ACTA ARITHMETICA
XIV (1968)

Sums of two squares in a quadratic ring

by

J. HARDY (Athens, Georgia)

1. At the present there is no practicable method of reducing binary quadratic forms with coefficients in a quadratic ring R of discriminant Δ, by which one could, for example, tell whether or not such a simple form as x^2+y^2 is in a genus of one class. G. Pall has shown in [2] how to transform the problem of expressing $\gamma = \alpha^2+\beta^2$ (α, β, γ in R) to one of representing the norm $N(\gamma)$ by the principal form of determinant Δ, in ordinary integers subject to certain conditions; and has illustrated his method for $\Delta = -4, 5, 8$. It is the purpose of this paper to determine the limitations of Pall's method, and to treat further cases. The formulas themselves are of interest. If $\Delta < 0$ (but not in the exceptional case where $-\Delta$ is a square) the number of representations, if not zero, is infinite. However, the number of sets of representations (with set defined in a natural way) is finite.

It will be helpful to review Pall's method. Small Latin letters will denote ordinary integers (in Z); we may set $\Delta = -4k+j$, $j = 0$ or 1, Δ nonsquare, $\varrho = \frac{1}{2}(-j+\sqrt{\Delta})$ and $R = \{x_0+x_1\varrho \mid x_0, x_1 \text{ in } Z\}$.

The equation

$$c_0+c_1\varrho = (a_0+a_1\varrho)^2+(b_0+b_1\varrho)^2 \tag{1}$$

is equivalent to the two equations

$$c_0 = a_0^2+b_0^2-k(a_1^2+b_1^2), \tag{2}$$

$$c_1 = 2(a_0a_1+b_0b_1)-j(a_1^2+b_1^2). \tag{3}$$

If we set $l = a_1^2+b_1^2$, the problem of counting the number of solutions of (1) is reduced to the problem of choosing non-negative integers l such that the form

$$\Phi = (c_0+kl)x^2+(c_1+jl)xy+ly^2 \tag{4}$$

is a sum of two squares of linear forms

$$(a_0x+a_1y)^2+(b_0x+b_1y)^2$$

with integral coefficients and summing the numbers $r_2(\Phi)$ of such representations. Here $r_2(\Phi)$ denotes the number of representations of Φ as the sum of squares of two linear forms with integral coefficients. Also in [2] Pall showed that $r_2(\Phi) = 0$ unless $\Phi = d_1\Phi_1$, where Φ_1 is primitive, positive definite or semidefinite, and of square determinant m^2, and d_1 is a positive integer such that no prime of the form $4n+3$ divides d_1 to an odd exponent; and that if $m^2 \neq 0$, the number of representations of Φ is $2r_2(d_1)$; if $m^2 = 0$, the number is $r_2(d_1)$.

Thus, l must be chosen so that (c_0, c_1, l) has no prime factor $4n+3$ to an odd exponent, and so that

$$(c_0+kl)l-\tfrac{1}{4}(c_1+jl)^2$$

is a square u^2. The last condition can be expressed as follows: if $j = 0$,

$$c_0^2+4kc_1'^2 = v^2+\Delta u^2, \tag{5}$$

where $v = 2kl+c_0$, $c_1 = 2c_1'$; if $j = 1$,

$$c_0^2-c_0c_1+kc_1^2 = v^2+\Delta u^2, \tag{6}$$

where $v = \frac{1}{2}(\Delta l+c_1)-c_0$. Since $N(c_0+c_1\varrho) = c_0^2-jc_0c_1+kc_1^2$, we notice that the left sides of both (5) and (6) are just $N(c_0+c_1\varrho)$.

An examination of Pall's method shows that it succeeds only if the form $v^2+\Delta u^2$ is in a genus of one class. It is necessary that v, u satisfy the condition that l be a non-negative integer, where

$$l = \begin{cases} (v-c_0)/2k & \text{if} \quad j = 0, \\ [2v+(2c_0-c_1)]/\Delta & \text{if} \quad j = 1. \end{cases} \tag{7}$$

In the following discussion of Pall's algorithm, we must consider separately the cases $\Delta > 0$ and $\Delta < 0$.

First assume $\Delta > 0$. In the case $\Delta = -4k$ we have $k < 0$ and $c_0 > 0$. Here $l = (v-c_0)/2k = (c_0-v)/|2k|$. Since $c_0^2 = |4k|c_1'^2+v^2+\Delta u^2 \geqslant v^2$, $c_0 \geqslant |v|$ and $l \geqslant 0$. Thus, if $c_0 \equiv \pm v \pmod{2k}$, then l is a non-negative integer for either sign of v. In the case $\Delta = -4k+1$ we have $k \leqslant 0$ and $2c_0-c_1 \geqslant 0$, $l = [2v-(2c_0-c_1)]/\Delta$. Since $(2c_0-c_1)^2 = \Delta c_1^2+4\Delta u^2+(2v)^2 \geqslant (2v)^2$, $2c_0-c_1 \geqslant |2v|$ and $l \geqslant 0$. Thus, if $2c_0-c_1 \equiv \pm 2v \pmod{\Delta}$, then l is a non-negative integer for either sign of v.

