p)y' &= \tfrac{1}{2}T'(2aX_0 + (b'/p)y_0) + \tfrac{1}{2}(d/p^2)U'y_0, \\ y' &= \tfrac{1}{2}U'(2aX_0 + (b'/p)y_0) + \tfrac{1}{2}T'y_0, \end{aligned} \tag{104}$$

and by

$$X' = (x' + Aby')/p,\ X' = \tfrac{1}{2}x',\ X' = (x' - y')/2, \tag{105}$$

respectively; T', U' being another solution of (101). Changing (x, y) to $(-x, -y)$ or (x', y') to $(-x', -y')$ if necessary, we may suppose $(T, U) = (T_k, U_k)$ and $(T', U') = (T_l, U_l)$, where T_k, U_k play the same role for (101) as t_k, u_k for $t^2-du^2=4$.

Let σ denote the least positive index such that $U_\sigma \equiv 0 \pmod{p}$. Hence $u_n = U_{n\sigma}/p$ and $t_n = T_{n\sigma}$ $(n=0, \pm 1, \pm 2, \cdots)$.

On solving for $2aX_0+(b'/p)y_0$ and y_0 from (104) and substituting in (103), and using relations for T_k, U_k analogous to (58) and (59_1), we obtain

$$(106)\qquad \begin{aligned} 2aX + (b'/p)y &= \tfrac{1}{2}T_{k-l}(2aX' + (b'/p)y') + \tfrac{1}{2}(d/p^2)U_{k-l}y', \\ y &= \tfrac{1}{2}U_{k-l}(2aX' + (b'/p)y') + \tfrac{1}{2}T_{k-l}y'. \end{aligned}$$

Now, in all three cases $p[2aX+(b'/p)y]=2ax+by$. Hence (106) may be written

$$(107)\qquad \begin{aligned} 2ax + by &= \tfrac{1}{2}T_{k-l}(2ax' + by') + \tfrac{1}{2}d(U_{k-l}/p)y', \\ y &= \tfrac{1}{2}(U_{k-l}/p)(2ax' + by') + \tfrac{1}{2}T_{k-l}y'. \end{aligned}$$

Now since $(2ax'+by')^2-dy'^2\neq 0$, these equations cannot hold with T_{k-l} and U_{k-l}/p replaced by any other numbers. Hence we see that (x, y) and (x', y') defined by (103) and (104) with $(T, U)=(T_k, U_k)$ and $(T', U')=(T_l, U_l)$ are equivalent if and only if $k\equiv l \pmod{\sigma}$. This proves (13) with σ as in (16).

McGill University,
Montreal, Canada