SUMS OF FOUR SQUARES IN A QUADRATIC RING[1]

BY

HARVEY COHN AND GORDON PALL

1. **Introduction.** Let d be a nonsquare integer of the form $4k+j$ (k integral, $j=0$ or 1). Let Z be the ring of rational integers, R_d the ring of numbers $\xi = x_0 + x_1\omega$, where $\omega = (j+\sqrt{d})/2$, x_0 and x_1 ranging over Z.

In §2 we will transform the problem of solving

$$\sigma = \xi_0^2 + \xi_1^2 + \xi_2^2 + \xi_3^2 \qquad (\xi_0, \cdots, \xi_3 \text{ in } R_d),$$

where $\sigma = s_0 + s_1\omega$ is a given number in R_d, into the problem of representing the norm $N\sigma = s_0^2 + js_0s_1 - ks_1^2$ by the form

$$F_d = t_0^2 + dt_1^2 + dt_2^2 + dt_3^2 \qquad (t_0, \cdots, t_3 \text{ in } Z);$$

with the nontrivial restriction on t_0 that $b = (T\sigma - 2t_0)/d$ shall be a nonnegative integer, $T\sigma$ denoting the trace $2s_0 + js_1$ of σ. This transformation of the problem uses a recent theorem of Pall and Taussky (see [12]) on the number of representations of a binary quadratic form as a sum of four squares of linear forms.

Relatively little is known of the theory of reduction of quadratic forms over R_d, as compared with Z. As an example, it seems to be true that $d=5$ and 8 are the only positive ring discriminants for which the form $H_d = \xi_0^2 + \cdots + \xi_3^2$ is in a genus of one class; but such results may be hard to prove, by available methods. Hence our transformation of the problem is advantageous. The restriction on the values of t_0 is no handicap in the study of qualitative questions, concerning the mere representability as a sum of four squares in R_d. Hence we are able to obtain quite complete results of a qualitatative kind in Part I (cf. Niven [7]). Certain conjectures made by Cohn on the basis of machine calculations (see [1]) are confirmed. We might have simplified some details of proof if we had restricted R_d to be maximal, as some writers do. Such restrictions are unnatural: thus it is as significant that a totally positive number $s_0 + s_1(-3)^{1/2}$ (with s_1 necessarily even) is a sum of four squares of numbers $x_0 + x_1(-3)^{1/2}$ as the similar fact for $s_0 + s_1\omega$, $\omega = \frac{1}{2}(1+(-3)^{1/2})$.

Among the simplest consequences of Part I is that the only values d for which every σ satisfying the obviously necessary conditions is a sum of four squares in R_d are $d=5$, 8, and 12, and the negative d's not divisible by 16. At the referee's suggestion we examined the remaining d's as regards sums of five or more squares,

Received by the editors September 7, 1961.

(1) Research supported in part by National Science Foundation Grant G-7412.

and found that if $d < 0$ and $16 \mid d$, five squares will suffice; while if $d > 12$ there are numbers not sums of any numbers of squares. Of interest is that for positive $d \equiv 1 \pmod 8$ there exist numbers of arbitrarily large norms, which satisfy the obviously necessary conditions and yet are not sums of four squares in R_d.

Our treatment is entirely elementary. In Part II we develop an algorithm whereby in certain cases our transformation of the problem permits derivation of formulae for the number of representations of σ as a sum of four squares. We carry this through for $d = 5$, 8, and as far as possible for 12. These cases had been treated previously, using Hilbert modular functions of two complex variables, by Götzky for $d = 5$ [5; 13], and by Cohn for $d = 8$ [2] and for some cases when $d = 12$ [2; 3] (making use of Theorem 7, Corollary 2 and (70a) below). Of interest is that, although when d is not a square the weighted number of representations of n by the genus of F_d is not a factorable function of n, it becomes factorable when n is confined to the multiplicative subgroup of norms $s_0^2 + js_0s_1 - ks_1^2$ of discriminant d. The algorithm here developed is being applied to forms in two or four variables by one of our students. For the literature in fields, not rings, see [4a].

Notations. Lower case Latin letters denote rational integers; Greek letters elements of R_d if not stated otherwise. In Part I, the symbols d, k, j, ω, R_d, Z have the meanings in the introductory paragraph. Throughout, $\sigma = s_0 + s_1\omega$; the norm $N\sigma = s_0^2 + js_0s_1 - ks_1^2$; the trace $T\sigma = 2s_0 + js_1$; $r_4(n)$ is the number of representations of n as a sum of four squares in Z_d; $r_4(\sigma, d)$ the number of representations of σ as a sum of four squares in R_d. In Part I, O and E designate odd or even numbers, which may change from one place to another; L similarly denotes "any" integer of the form $4^h(8n + 7)$, h nonnegative, h and n integral.

PART I

2. **The Pall-Taussky formula and its transformation to our problem.** For given s_0, s_1 we wish to solve the equation

$$s_0 + s_1\omega = (a_0 + b_0\omega)^2 + \cdots + (a_3 + b_3\omega)^2 \tag{1}$$

in integers $a_0, b_0, \cdots, a_3, b_3$. Since ω is irrational and $\omega^2 = j\omega + k$, the solution is equivalent to expressing s_0 in all ways as $a + kb$ in nonnegative integers a and b, and finding the integers a_i, b_i such that

$$a = \sum a_i^2, \quad b = \sum b_i^2, \quad s_1 - jb = 2\sum a_ib_i. \tag{2}$$

Here the summation index i goes from 0 to 3. Now (2) amounts to expressing a binary quadratic form as a sum of four squares of linear forms with integral coefficients:

$$ax^2 + (s_1 - jb)xy + by^2 = \sum (a_ix + b_iy)^2. \tag{3}$$

The Pall-Taussky formula is for the number of such expressions of a binary

quadratic form, and is in our present notations as follows. Necessarily, $s_1 - jb$ is even. Let e denote the g.c.d. $(a,(s_1 - jb)/2, b)$, le the g.c.d. $(a, s_1 - jb, b)$, so that l is 1 or 2. Then the Pall-Taussky formula is

$$\sum_{(t_1,t_2,t_3)} r_4(lh), \tag{4}$$

where $h = (t_1, t_2, t_3, e)$, and one term of the sum occurs for each ordered triple t_1, t_2, t_3 of integers satisfying

$$ab - (s_1 - jb)^2/4 = t_1^2 + t_2^2 + t_3^2. \tag{5}$$

Accordingly, $r_4(\sigma, d)$ will be obtained from (4) by summing (4) over b, or, what is the same thing,

$$r_4(\sigma, d) = \sum_{(b,t_1,t_2,t_3)} r_4(lh), \tag{6}$$

where b ranges over all nonnegative integers ($b > 0$ if $s_0 < 0$; $b \equiv s_1 \pmod 2$ if d is odd), and for each such b, the t_i range over integers satisfying

$$(s_0 - kb)b - (s_1 - jb)^2/4 = t_1^2 + t_2^2 + t_3^2. \tag{5'}$$

The product of the left member of (5′) by $d = 4k + j$ simplifies to $N\sigma - t_0^2$, where $t_0 = (T\sigma - db)/2$. Hence (5′) can be replaced by

$$N\sigma = t_0^2 + dt_1^2 + dt_2^2 + dt_3^2, \tag{7}$$

where t_0 is to be restricted so that $(T\sigma - 2t_0)/d$ is a nonnegative integer b. Automatically, b has the parity of s_1 if d is odd. It is not hard to deduce from (7), written in the form

$$(T\sigma)^2 - (2t_0)^2 = d(s_1^2 + 4t_1^2 + 4t_2^2 + 4t_3^2), \tag{7'}$$

and the fact that $b \geqq 0$, and that $Q_b \geqq 0$, where

$$Q_b = \{N\sigma - ((T\sigma - db)/2)^2\}/d, \tag{8}$$

that if d is positive, then the solvability of (1) requires that

$$N\sigma \geqq 0 \text{ and } T\sigma \geqq 0. \tag{9}$$

In other words, σ must be totally positive, a fact otherwise evident. Total positiveness of σ, and s_1 even if d is even, are the "trivially necessary" conditions for solvability of (1) when d is positive.

Further, if d is positive and (9) holds, then for any integer t_0 satisfying (7) and $2t_0 \equiv T\sigma \pmod d$, the integer b determined by $b = (T\sigma - 2t_0)/d$ is always nonnegative; for, $Q_b \geqq 0$ if and only if

$$(T\sigma - 2(N\sigma)^{1/2})/d \leqq b \leqq (T\sigma + 2(N\sigma)^{1/2})/d, \tag{10}$$

where, since $(T\sigma)^2 = 4N\sigma + ds_1^2$, the left member is nonnegative. Thus when d is

positive, b is confined to a finite interval of length $4(N\sigma)^{1/2}/d$. But if $d < 0$, $Q_b \geqq 0$ if and only if $b \geqq (T\sigma - 2(N\sigma)^{1/2})/d$, an interval of infinite length. This advantage to d negative is somewhat compensated by the fact that, as (7′) shows, changing t_0 to $-t_0$ then changes the sign of b.

Our basic result will be used so often that we state it as a theorem:

THEOREM 1. *Let σ have s_1 even if d is even. Then* (1) *is solvable if and only if there exists a nonnegative integer b for which Q_b is a nonnegative integer not of the form L.*

The condition $2t_0 \equiv T\sigma \pmod{d}$ is satisfied for all integral solutions $t_0, \cdots, t_3$ of (7) in certain cases, and for exactly half the solutions in certain others:

THEOREM 2. *If d or $\frac{1}{4}d$ is a prime, then if* (9) *holds, and s_1 is even when d is even,* (1) *is solvable if and only if $N\sigma$ is represented by F_d.*

Proof. For any solution of (7),

$$(T\sigma)^2 \equiv (2t_0)^2 \pmod{d} \text{ if } d \text{ is odd}, \qquad s_0^2 \equiv t_0^2 \pmod{d} \text{ if } d \text{ is even}.$$

Hence if d is an odd prime, $2t_0 \equiv T\sigma \pmod{d}$ holds for both signs of t_0 if $d \mid N\sigma$, by choice of that sign otherwise. If $d = 4p$ (p prime), we need $t_0 \equiv s_0 \pmod{2p}$; this holds automatically if $p \mid s_0$, by choice of sign of t_0 otherwise.

3. **The universal discriminants.** A discriminant d is called universal if (1) is solvable for every σ satisfying the obviously necessary conditions, (9) if $d > 0$, $2 \mid s_1$ if $2 \mid d$. For field discriminants, some restrictions on d were known quite early but there probably is no exact reference prior to 1928 [5].

LEMMA 1. *d is not universal if d is divisible by* 16 *or $d > 12$.*

Proof. It will be convenient, when $d = 4k$, to set

$$\begin{aligned} k &= 2^u k', \ k' \quad \text{odd}, \ u \geqq 0; \quad N\sigma = 2^w s, \qquad s \text{ odd}, \ w \geqq 0; \\ s_0 &= 2^v s_2, \ s_2 \quad \text{odd}, \ v \geqq 0; \quad s_1 = 2^{g+1} s_3, \quad s_3 \text{ odd}, \ g \geqq 0; \end{aligned} \tag{11}$$

the last two if $s_0 s_1 \neq 0$, otherwise we can take v or g arbitrarily large.