We want $v^2 \equiv c_0^2 \pmod{4k}$ to imply $c_0 \equiv \pm v (2k)$ in case $j = 0$, and $(2v)^2 \equiv (2c_0-c_1)^2 \pmod{\Delta}$ to imply $2c_0-c_1 \equiv \pm 2v \pmod{\Delta}$ if $j = 1$. This means that, if $j = 0$, k can only be $-1, -2, -p, -2p$ (p any odd prime); and if $j = 1$, Δ can only be an odd prime $p \equiv 1 \pmod 4$. In Article 303 of [1] we find the 65 known values of $\Delta > 0$ for which $v^2+\Delta u^2$ is in a genus of one class. In the case $j = 0$ and with k restricted as mentioned above, the possible values of Δ are $4, 8, 12, 24, 28, 40, 88$, and 232. In the case $j = 1$, the possible values of Δ are 5, 13, and 37.

Again, consider $\Delta = -4k > 0$. If $k = -p$, then $c_0^2 \equiv v^2 \pmod{4p}$ implies $c_0 \equiv \pm v \pmod{2p}$ for one or both signs of v. If $k = -2p$, then $c_0^2 \equiv v^2 \pmod{8p}$ can be split into $c_0^2 \equiv v^2 \pmod 8$ and $c_0^2 \equiv v^2 \pmod p$. If $(c_0, 2) = 1 = (c_0, p)$, then $c_0 \equiv \pm v \pmod 4$ for one and only one sign of v and $c_0 \equiv \pm v \pmod p$ for one and only one sign of v. Thus, we may not be able to guarantee $c_0 \equiv \pm v \pmod{4p}$ whenever $c_0^2 \equiv v^2 \pmod{8p}$ without placing restrictions on c_0, i.e., c_0 even or divisible by p. Since we wish to confine ourselves here to cases where the method works for all c_0, c_1, we shall concern ourselves only with the cases where $k = -p$, i.e., $\Delta = 12, 28$.

Finally, we consider the case $\Delta < 0$. If $\Delta = -4k$, the condition $l \geqslant 0$ may not be satisfied for both signs of v, and $c_0 \equiv \pm v \pmod{2k}$ may hold for only one sign of v with the corresponding $l < 0$. We therefore assume in this paper since $l \geqslant 0$ is not satisfied automatically that $c_0 \equiv \pm v \pmod{2k}$ for both signs of v. Also, if $\Delta = -4k+1$, the condition $l \geqslant 0$ may not be satisfied for both signs of v. Again, we shall assume since $l \geqslant 0$ is not satisfied automatically that $2c_0-c_1 \equiv \pm 2v \pmod{\Delta}$ for both signs of v.

Again, we want $v^2 \equiv c_0^2 \pmod{4k}$ to imply $c_0 \equiv \pm v \pmod{2k}$ in case $j = 0$, and $(2v)^2 \equiv (2c_0-c_1)^2 \pmod{\Delta}$ to imply $2c_0-c_1 \equiv \pm 2v \pmod{\Delta}$ if $j = 1$. If $j = 0$, k can only be $1, 2, p, 2p$ (p any odd prime). Since we want the preceding implication to hold for all c_0, c_1, we must restrict ourselves to the cases where $k = 2$ or $k = p$. If $j = 1$, Δ can only be $-p$ where $p \equiv 3 \pmod 4$.

We may sum up the preceding remarks in the following statement.

THEOREM. *Assume $c_0+c_1\varrho$ is totally positive and that c_1 is even if $4|\Delta$ in the case $\Delta > 0$. Then Pall's algorithm succeeds in giving a formula for the number of representations of $c_0+c_1\varrho$ as a sum of two squares in the quadratic ring $R = \{x_0+x_1\varrho \mid x_0, x_1 \text{ in } Z\}$ if*

(a) *$v^2+\Delta u^2$ is in a genus of one class;*

(b) *all solutions v, u of (5) or (6) have l integral by choice of sign of v if $\Delta > 0$, and for either sign of v if $\Delta < 0$.*

Again, we remark that the positive values of Δ for which Pall's algorithm succeeds are $4, 5, 8, 12, 13, 28$, and 37. It is conjectured that there may be an infinite number of negative values of Δ for which the method succeeds.

2. In discussing the representability of numbers by the form $x^2+\Delta y^2$, we make use of the following well-known result.

LEMMA 1. *An integral, binary quadratic form of discriminant d does not represent a prime p such that $(d|p) = -1$.*

If $\Delta \equiv 1 \pmod 4$, all odd numbers prime to 2Δ represented by the form $x^2+\Delta y^2$ must be congruent to 1 modulo 4. If Δ^* denotes the odd prime dividing Δ, then $x^2+\Delta y^2$ represents primes p such that $p \equiv 1 \pmod 4$ and $(-\Delta^*|p) = 1$. In the case $\Delta \equiv 0 \pmod 4$, let $m = c_0^2+4kc_1'^2$. The exponents of primes q dividing m such that $q \equiv 3 \pmod 4$ and $(-\Delta^*|q) = 1$ must be even by Lemma 1. Likewise, the exponents of primes $\varkappa$ and π dividing m such that $(-\Delta^*|\pi) = -1 = (-\Delta^*|\varkappa)$ and $\pi \equiv 1 \equiv -\varkappa \pmod 4$ must be even. In the case $\Delta \equiv 1 \pmod 4$, let

$$m = c_0^2 - c_0c_1 + kc_1^2 = (c_0 - \tfrac{1}{2}c_1)^2 - (\Delta/4)c_1^2.$$

The exponents of the primes q, π, $\varkappa$ dividing m with the above mentioned properties must also be even. In the case $\Delta = 13$ and 37, the corresponding values of k are odd. Since $2|c_0^2 - c_0c_1 + kc_1^2$ implies c_0 and c_1 are even, the power of 2 in m must be even.