To obtain a number σ for which (1) is unsolvable, when $16 \mid d$, we can take $g = 0$, and $v = \frac{1}{2}(u + 2)$ (> 1) or $v = \frac{1}{2}(u + 3)$ (> 2) according as u is even or odd. Then $t_0/2^v = s_2 - 2^{u+1-v} k' b$ is odd for every integer b, and $N\sigma = 2^{2v} s_2^2 - d s_3^2$. Hence $N\sigma - t_0^2$ has the excluded form dL for every integer b.

If d is positive take $\sigma = s_0 + (2 - j)\omega$, where s_0 is the positive integer determined by the inequalities

$$(2s_0 - 1)^2 < d < (2s_0 + 1)^2 \ (d \text{ odd}), \quad (s_0 - 1)^2 < 4k < s_0^2 \ (d \text{ even}).$$

Then $2s_0 + 1 < 2 + d^{1/2}$, $s_0 < 1 + (4k)^{1/2}$ respectively, and hence (cf. (10))

$(T\sigma+2(N\sigma)^{1/2})/d<(2+d^{1/2}+(4+4d^{1/2})^{1/2})/d$ or $(2+4k^{1/2}+2(1+4k^{1/2})^{1/2})/d<1$, provided $d>12$. Hence (1) is unsolvable for this σ if $d>12$.

LEMMA 2. *If $d>12$, the number $s_0+(2-j)\omega$ defined above is not a sum of five, or indeed any number of, squares of elements of R_d.*

Proof. We will suppose $j=1$, the proof for $j=0$, starting with the inequality $0<s_0-2k^{1/2}<1$, being similar. We have

$$0<s_0+\bar{\omega}<1, \text{ where } \bar{\omega}=(1-d^{1/2})/2.$$

Hence if $s_0+\bar{\omega}$ is a sum of squares $\sum\alpha^2$, all the terms satisfy $0\leqq\alpha^2<1$, and hence for any nonzero term α^2, $\bar{\alpha}^2>1$. Since $s_0+\bar{\omega}$ is not a sum of four squares, at least five of the terms α^2 are not zero, and being less than 1 each of these terms is irrational. If one of these, say α^2, is $(t+u\sqrt{d})/2$, then $\bar{\alpha}^2=(t-u\sqrt{d})/2$, and $\bar{\alpha}^2-\alpha^2=-u\sqrt{d}\geqq\sqrt{d}$ (since $\bar{\alpha}^2>\alpha^2$). Subtracting from $s_0+\omega=\sum\bar{\alpha}^2$, we have $\sqrt{d}\geqq 5\sqrt{d}$, a contradiction.

THEOREM 3. *d is universal if and only if d is 5, 8, or 12, or negative but not divisible by 16. If $d>12$ there exists a totally positive number $s_0+(2-j)\omega$ which is not a sum of squares; if $d<0$ and $16\mid d$, every number (with s_1 even) is a sum of five squares.*

Since as noted after (10) the interval for b is infinite, the proof for $d<0$ is an immediate deduction from Theorems 4, 5, 6, along with observation (for the last part of Theorem 3) that either σ or $\sigma-1$ will not satisfy (13). We assume $d>0$. By Lemma 1, d can only be 5, 8, or 12, and by Theorem 2 it suffices to show that F_d represents all positive norms $s_0^2+js_0s_1-ks_1^2$ (s_1 even if $d=8$ or 12).

If $d=5$ no norm is double an odd. It therefore suffices to treat odd norms of the forms $5q+0$, 4, or 16, with $q=8k+7$; note $5q-25$, $q-5\neq L$; $5q+4-9$, $q-1\neq L$; $5q+16-1$, $q+3\neq L$. If $d=8$, note first that F_2 represents all positive integers: thus, $2n+0,1$, $n=4^h(8k+7)$; $2n-4$, $n-2\neq L$; $2n+1-9$, $n-4\neq L$ if $h=0,1$; $2n+1-25$, $n-12\neq L$ if $h\geqq 2$. Hence F_8 represents all even norms. There remain only odd norms $8n+1$, $n=4^h(8k+7)$; $8n+1-9$, $n-1\neq L$ if $h=0,1$; $8n+1-25$, $n-3\neq L$ if $h\geqq 2$. Let $d=12$. First, F_{12} represents all even norms, since F_3 represents all positive $3n+0$, 1; for if $n=4^h(8k+7)$, use $3n-9$, $n-3\neq L$ if $h\geqq 1$; $3n-36$, $n-12\neq L$ if $h=0$; $3n+1-4$, $n-1\neq L$ if $h=0,1$; $3n+1-16$, $n-5\neq L$ if $h\geqq 2$. For odd norms $12n+1$, if $n=4^h(8k+7)$, $12n+1-25$, $n-2\neq L$.

Previous proofs of universality for $d=5$ and 8 used modular functions; for $d=12$, there is a previous proof [2; 3] only if σ is even or $N\sigma$ large.

4. **Further analysis of Theorem 1.** Assume σ to satisfy the necessary conditions (9), and s_1 even if d is even.

If $d > 0$ the interval (10) contains at least q integers b (with the parity of s_1 if d is odd) if

$$N\sigma \geqq q^2d^2/4 \ (d \text{ odd}), \quad N\sigma \geqq q^2d^2/16 \ (d \text{ even}). \tag{12}$$

If it can be shown that $Q_b \neq L$ for at least one of every q (or $2q$, if d is odd) consecutive integers b, then it will follow that (1) is solvable if $d < 0$, and when (12) holds if $d > 0$.

Theorem 4 will give the cases in which Q_b has the form L for every integer b, so that (1) is surely not solvable. In all other cases Theorems 5 and 6 will prove the existence of an integer q (which we have tried to make best possible in each case) with the aforestated property. Hence in these other cases (1) is solvable if $d < 0$, or (12) holds and $d > 0$.

4a. **Cases in which $Q_b = L$ for every b.**

THEOREM 4. *Let d, s_1 be even. Then Q_b has the excluded form L for every integer b in the following cases*:

$$w < 2v, w < 2u; \ w > 2v, u \geqq v; \ w = 2v, u - v > y; \tag{13}$$

which occur only if $32 \mid d$, $16 \mid d$, $128 \mid d$ *respectively. Here we use the notations in* (11), *and also if* $w = 2v$, $s - s_2^2 = k'2^y m$, m *odd*, $y \geqq 0$, *with the convention when* s_0, s_1 *or* $s - s_2^2$ *vanishes, that* v, g, *or* y *is "large."*

Proof. We can write

$$2^w s = 2^{2v}s_2^2 - 2^{u+2+2g}\, s_3^2 k', \quad c = 2^v s_2 - 2^{u+1}k'b, \tag{14}$$

and have that Q_b is not of the form L if and only if

$$2^w s - c^2 \text{ is not of the form } 2^u k'L. \tag{15}$$

CASE (13_1). $w = u + 2 + 2g$ by (14), $s = 2^{2v-w}s_2^2 - k's_3^2$. Hence if $2v - w \geqq 3$, $s \equiv -k' \bmod 8$ and $2^{w+3} \mid c^2$ for every b. If $2v - w = 1$ or 2, $s \equiv 2^{2v-w} - k' \bmod 8$, $2^{-w}c^2 \equiv 2^{2v-w} \pmod 8$ for all b. CASE (13_2). By (14), $u + 2 + 2g = 2v$, u is even, $c = 2^v c'$ with $c' = s_2 - 2^{u+1-v}k'b$ odd; $2^w s = 2^{2v}(s_2^2 - k's_3^2)$, $2^{w-2v}s - c'^2 \equiv -k' \pmod 8$. CASE (13_3). $w = 2v < u + 2 + 2g$, $s - s_2^2 = -2^{u+2+2g-2v}k's_3^2$. Hence $y \equiv u \bmod 2$, $m \equiv 7 \bmod 8$. Thus (15) is again demonstrated, since $u + 2 - v \geqq y + 3$ and

$$s - 2^{-2v}c^2 = k'2^y\{m + 2^{u+2-v-y}s_2 b - 2^{2u+2-2v-y}k'b^2\}. \tag{16}$$

If (13_1) holds, $2u - 1 \geqq u + 2$, $u \geqq 3$. If (13_2) holds, $2u \geqq 2v \geqq u + 2$, $u \geqq 2$. If (13_3) holds, $u - v > y \geqq 1$ and $y = u + 2 + 2g - 2v$; hence $u \geqq 5$.

4b. **Sufficient conditions for solvability of (1) when d is odd.**

THEOREM 5. *Let d be odd. Then* (1) *is solvable when* (12_1) *holds, with*

$$
\begin{aligned}
&q = 2, && \text{if } N\sigma \text{ is odd; or if } N\sigma \equiv 0,\ d \equiv 5 \pmod 8;\\
&q = 4, && \text{if } N\sigma \equiv 4,\ d \equiv 5 \pmod 8;\\
&q = 2^{[w/2]}, && \text{if } N\sigma = 2^w s,\ s \text{ odd},\ w > 0,\ d \equiv 1 \pmod 8.
\end{aligned} \tag{17}
$$

Proof. The numbers $B = (T\sigma - db)/2$ form an arithmetic progression with odd common difference d, so that each residue class mod 2^n occurs once in 2^n consecutive terms. We must assure the existence of a B for which $N\sigma - B^2$ is not of the form dL.

(i) If $N\sigma$ is odd we have $q = 2$. For if $N\sigma \equiv 3$, $N\sigma - O^2 \equiv 2$; if $N\sigma \equiv 1$, $N\sigma - E^2 \equiv 1 \pmod 4$. ($O$, E designate odd and even numbers respectively.)

(ii) If $d \equiv 1 \pmod 8$ and $N\sigma = 2^w s$ (w, s odd), we can take $q = 2^{(w-1)/2}$, and in general not less. For,

$$2^w s - (2^{(w-1)/2}O)^2 = 2^{w-1}(4n+1),\ 2^w s - (2^{(w-1)/2}E)^2 = 2^w O.$$

But if $0 \leqq c < (w-1)/2$, $2^w s - (2^c O)^2 = 2^{2c}(8n-1)$ has the excluded form dL.

(iii) If $d \equiv 1 \pmod 8$ and $N\sigma = 2^{2f+2}s$ (s odd, $f \geqq 0$), we can take $q = 2^{f+1}$. For, $N\sigma - (2^f O)^2 = 2^{2f}(8n+3)$.

(iv) If $d \equiv 5 \pmod 8$ it is elementary that 2 cannot divide $N\sigma$ to an odd exponent. If $N\sigma \equiv 4 \pmod 8$, $N\sigma - O^2$ has the excluded form dL. But one of $4(4n+1) - (2E)^2 = 4(4n+1)$, $4(4n+3) - (2O)^2 = 4(4n+2)$ applies; hence $q = 4$.

(v) If $d \equiv 5 \pmod 8$ and $8 \mid N\sigma$, $N\sigma - O^2 = 8n + 7 \neq dL$; hence $q = 2$.