LEMMA 2. *Let $r'(n)$ denote the number of proper representations of n by the system of positive, primitive binary quadratic forms of discriminant d (< 0). If $(d|p) = 1$, then*

$$r'(p^t m) = \begin{cases} 2r'(m) & \text{if} \quad t > 0, \\ r'(m) & \text{if} \quad t = 0. \end{cases}$$

This result may be found in [3].

3. We now proceed to illustrate Pall's method for the case $\Delta = 12$. The problem is now reduced to finding the number of solutions v, u of $c_0^2 - 12c_1'^2 = v^2+12u^2$ which give a non-negative integral value of l such that $d_1 = (c_0, c_1', l)$ contains no prime factor of the form $4n+3$ to an odd exponent. Then for each such value of l, the number of solutions of (1) is $2r_2(d_1)$ if $u^2 \neq 0$ or $r_2(d_1)$ if $u^2 = 0$. Since v, u and v, $-u$ give the same value of l, the factor 2 or 1 multiplying $r_2(d_1)$ will work out correctly if we count all solutions v, u of $c_0^2 - 12c_1'^2 = v^2+12u^2$. We note here that

$$d_1 = (c_0, c_1', l) = (c_0, c_1', v) = (c_0, c_1', v, u).$$

By the preceding remarks on the representability of numbers by the form x^2+12y^2, we may put

$$c_0^2 - 12c_1'^2 = 2^a 3^s \prod p_i^{2\gamma_i+\delta_i} \prod q_i^{2\beta_i} \prod r_i^{2e_i}$$

where the p_i denote primes of the form $12n+1$ and γ_i is the exponent to which p_i occurs in (c_0, c_1'), the q_i are primes of the form $12n \pm 5$, and the r_i are primes of the form $12n+11$.

We first consider the case of $c_0^2 - 12c_1'^2$ odd and prime to 3. If q is a prime such that $q \equiv 5 \pmod{12}$, then $q \equiv 1 \pmod 4$ and $(-3|q) = -1 = (3|q)$. By Lemma 1, $q^\beta \| (v, u)$ and $q^\beta \| (c_0, c_1')$; hence

$$q^\beta \| d_1 \quad \text{and} \quad r_2(d_1) = r_2(q^\beta d_1') = (1+\beta) r_2(d_1').$$

Thus, $r_2(d_1)$ is multiplied by the factor $(1+\beta_i)$ for each $q_i \equiv 5 \pmod{12}$.

If $q \equiv -5 \pmod{12}$ then $q \equiv 3 \pmod 4$, $(-3|q) = 1$, and $(3|q) = -1$. Again, by Lemma 1, $q^\beta \| (c_0, c_1')$. Suppose $q^e \| (v, u)$, $e \leqslant \beta$. Then $q^e \| d_1$, and e must be even if the number of solutions of (1) is to be non-zero. Then $e = 0, 2, \ldots, \beta$ or $\beta-1$, according as β is even or odd. Now $r_2(q^e d_1') = r_2(d_1')$. We now consider solutions of $v_1^2+12u_1^2 = q^{2\beta-2e}m$. By Lemma 2, if $0 \leqslant e < \beta$,

$$r'(q^{2\beta-2e}m) = 2r'(m).$$

If β is even and $e = \beta$, then

$$r'(q^{2\beta-2e}m) = r'(m).$$

For β even, $r_2(d_1)$ is multiplied by twice the number of even integers $\geqslant 0$ and $< \beta$, plus one; for β odd, $r_2(d_1)$ is multiplied by twice the number of even integers $\geqslant 0$ and $\leqslant \beta-1$. In either case, the factor is $1+\beta$; hence $r_2(d_1)$ is multiplied by $1+\beta_i$ for each $q_i \equiv -5 \pmod{12}$.

If $r \equiv 11 \pmod{12}$ then $r \equiv 3 \pmod 4$, $(-3|r) = -1$, and $(3|r) = 1$. $r^e \| (v, u)$ by Lemma 1. Let $r^e \| (c_0, c_1')$, $e \leqslant \varepsilon$. Then $r^e \| d_1$, and we must assume that e is even if the number of solutions of (1) is to be non-zero. Since $r_2(r^e d_1') = r_2(d_1')$, $r_2(d_1)$ is multiplied by the factor 1 for each $r_i \equiv 11 \pmod{12}$.

If $p \equiv 1 \pmod{12}$, we have $p^{2\gamma+\delta} \| c_0^2 - 12c_1'^2$ and $p^\gamma \| (c_0, c_1')$. Suppose $p^e \| (v, u)$. Then $e < \gamma$ or $\gamma \leqslant e \leqslant \gamma + \delta/2$ or $\gamma + (\delta-1)/2$, according as δ is even or odd. We again consider $v_1^2+12u_1^2 = p^{2\gamma+\delta-2e}m$. For $0 \leqslant e < \gamma$, $r'(p^{2\gamma+\delta-2e}m) = 2r'(m)$, and $r_2(d_1) = r_2(p^e d_1') = (1+e)r_2(d_1')$ since $p^e \| d_1$. As e runs from 0 to $\gamma-1$, $r_2(d_1)$ is multiplied by the sum $2(1+2+\ldots+\gamma) = \gamma(\gamma+1)$. If $\gamma \leqslant e$, then $p^\gamma \| d_1$ and $r_2(d_1) = (1+\gamma)r_2(d_1')$. For δ even, e runs from γ to $\gamma+\delta/2$. If $\gamma \leqslant e < \gamma+\delta/2$, $r'(p^{2\gamma+\delta-2e}m) = 2r'(m)$; if $e = \gamma+\delta/2$, $r'(p^{2\gamma+\delta-2e}m) = r'(m)$. Thus, $r_2(d_1)$ is multiplied by $2(1+\gamma)(\delta/2)+(1+\gamma) = (1+\gamma)(1+\delta)$. For δ odd, e runs from γ to $\gamma+(\delta-1)/2$, $r'(p^{2\gamma+\delta-2e}m) = 2r'(m)$ and $r_2(d_1)$ is multiplied by $2(1+\gamma) \times [1+(\delta-1)/2] = (1+\gamma)(1+\delta)$. In either case, we have the factor $(1+\gamma)(1+\delta)$. Combining the results for $0 \leqslant e < \gamma$ and $\gamma \leqslant e$ and adding factors, we obtain $\gamma(1+\gamma)+(1+\delta)(1+\gamma) = (1+\gamma)(1+\gamma+\delta)$ as the multiplying factor of $r_2(d_1)$. Therefore, $r_2(d_1)$ is multiplied by $(1+\gamma_i) \times (1+\gamma_i+\delta_i)$ for each $p_i \equiv 1 \pmod{12}$. If ν denotes the number of integral solutions of (1), then

$$\nu = 4 \prod (1+\gamma_i)(1+\gamma_i+\delta_i) \prod (1+\beta_i). \tag{8}$$

We now consider the case of $c_0^2-12c_1'^2$ odd but divisible by 3. Both c_0 and v are divisible by 3 and putting $c_0 = 3c_0'$ and $v = 3v'$, we obtain $3c_0'^2-4c_1'^2 = 3v'^2+4u^2$ which is impossible unless c_1' and u are divisible by 3. Putting $c_1' = 3c_1''$ and $u = 3u'$, we get $c_0'^2-12c_1''^2 = v'^2+12u'^2$. Continuing in this manner, we finally obtain $c_0^{*2}-12c_1^{*2} = v^{*2}+12u^{*2}$ with $(c_0^*, 3) = 1 = (v^*, 3)$. The exponent s to which 3 occurs in $c_0^2-12c_1'^2$ must be even, say $s = 2\sigma$. Then $c_0^2-12c_1'^2 = 3^{2\sigma}m$ and $3^\sigma \| (c_0, c_1)$. Since $c_0 \equiv v \pmod 6$ and $c_0 \equiv -v \pmod 6$, we get two values for l. We now have $d_1 = (c_0, c_1', 3^{\sigma-1}(c_0^*+v^*))$ and $d_1 = (c_0, c_1', 3^{\sigma-1}(c_0^*-v^*))$. $3^{\sigma-1}\| d_1$ if $c_0^* \not\equiv -v^* \pmod 3$ or if $c_0^* \not\equiv v^* \pmod 3$. $3^\sigma \| d_1$ if $c_0^* \equiv -v^* \pmod 3$ or if $c_0^* \equiv v^* \pmod 3$. We cannot have both $c_0^* \not\equiv -v^* \pmod 3$, $c_0^* \not\equiv v^* \pmod 3$ and both $c_0^* \equiv -v \pmod 3$, $c_0^* \equiv v^* \pmod 3$. Therefore, only one value of l will result in a d_1 exactly divisible by an even power of 3. Since the power of 3 in d_1 does not affect $r_2(d_1)$, formula (8) holds in this case also.

Finally, we consider the case of $c_0^2-12c_1'^2$ even. Both c_0 and v are even, and putting $c_0 = 2c_0'$ and $v = 2v'$, we obtain $c_0'^2-3c_1'^2 = v'^2+3u^2$.

If $a > 2$ then $c_0'^2-3c_1'^2$ is even, and $v' \equiv u \pmod 2$, i.e., $v' = u+2t$. Substituting, we have $v'^2+3u^2 = 4(u^2+ut+t^2)$. Since $4 \mid c_0'^2-3c_1'^2$, c_0' and c_1' are even. Putting $c_0' = 2c_0''$ and $c_1' = 2c_1''$, we get $c_0''^2-3c_1''^2 = u^2+ut+t^2$. Suppose $c_0''^2-3c_1''^2 = 2^{a-4}m$ where m is odd. From results in [3], we see that if $a-4$ is even, the number of representations of $2^{a-4}m$ by u^2+ut+t^2 is the same as the number of representations of m by u^2+ut+t^2; if $a-4$ is odd, the number of representations is zero. Thus, a must be even, say $a = 2a$. Suppose now that $c_0''^2-3c_1''^2 = m$, where m is odd. Since x^2+3y^2 is equivalent to $2(x^2+xy+y^2)$, we have that the number of representations of m by x^2+xy+y^2 is 3 times the number of representations of m by x^2+3y^2. If $m = x^2+3y^2$, we must have x odd and y even, otherwise $m \equiv 3 \pmod 4$ and could not be represented by x^2+12y^2. This gives $m = x^2+12y'^2$, and the number of representations of m by $x^2+12y'^2$ has been determined. Then

$$r = 12\prod(1+\gamma_i)(1+\gamma_i+\delta_i)\prod(1+\beta_i).$$

If $a = 2$ then $c_0'^2-3c_1'^2$ is odd, and we have two possibilities: c_0' odd, c_1' even or c_0' even, c_1' odd. If c_0' is odd and c_1' is even, say $c_1' = 2c_1''$, we have $c_0'^2-12c_1''^2 = v'^2+3u^2$. v' must be odd and u even, say $u = 2u'$, since v'^2+3u^2 cannot represent odd numbers congruent to 3 modulo 4. Therefore, $c_0'^2-12c_1''^2 = v'^2+12u'^2$, and this case is already done.