4c. **Note on discriminants of the form** $8n + 1$.

THEOREM 5′. *If d is positive and $\equiv 1 \pmod 8$ there exist totally positive σ of arbitrarily large norms for which* (1) *is not solvable.*

This is suggested by (17) since q increases with the power of 2 in $N\sigma$, but of course this is no proof. To prove the theorem notice first that if $t_0, \cdots, t_3$ are integers for which F_d is divisible by 8, then $t_0, \cdots, t_3$ are even. Hence if F_d fails to represent one even norm n, it does not represent the infinitely many $4^k n$. It remains then only to prove the following lemma.

LEMMA. *If $d \geqq 17$, $d \equiv 1 \pmod 8$, then there exists between 1 and d an even nonsquare integer of the form $x^2 + x + (1-d)/4$.*

Proof. The condition $0 < x^2 + x + (1-d)/4 < d$ is satisfied if

$$(-1 + d^{1/2})/2 < x < (-1 + (5d)^{1/2})/2,$$

the even squares between 0 and d are $(2z)^2$ where $1 \leqq z < d^{1/2}/2$; and

$$((5d)^{1/2} - d^{1/2})/2 - 1 > d^{1/2}/2 \text{ if } d \geqq 41.$$

We can use $2^2 + 2 - 4$ for $d = 17$, and $4^2 + 4 - 8$ for $d = 33$.

We will examine $d = 17$ in detail. By Theorem 2 we have only to study the norms

represented by F_{17}. By the foregoing we can confine our first attention to norms not divisible by 8; and by Theorem 5, $q = 1$ or 2 for such norms, so that we can assume $N\sigma \leqq 289$. A norm $s_0^2 + s_0 s_1 - 4s_1^2$ is an integer of the form $17n + x^2$ $(x = 0, 1, \cdots, 8)$, and cannot be divisible to an odd exponent by any prime p such that $(17 \mid p) = -1$; the last applies in particular to $p = 3$, 5, and 7. In F_{17} we can take $t_0 = x$ provided n is represented by $t_1^2 + t_2^2 + t_3^2$. We have therefore left to examine $n = -1$ with $x = 5, 6, 7, 8$; $n = -2$ with $x = 6, 7, 8$; $n = -3$ with $x = 8$; and $n = 7$ and 15. It will be found that all the numbers $17 \cdot 7 + x^2$ and $17 \cdot 15 + x^2$ are divisible to an odd exponent by 3, 5, or 7, except for 128, not represented by F_{17}; 144 and 256, obviously represented; $200 = 8^2 + 17 \cdot 8$, $263 = 7^2 + 17 \cdot 11$, $288 = 4^2 + 17 \cdot 16$, $271 = 13^2 + 17 \cdot 6$. Two numbers 15 and 30, obtained for $n = -2$ or -3, are also eliminated. We have thus left to consider only the numbers

$$2^{2z+1}, \text{ 13, 19, and 47,} \tag{18}$$

it being noted that 52, 76, and 188 are represented by F_{17}. The last two statements of the following theorem can be verified without difficulty.

THEOREM 5″. *If $d = 17$, the only totally positive numbers σ for which* (1) *is not solvable are those whose norms are listed in* (18). *Those of norms 2^{2z+1} $(z \geqq 3)$ can be expressed as a sum of five squares in R_{17}. Those of norms* 2, 8, 32, 13, 19, *and* 47 *cannot be expressed as the sum of any number of squares.*

4d. **Sufficient conditions for solvability of** (1) **when d is even.** The cases remaining from Theorem 4 can be formulated as $w \geqq 2u$, $u < v$, $w \neq 2v$; and $w = 2v$, $u - v \leqq y$. Hence they can be reformulated thus: $w \geqq 2u$, $u < v$; and $w = 2v$, $0 \leqq u - v \leqq y$. It will be noted in the following theorem that q is unbounded with the power of 2 in $N\sigma$ when the odd part of d has the form $8n + 1$. In all other cases there is a constant c such that (cf.(12)) (1) is solvable if $N\sigma \geqq cd^2$, σ being totally positive and s_1 even. The largest such c, given by $q = 5$, is 25/16. The notations of Theorem 4 are still used in Theorem 6.

THEOREM 6. *Assume d even, s_1 even. We can take q as follows:*

1°. *If* $w = 2u + 2f$ $(f \geqq 0)$ *and* $u < v$, *then* $q = 2$ *except that*
$q = 2^{f-2}$ *if u is even*, $k' \equiv 1 \pmod 8$, $f > 2$; $q = 4$ *if* $f = 1$, u *even*,
$s \equiv -k' \equiv 1 \pmod 4$, *or if* $f = 2$, u *even*, $k' \equiv 5 \pmod 8$.

2°. *If* $w = 2u + 1 + 2f$ $(f \geqq 0)$ *and* $u < v$, *then* $q = 2$ *except that*
$q = 2^{f-1}$ *if* $k' \equiv 1 \pmod 8$, u *even*, $f \geqq 1$;
$q = 1$ *if* $k' \equiv 1 + 2s$ *or* $5 \pmod 8$, u *even*, $f \geqq 1$.

3°. *If* $0 \leqq u - v \leqq y$, $w = 2v$, $s - s_2^2 = k'2^y m$ *(hence* $m \equiv 7 \bmod 8$, $y - u$ *even), then*
$q = 2$ *if* $u - v = y$; *or* $u - v < y - 1$, v odd, $u > v$; *or* $u - v = y - 1$, $y > 1$;
$q = 3$ *if* $u = v$ *and* $y = 1$; *or* $u - v < y - 1$ *and v is even*;
$q = 5$ *if v is odd*, $u = v$ *and* $y > 1$.