If c_0' is even and c_1' is odd, we have $4c_0''^2-3c_1'^2 = v'^2+12u^2$, where $c_0' = 2c_0''$. We now have to find all representations of $4c_0''^2-3c_1'^2$ by v'^2+12u^2 such that l is a non-negative integer and (c_0, c_1', l) contains no prime factor of the form $4n+3$ to an odd exponent. We follow the same procedure as before and obtain the following formula:

$$r = 4\prod(1+\gamma_i)(1+\gamma_i+\delta_i)\prod(1+\beta_i).$$

Summing up, we have the following

THEOREM 1. *To find the number r of integral solutions of*

$$c_0+2c_1'\sqrt{3} = (a_0+a_1\sqrt{3})^2+(b_0+b_1\sqrt{3})^2,$$

where $c_0 > 0$, we may set

$$c_0^2-12c_1'^2 = 2^{2\alpha}3^{2\sigma}\prod p_i^{2\gamma_i+\delta_i}\prod q_i^{3\beta_i}\prod r_i^{2\varepsilon_i}$$

where the p_i denote primes of the form $12n+1$ and γ_i is the exponent to which p_i occurs in (c_0, c_1'), the q_i are primes of the form $12n\pm5$, and the r_i are primes of the form $12n+11$. In order that r shall not be zero, it is necessary that the exponents of the primes $2, 3$, q_i and r_i be even, as indicated, and that the r_i shall occur in (c_0, c_1') to even exponents $\geqslant 0$. With these conditions holding,

$$r = 4\varepsilon_\alpha\prod(1+\gamma_i)(1+\gamma_i+\delta_i)\prod(1+\beta_i)$$

where $\varepsilon_\alpha = 1$ if $\alpha = 0$ or 1 and $\varepsilon_\alpha = 3$ if $\alpha \geqslant 2$.

The procedure for the case of $\Delta = 28$ is the same as that for $\Delta = 12$ except for the prime 2, which we shall now indicate. Here, $c_0^2-28c_1'^2 = v^2+28u^2$. Suppose $c_0^2-28c_1'^2 = 2^\alpha m$ where m is odd and $\alpha > 0$. Both c_0 and v are even, say $c_0 = 2c_0'$ and $v = 2v'$. This gives $c_0'^2-7c_1'^2 = 2^{\alpha-2}m = v'^2+7u^2$. If $c_0'^2-7c_1'^2$ is even, then $v' \equiv u \pmod 2$, i.e., $v' = u+2t$. Substituting, we obtain $v'^2+7u^2 = 4(2u^2+ut+t^2)$. The number of representations of $4n$ by the form x^2+7y^2 is the same as the number of representations of n by the form $x^2+xy+2y^2$. In this case, $n = 2^{\alpha-4}m$ and the number of representations of $2^{\alpha-4}m$ by $x^2+xy+2y^2$ is $\alpha-3$ times the number of representations of m by $x^2+xy+2y^2$. This result may be found in [3]. If $c_0'^2-7c_1'^2$ is odd, then $\alpha = 2$, and we have $c_0'^2-7c_1'^2 = m = v'^2+7u^2$. This case can be handled as before. We can now state the following

THEOREM 2. *To find the number r of integral solutions of*

$$c_0+2c_1'\sqrt{7} = (a_0+a_1\sqrt{7})^2+(b_0+b_1\sqrt{7})^2,$$

where $c_0 > 0$, we may set

$$c_0^2-28c_1'^2 = 2^\alpha 7^{2\sigma}\prod p_i^{2\gamma_i+\delta_i}\prod q_i^{2\beta_i}\prod r_i^{2\varepsilon_i}$$

where the p_i are primes of the form $28n+1$, $28n+5$, $28n+9$, $28n+25$ and γ_i is the exponent to which p_i occurs in (c_0, c_1'), the q_i are primes of

the form $28n+3$, $28n\pm11$, $28n\pm13$, $28n+23$, *and the* r_i *are primes of the form* $28n+19$ *and* $28n+27$. *In order that* v *shall not be zero, it is necessary that the exponents of the primes* 7, q_i, *and* r_i *be even, as indicated, and that the* r_i *shall occur in* (c_0, c_1') *to even exponents* $\geqslant 0$, *with these conditions holding,*

$$v = 4\varepsilon_a \prod (1+\gamma_i)(1+\gamma_i+\delta_i) \prod (1+\beta_i)$$

where $\varepsilon_a = 1$ *if* $a = 0, 2$ *and* $\varepsilon_a = a-3$ *if* $a \geqslant 4$.

Following Pall's proof of Theorem 3 in [2] for the case $\Delta = 5$, we obtain the results for the cases $\Delta = 13$ and $\Delta = 37$. These results are stated in the next two theorems.