Proof. In 1° and 2°, $c = 2^{u+1}c'$, where $c' = 2^{v-u-1}s - k'b$ runs over an arithmetic progression with odd common difference k'. We are to choose b so that

$$2^w s - 2^{2u+2}c'^2 \not\equiv 2^u k'L.$$

If $w = 2u$ or $2u+1$ this becomes

$$s - 2^{2u+2-w}c'^2 \not\equiv 2^{u-w}k'L. \tag{19}$$

Since $w < 2v$, $w = u + 2 + 2g$, so that $u - w$ is even. Also,

$$s = -k's_3^2 + 2^{2v-w}s_2^2 \equiv -k' \text{ or } -k' + 2^{2v-w} \pmod 8.$$

Hence (19) holds only by choice of parity of c', whence $q = 2$.

If $w = 2u + 2f$, $f \geqq 1$, we must secure

$$2^{2f-2}s - c'^2 \not\equiv 2^{-u}k'L.$$

Consider $f = 1$. One of c' odd or even will serve (hence $q = 2$) if u is odd; or u is even, $s \equiv 3 \pmod 4$; or u is even, $s \equiv k' \equiv 1 \pmod 4$. But if u is even and $s \equiv -k' \equiv 1 \pmod 4$, we take $q = 4$, using $s - (2n)^2$ (n odd or even).

Consider $f > 1$. We can use $c' = 2^{f-2}O$ if u is odd or $k' \not\equiv 5 \pmod 8$; $2^{f-1}O$ if u is even and $s \equiv 3 \pmod 4$; $2^{f-1}E$ if u is odd or $s \equiv k' \equiv 1 \pmod 4$; 2^rO ($0 \leqq r \leqq f-3$) if u is odd or $k' \not\equiv 1 \pmod 8$. Hence $q = 2$ if u is odd; or $f = 2$, $k' \not\equiv 5 \pmod 8$; or $k' \equiv 3 \pmod 4$; or u even, $k' \equiv 5 \pmod 8$, $f > 2$. But $q = 2^{f-2}$ if u is even, $k' \equiv 1 \pmod 8$, $f > 2$; $q = 4$ if u is even, $k' \equiv 5 \pmod 8$, $f = 2$.

If $w = 2u + 2f + 1$ ($f \geqq 1$), we must secure $2^{2f-1}s - c'^2 \not\equiv 2^{-u}k'L$. We can use $c' = 2^{f-1}O$ if u is odd or $k' \not\equiv 2s - 1 \pmod 8$; $c' = 2^{f-1}E$ if u is even; $c' = 2^rO$ ($0 \leqq r \leqq f-2$) if $k' \not\equiv 1 \pmod 8$ or u is odd. Hence $q = 1$ if u is even and $k' \equiv 1 + 2s$ or $5 \pmod 8$; $q = 2$ if u is odd or $k' \equiv 1 - 2s \pmod 8$; $q = 2^{f-1}$ if $k' \equiv 1 \pmod 8$, u even.

Consider $w = 2v$, $u \geqq v$. Then $w < u + 2 + 2g$ and $y = u + 2 + 2g - 2v$, $m \equiv 7 \pmod 8$. We can use (16), with now $u - v \leqq y$. If $u - v = y$, b odd will serve, hence $q = 2$. If $u - v = y - 1$, $7 + 2b - 2^y k'b^2$ is not of the form L if b is odd, unless $y = 1$; and in the last case, $b \equiv 2$ and one of $b \equiv 1, 3 \pmod 4$ will do, so that $q = 3$. If $u - v < y - 1$, then for all values of b, $2^{u+2-v} \mid s - c_b^2$, where $c_b = s_2 - 2^{u+1-v}k'b$. We can suppose then that for a certain b, Q_b is of the form L, and hence $s - c_b^2 = k'2^z(8n+7)$, $z \equiv u \pmod 2$, $u + 2 - v \leqq z$. Then, trying $b + 1$, we consider

$$s - (c_b - 2^{u+1-v}k')^2 = k'2^{u-v+2}\{2^{z-u+v-2}(8n+7) + c_b - 2^{u-v}k'\}.$$

Thus Q_{b+1} is not of the form L if v is odd and $u > v$; hence $q = 2$. If v is even, $q = 3$, since $s - (c_b - 2^{u+1-v}2k')^2$ is not of the excluded form, being equal to

$$\begin{aligned} &k'2^{u-v+3}\{2^{z-u+v-3}(8n+7) + c_b - 2^{u-v+1}k'\} && \text{if } z > u - v + 2, \\ &k'2^{u-v+2}\{8n + 7 + 2c_b - 2^{u-v+2}k'\} && \text{if } z = u - v + 2. \end{aligned}$$

Finally, if v is odd and $u = v$, $q = 5$ is obtainable, as we can use

$$s - (c_b - 2^{u-v+1}4k')^2 = 8k'(8n + 7 + 2c_b - 8k') \quad \text{if } z = 3,$$
$$= 16k'(2^{z-4}(8n + 7) + c_b - 4k') \quad \text{if } z > 4.$$

4e. **Lists for some discriminants, of all totally positive numbers τ, with s_1 even if d is even, for which (1) is not solvable.** These lists form a small part of the unpublished output of [1]; the proof that the lists are complete is easily given using the foregoing theorems. By Theorem 2 it suffices to list the norms when d or $\frac{1}{4}d$ is a prime. In other cases, noting that σ and $\sigma\theta^2$ behave alike (θ denoting a unit in R_d), we list one σ from each such equivalence class. Notice the example, when $d = 24$, of two numbers (1 and $5 + 2\omega$) of the same norm, one of which is, the other not, a sum of four squares. In view of the theorem [6; 7] that if σ is not a sum of five or fewer squares, then σ cannot be expressed as a sum of any number of squares, it is interesting to give the cases in the following lists in which σ is a sum of five squares: norm 92 when $d = 13$; norms 281 and 284 when $d = 40$; norms 308 (both $22 + 4\omega$ and $88 + 26\omega$) and 317 when $d = 44$. The largest observed ratio $N\sigma: d^2$ for which σ was not a sum of four squares was for $\sigma = 74 + 26\omega$ with $d = 29$, where $N\sigma/d^2$ was 2668/841.

$d = 13$: norms 3, 12, 23, 92. $d = 24$: $5 + 2\omega$ of norm 1, $6 + 2\omega$ of norm 12.

$d = 28$: norms 8 and 21. $d = 44$: norms 5, 20, 37, 56, 77, 308, 317.

$d = 40$: $7 + 2\omega$, $8 + 2\omega$, $9 + 2\omega$, $10 + 2\omega$, $18 + 2\omega$, $21 + 4\omega$, of respective norms 9, 24, 41, 60, 284, and 281.

PART II

Formulae for the number of solutions of (1) when $d = 5, 8, 12$.

5. **Formulae for the number of representations of $n = N\sigma$ by F_d.** Since the discriminant of F_d is not a square, the weighted number of representations of a positive integer n by the genus of F_d is not a factorable function of n. It is interesting then that this weighted number of representations becomes factorable, in the cases $d = 5, 8, 12$ (and perhaps more generally), if n is restricted to the set of numbers represented by the principal *binary* form of discriminant d. (These numbers, of course, from a multiplicative semigroup.)

If $d = 5$, $N\sigma$ can be given the notation

$$n = s_0^2 + s_0 s_1 - s_1^2 = 2^{2u}5^v m; \; u, v \geqq 0; \; m \equiv 1 \text{ or } 9 \pmod{10}. \tag{20}$$

A classical formula [4] for the number of representations of $2^a5^b m$ by F_5 is $k_2 k_5 k_m$, where

$$k_2 = (2^{a+1} - (-1)^a 5)/3, \quad k_5 = 5^b + (-1)^a \left(m \,|\, 5\right), \quad k_m = \sum_{m=qq'} \left(q' \,|\, 5\right) q. \tag{21}$$

Notice that k_5 depends on the factors other than 5 in n, so that the formula is not factorable. But if n is a norm (as in (20)), the formula reduces to $2g(2^{2u}5^v m)$,

where $g(n)$ is the factorable function defined for every positive integer n as follows:

$$g(1) = 1,\ g(n_1 n_2) = g(n_1)g(n_2) \text{ if } (n_1, n_2) = 1; \tag{22}$$

$$g(2^{2u}) = |2^{2u+1} - 5|/3,\ g(2^{2u+1}) = 0,\ g(5^v) = (5^v + 1)/2, \tag{23}$$

$$g(m) = \sum_{m = qq'} (q' \mid 5)q. \tag{24}$$

If $d = 8$, $N\sigma$ can be given the notation

$$n = s_0^2 - 8s_3^2 = 2^u m, \text{ where } u = 0, m \equiv 1 \pmod 8, \text{ or } u \geqq 2, m \equiv \pm 1 \pmod 8. \tag{25}$$

The formula [4] for the number of representations of n by F_8 reduces when n is a norm to $2g(n)$, where $g(n)$ can be defined for all positive integers n by (22) and

$$g(2^u) = 2^{u-1} - 1 \text{ if } u \geqq 1;\ g(m) = \sum_{m = qq'} (2 \mid q')q. \tag{26}$$

If $d = 12$, the genus of F_{12} consists of two classes, that of F_{12} and that of

$$F''_{12} = 4t_0^2 + 3(3t_1^2 + 3t_2^2 + 3t_3^2 - 2t_2t_3 - 2t_3t_1 - 2t_1t_2). \tag{27}$$

Since F_{12} and F''_{12} have the same number of unimodular automorphs, classical methods yields a formula not unlike that for F_5, for $F_1(n) + F_2(n)$, where $F_1(n)$ and $F_2(n)$ denote the number of representations of n by F_{12} and F''_{12} respectively. If n is a norm and positive, we can write

$$\begin{aligned} n &= s_0^2 - 12s_3^2 = 2^u 3^v m, \text{ where } u = 0 \text{ or } u \geqq 2,\ v \geqq 0, \text{ and} \\ m &\equiv 1 \pmod{12} \text{ if } u + v \text{ is even, } m \equiv -1 \pmod{12} \text{ if } u + v \text{ is odd.} \end{aligned} \tag{28}$$

It can be shown for n a positive norm that $F_1(n) + F_2(n) = 2g(n)$, where $g(n)$ is the factorable function defined for all positive integers n (whether norms or not) by (22) and

$$g(2^u) = |2^u - 2| (u \geqq 0),\ g(3^v) = (3^v + 1)/2, \tag{29}$$

$$g(m) = \sum_{m = qq'} (2 \mid q')q. \tag{30}$$

In §10 we will prove

THEOREM 7. *$F_1(n) = F_2(n)$ if n is even, or if n is divisible to an odd exponent by 3 or by any prime p such that $p \equiv -1 \pmod{12}$.*

By a familiar argument in elementary number theory, if $g(n)$ is a factorable function, and $g'(n)$ is the factorable function defined by $g'(p^a) = g(p^a) - g(p^{a-2})$ if $a \geqq 2$, $g'(p^a) = g(p^a)$ if $a = 0$ or 1, then $g(n) = \sum g'(n/q^2)$, summed over the square factors q^2 of n. From this remark readily follows