THEOREM 3. *To find the number* v *of integral solutions of*

$$c_0+c_1\varrho = (a_0+a_1\varrho)^2+(b_0+b_1\varrho)^2,$$

where

$$\varrho = (-1+\sqrt{13})/2, \quad c_0 > 0, \quad c_0 \geqslant c_1/2,$$

we may set

$$c_0^2-c_0c_1-3c_1^2 = 2^{2\alpha}13^{\sigma}\prod p_i^{q_i}\prod q_i^{2\beta_i}\prod \pi_i^{2\varepsilon_i}\prod \varkappa_i^{2\eta_i},$$

where the p_i *denote primes such that*

$$(-13\,|\,p) = 1 \quad \text{and} \quad p \equiv 1 \pmod 4;$$

the q_i *satisfy*

$$(-13\,|\,q) = 1 \quad \text{and} \quad q \equiv 3 \pmod 4;$$

similarly

$$(-13\,|\,\pi) = -1 = (-13\,|\,\varkappa), \quad \pi \equiv 1 \equiv -\varkappa \pmod 4.$$

In order that v *shall not be zero, it is necessary that the exponents of the* q_i, π_i, *and* $\varkappa_i$ *shall be even, as indicated, and that the* $\varkappa_i$ *shall occur in* (c_0, c_1) *to even exponents* $\geqslant 0$. *With these conditions holding,*

$$v = 4(1+\sigma)\prod (1+\gamma_i)(1+\gamma_i+\delta_i)\prod (1+\beta_i)\prod (1+\varepsilon_i),$$

where $\alpha_i = 2\gamma_i+\delta_i$ *and* γ_i *is the exponent to which* p_i *occurs in* (c_0, c_1).

THEOREM 4. *To find the number* v *of integral solutions of*

$$c_0+c_1\varrho = (a_0+a_1\varrho)^2+(b_0+b_1\varrho)^2,$$

where

$$\varrho = (-1+\sqrt{37})/2, \quad c_0 > 0, \quad c_0 \geqslant c_1/2,$$

we may set

$$c_0^2-c_0c_1-9c_1^2 = 2^{2\alpha}37^{\sigma}\prod p_i^{q_i}\prod q_i^{2\beta_i}\prod \pi_i^{2\varepsilon_i}\prod \varkappa_i^{2\eta_i},$$

where the p_i *denote primes such that*

$$(-37\,|\,p) = 1 \quad \text{and} \quad p \equiv 1 \pmod 4;$$

the q_i *satisfy*

$$(-37\,|\,q) = 1 \quad \text{and} \quad q \equiv 3 \pmod 4;$$

similarly

$$(-37\,|\,\pi) = -1 = (-37\,|\,\varkappa), \quad \pi \equiv 1 \equiv -\varkappa \pmod 4.$$

In order that v *shall not be zero, it is necessary that the exponents of the* q_i, π_i, *and* $\varkappa_i$ *shall be even, as indicated, and that the* $\varkappa_i$ *shall occur in* (c_0, c_1) *to even exponents* $\geqslant 0$. *With these conditions holding*

$$v = 4(1+\sigma)\prod (1+\gamma_i)(1+\gamma_i+\delta_i)\prod (1+\beta_i)\prod (1+\varepsilon_i),$$

where $\alpha_i = 2\gamma_i+\delta_i$ *and* γ_i *is the exponent to which* p_i *occurs in* (c_0, c_1).

4. In this part we shall make use of the following notions and results from [4].

Two representations of m in the form $f = [a, b, c] = ax^2+bxy+cy^2$ will be called *equivalent* if they are transformable one into the other by integral unimodular 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 $f(m)$.

For any d $(= b^2-4ac)$ there are a finite number h of (primitive) classes of forms, say $C_0, C_1, \ldots, C_{h-1}$. Representative forms from these classes are denoted respectively $f_0, f_1, \ldots, f_{h-1}$. The system of representative forms will be designated S. The sum of the numbers of sets of representations of n in the h forms will be denoted by $S(n)$, so that

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

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

$$\begin{aligned} x &= \tfrac{1}{2}(t-bu)x_0-cuy, \\ y &= aux_0+\tfrac{1}{2}(t+bu)y, \end{aligned} \tag{9}$$

as t, u *range over all solutions of*

$$t^2-du^2 = 4.$$

If x, y and x_0, y_0 are related by (9), we say x, y and x_0, y_0 are equivalent representations on f. All x, y equivalent to a given one comprise a set. The g.c.d. of x and y is the same for all x, y of a set. Sets in which x, y have g.c.d. 1 are called *primitive sets*.

Let $f'(m)$ denote the number of primitive sets of representations of m in $f=[a,b,c]$. The number of primitive sets of representations of m in S is

$$S'(m)=f'_0(m)+f'_1(m)+\ldots+f'_{h-1}(m).$$

Also,

$$S(n) \text{ and } S'(n) \text{ are factorable,}$$

and

$$S'(1)=S'(-1)=S(1)=S(-1)=1.$$

For any prime $p\geqslant 2$,

$$\begin{aligned} S'(p^a) &= 1+(d|p) && \text{if} \quad p\nmid d,\\ S(p^a) &= a+1 && \text{if} \quad (d|p)=1,\\ &= \tfrac{1}{2}\{1+(-1)^a\} && \text{if} \quad (d|p)=-1,\\ &= 1 && \text{if} \quad p|d \text{ but } p^2\nmid d \text{ if } p>2 \text{ or } d\equiv 0 \text{ or } 4 \pmod{16} \text{ if } p=2. \end{aligned}$$

In this section we shall treat the case of $\Delta<0$, i.e., $v^2+\Delta u^2$ is an indefinite form. As noted before, the number of solutions of (1) in integers is infinite if not zero. If (1) has an infinite number of solutions, they may be divided into a finite number of sets of solutions. Following Pall's suggestions in [2], we proceed to examine how this might be done.

If we take $c_0+c_1\varrho=1$, we have $v^2+\Delta u^2=1$, i.e., we have to solve the Pell equation

$$x^2+\Delta u^2=1 \tag{10}$$

with $x=1+(\Delta l)/2$. Let x_1, u_1 be the least positive solution of (10). If $x_1\equiv 1 \pmod{\Delta}$, the same will hold for all positive solutions x, since the general solution with x_k and u_k positive satisfies the recursion formula $x_{k+1}x_1+u_ku_1$. If $x_1\not\equiv 1 \pmod{\Delta}$, then $x_2=x_1^2+\Delta u_1^2\equiv 1 \pmod{\Delta}$, and only the values x_k with k even will furnish integral values of l in $x_k=1+\frac{}{}+(\Delta l)/2$. In either case the number of values of l so obtained is infinite, and since d_1 (the g.c.d. of $1, 0, l$) is 1, eight representations as a sum of two squares correspond to each value of l (four representations if $u=0$, $x=1$, $l=0$).

We first consider the case $\Delta=-4k$. For any $c_0+c_1\varrho$, consider a particular solution l_0, u_0 of

$$(2kl_0+c_0)^2-4ku_0^2=c_0^2+4kc_1^2 \tag{11}$$

for which $l_0\geqslant 0$ and (c_0, c_1, l_0) contains no prime factor $4n+3$ to an odd exponent. For any r, s such that $r^2-4ks^2=1$ and $r\equiv 1 \pmod{2k}$, the expressions

$$\begin{aligned} 2kl+c_0 &= r(2kl_0+c_0)+rksu_0,\\ u &= s(2kl_0+c_0)+ru_0 \end{aligned} \tag{12}$$

determine another solution l, u of (11). We say that such solutions are in the same set. Since $k=1, 2,$ or p, $(c_0, c_1, l_0)=(c_0, c_1, l)$; hence (c_0, c_1, l) contains no prime factor $4n+3$ to an odd exponent. Each set contains a subset of solutions l, u of (11) for which $l\geqslant 0$. It is these subsets which are of interest to us. The values of $d_1=(c_0, c_1, l)$ are the same for all solutions in a set. Thus, $2r_2(d_1)$ representations as a sum of two squares correspond to each value of $l\geqslant 0$ with $u\neq 0$; $r_2(d_1)$ representations correspond to each value of $l\geqslant 0$ with $u=0$. Each member l, u with $l\geqslant 0$ of a set of solutions of (11) produces $2r_2(d_1)$ (or $r_2(d_1)$) solutions of (1). Hence, for each set of solutions of (11) with non-negative values of l, there corresponds $2r_2(d_1)$ (or $r_2(d_1)$) sets of solutions of (1). An examination of (9) with $d=16k$, $a=1$, $b=0$, $c=-4k$ shows that solutions of (11) determined by (12) are in the same set in the sense of [4]. We can find the number of sets of solutions of (1) by finding the number of sets of solutions of (11) with the results in [4] and the value of d_1 associated with each set. For each solution l, u of (11), there corresponds a solution v, u of (5) with $v=2kl+c_0$. With each solution v, u of (5) are associated the three other solutions $-v, -u$, $v, -u$ and $-v, u$ if $u\neq 0$ (only $-v, u$ if $u=0$). The solutions v, u and $-v, -u$ of (5) are in the same set in the sense of [4]; likewise $v, -u$ and $-v, u$ belong to the same set. The number of sets of solutions of (11) can be determined from the number of sets of solutions of (5).

For the case $\Delta=-4k+1$, the same procedure can be carried out with the obvious modifications.

For the case $\Delta=-8$, we obtain the following result.

THEOREM 5. *To find the number N of sets of integral solutions of*

$$c_0+2c_1'\sqrt{-2}=(a_0+a_1\sqrt{-2})^2+(b_0+b_1\sqrt{-2})^2,$$

we may set

$$c_0^2+8c_1'^2=2^a\prod p_i^{2\gamma_i+\delta_i}\prod q_i^{2\beta_i}\prod r_i^{2\varepsilon_i}\prod s_i^{2\eta_i}$$

where the p_i denote primes of the form $8n+1$ and γ_i is the exponent to which p_i occurs in (c_0, c_1'), the q_i are primes of the form $8n+5$, the r_i are primes of the form $8n+7$, and the s_i are primes of the form $8n+3$. In order that N shall not be zero, it is necessary that the exponents of the q_i, r_i and s_i be even, as indicated, and that the s_i shall occur in (c_0, c_1') to even exponents $\geqslant 0$. With these conditions holding,

$$N=4\zeta_a\prod(1+\beta_i)\prod(1+\varepsilon_i)\prod(1+\gamma_i)(1+\gamma_i+\delta_i)$$

where $\zeta_0=1$ and $\zeta_a=2$ if $a>0$.

The method of proof here is quite similar to that of Theorem 1 except for the prime 2.

We now state the general result for $\Delta = -4p$, p and odd prime.

THEOREM 6. *To find the number N of sets of integral solutions of*

$$c_0+2c_1'\sqrt{-p} = (a_0+a_1\sqrt{-p})^2+(b_0+b_1\sqrt{-p})^2,$$

we may set

$$c_0^2+4pc_2'^2 = 2^a p^b \prod p_i^{2\gamma_i+\delta_i} \prod q_i^{2\beta_i} \prod \pi_i^{2\varepsilon_i} \prod \varkappa_i^{2\eta_i},$$

where the p_i denote primes such that

$$(p\,|\,p_i) = 1 \quad \textit{and} \quad p_i \equiv 1 \pmod 4;$$

the q_i satisfy

$$(p\,|\,q_i) = 1 \quad \textit{and} \quad q_i \equiv 3 \pmod 4;$$

similarly

$$(p\,|\,\pi_i) = -1 = (p\,|\,\varkappa_i), \quad \pi_i \equiv 1 \equiv -\varkappa_i \pmod 4.$$

In order that N shall not be zero, it is necessary that the exponents of the q_i, π_i, and $\varkappa_i$ shall occur in (c_0, c_1') to even exponents $\geqslant 0$. With these conditions holding,

$$N = 4\zeta_a\theta_b \prod (1+\beta_i) \prod (1+\varepsilon_i) \prod (1+\gamma_i)(1+\gamma_i+\delta_i)$$

where γ_i denotes the power of p_i dividing (c_0, c_1') and, where ζ_a and θ_b are determined as follows:

$$\theta_b = \begin{cases} b+1 & \textit{if} \quad p \equiv 1 \pmod 4, \\ 1 & \textit{if} \quad p \equiv 3 \pmod 4 \ \textit{and} \ b \ \textit{is even}, \\ 2 & \textit{if} \quad p \equiv 3 \pmod 4 \ \textit{and} \ b = 2\sigma+1 \ \textit{with} \ \sigma \ \textit{even}, \\ 0 & \textit{if} \quad p \equiv 3 \pmod 4 \ \textit{and} \ b = 2\sigma+1 \ \textit{with} \ \sigma \ \textit{odd}; \end{cases}$$

$$\zeta_a = \begin{cases} 1 & \textit{if} \quad p \equiv 3 \pmod 4, \ a = 0, 2 \ \textit{or} \ a \geqslant 3, \\ 1 & \textit{for} \quad a = 0, 2, \ \textit{and} \ p \equiv 1 \pmod 4, \\ a-3 & \textit{for} \quad a \geqslant 4 \ \textit{and} \ p \equiv 1 \pmod 8, \\ 1 & \textit{for} \quad a \geqslant 4, \ a \ \textit{even}, \ p \equiv 5 \pmod 8, \\ 0 & \textit{for} \quad a \geqslant 4, \ a \ \textit{odd}, \ p \equiv 5 \pmod 8. \end{cases}$$

For the cases $\Delta = -4k+1 = -p$, where $p \equiv 3 \pmod 4$, we can prove the following theorem by our method.

THEOREM 7. *Let $\varrho = (-1+\sqrt{-p})/2$. To find the number N of sets of integral solutions of*

$$c_0+c_1\varrho = (a_0+a_1\varrho)^2+(b_0+b_1\varrho)^2,$$

we may set

$$c_0^2-c_0c_1+kc_1^2 = 2^a p^b \prod p_i^{2\gamma_i+\delta_i} \prod q_i^{2\beta_i} \prod \pi_i^{2\varepsilon_i} \prod \varkappa_i^{2\eta_i},$$

where the p_i denote primes such that

$$(p\,|\,p_i) = 1 \quad \textit{and} \quad p_i \equiv 1 \pmod 4;$$

the q_i satisfy

$$(p\,|\,q_i) = 1 \quad \textit{and} \quad q_i \equiv 3 \pmod 4;$$

similarly

$$(p\,|\,\pi_i) = -1 = (p\,|\,\varkappa_i), \quad \pi_i \equiv 1 \equiv -\varkappa_i \pmod 4.$$

In order that N shall not be zero, it is necessary that the exponents of the q_i, π_i, and $\varkappa_i$ shall be even, as indicated, and that the $\varkappa_i$ shall occur in (c_0, c_1) to even exponents $\geqslant 0$. With these conditions holding,

$$N = 4\theta_b \prod (1+\beta_i) \prod (1+\varepsilon_i) \prod (1+\gamma_i)(1+\gamma_i+\delta_i)$$

where γ_i denotes the power of p_i dividing (c_0, c_1) and $\theta_b = 1$ if b is even, $\theta_b = 2$ if $b = 2\sigma+1$ and σ is even, and $\theta_b = 0$ if $b = 2\sigma+1$ and σ is odd.

Once a practical reduction technique for binary quadratic forms with coefficients in a quadratic ring becomes available, it will be interesting to see whether the discriminants of the rings for which x^2+y^2 is in a genus of one class turn out to be those for which Pall's method succeeds.

The author would like to point out that some of these results are cognate with those of Nagell in [5] but were obtained by an entirely different method.

References

[1] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[2] G. Pall, *Sums of two squares in a quadratic field*, Duke Math. Journ. 18 (1951), pp. 399-409.

[3] — *The structure of the number of representations function in a positive binary quadratic form*, Math. Zeitschr. 36 (1933), pp. 321-343.

[4] — *The structure of the number of representations function in a binary quadratic form*, Trans. Amer. Math. Soc. 35 (1933), pp. 491-509.

[5] Trygve Nagell, *On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields*, Nova Acta Soc. Sci. Upsal 4 (11) (1953).

THE UNIVERSITY OF GEORGIA
ATHENS, GEORGIA

Reçu par la Rédaction le 18. 8. 1967