THEOREM 8. *If D is a divisor of n, the number of solutions of*

$$n = t_0^2 + d(t_1^2 + t_2^2 + t_3^2),\ (t_0, t_1, t_2, t_3, D) = h', \tag{31}$$

is $2g_{D/h'}(n/h'^2)$ *if* $d = 5$ *or* 8; *but* $g_{D/h'}(n/h'^2)$ *if* $d = 12$ *and* $F_1(n/h'^2) = F_2(n/h'^2)$. *Here* $g_k(n)$ *is the "simultaneously factorable" function defined for positive integers* n, *and factors* k *of* n *as follows. If* $n = n_1n_2$ *with* $(n_1, n_2) = 1$, *we can write* $k = k_1k_2$, *where* k_1 *divides* n_1 *and* k_2 *divides* n_2, *and require that*

$$g_k(n) = g_{k_1}(n_1)\,g_{k_2}(n_2), \tag{32}$$

if $n = p^a$ *and* $k = p^b$ $(0 \leqq b \leqq a)$,

then $g_k(n) = g(p^a)$ *if* $a = 0$ *or* 1, *or* $b = 0$, (33)

$$g_k(n) = g(p^a) - g(p^{a-2}) \text{ if } a \geqq 2 \text{ and } b > 0.$$

6. **Discussion of h and l when $d = 5$.** To obtain $r_4(\sigma, 5)$ by (6), we must, for each solution $t_0, \cdots, t_3$ of (7) for which $b = (2s_0 + s_1 - 2t_0)/5$ is an integer, construct $r_4(lh)$ and evaluate the sum of the numbers $r_4(lh)$. Here $h = (t_1, t_2, t_3, e)$, where $e = (s_0, (s_1 - b)/2, b)$; and $l = 2$ if the power of 2 in $b - s_1$ does not exceed that in (s_0, b), otherwise $l = 1$. Since $r_4(2h) = r_4(h)$ when h is even, the value of l need only be considered when h is odd.

Inserting the components of e, and noting by (7) that the g.c.d. of s_0, s_1, t_1, t_2, t_3 must divide t_0, we have

$$\begin{aligned} h &= (t_1, t_2, t_3, s_0, (2s_0 + s_1 - 2t_0)/5, (s_0 - 2s_1 - t_0)/5) \\ &= (t_1, t_2, t_3, s_0, s_1, (s_0 - 2s_1 - t_0)/5) \\ &= (t_0, t_1, t_2, t_3, s_0, s_1, (s_0 - 2s_1 - t_0)/5), \\ h &= (t_0, t_1, t_2, t_3, s_0, s_1, (2s_0 + s_1 - 2t_0)/5). \end{aligned} \tag{34}$$

We must determine whether $h = h'$ or $h'/5$, *where*

$$h' = (t_0, t_1, t_2, t_3, s_0, s_1). \tag{35}$$

Evidently, $h = h'$ if either (t_0, t_1, t_2, t_3) is prime to 5, or $v < 2$ (in (20)), since in the last case $D = (s_0, s_1)$ is prime to 5. Hence, if 5^y denotes the power of 5 in (t_0, t_1, t_2, t_3), we can suppose $v \geqq 2$, $y > 0$, that is $0 < 2y \leqq v$.

If $y < v/2$, then $5^{y+1} \mid t_0$. Notice from

$$(2s_0 + s_1)^2 - 5s_1^2 = 2^{2u+2}5^v m$$

that if v is even, $5^v \parallel (2s_0 + s_1)^2$ and $5^v \mid s_1^2$; and if v is odd, $5^{v+1} \mid (2s_0 + s_1)^2$ and $5^{v-1} \parallel s_1^2$. Hence if $y < v/2$, $5^{y+1} \mid (2s_0 + s_1 - 2t_0)$, and so $h = h'$.

But if $y = v/2 > 0$, then $(2s_0 + s_1)^2 - (2t_0)^2$ is divisible by 5^{2y+1}, hence one of $2s_0 + s_1 + 2t_0$ and $2s_0 + s_1 - 2t_0$ is divisible by 5^{y+1}, the other by 5^y (but not by 5^{y+1}, since 5^{y+1} does not divide t_0). Hence

$$h = h' \text{ for one sign of } t_0,\ h = h'/5 \text{ for the other.} \tag{36}$$

If $u = 0$, $l = 1$. For s_0 or b is odd.

If $u = 1$, then $s_0, s_1, t_0, t_1, t_2, t_3$ must be even, and it is immaterial whether l is 1 or 2. If $u \geqq 2$ and $t_0, \cdots, t_3$ are odd, then $l = 2$, since $s_0 \equiv s_1 \equiv 0$, $b \equiv 2 \pmod 4$.

7. **The formula for** $r_4(\sigma, 5)$. We can now reformulate (6) in terms of h' rather than h. If h' is any divisor of $D = (s_0, s_1)$, then the condition that $(t_0, t_1, t_2, t_3, s_0, s_1) = h'$ means, on setting $t_i = h'u_i$, that $u_0, \cdots, u_3$ are solutions of (31), with n replaced by n/h'^2 and $k = D/h'$. Let $\zeta(q)$ denote the sum of the divisors of q. Now $r_4(lh)$ is the product of the numbers $\zeta(p^r)$ (p^r ranging over the prime-powers in h), times 8 or 24 according as lh is odd or even. To compensate for the case of (36) we can use in place of $\zeta(5^r)$ (where $5^r \| h'$) the factor $(\zeta(5^r) + \zeta(5^{r-1}))/2$. Thus:

$$r_4(\sigma, 5) = 8\varepsilon \sum_{h' \mid D} g_{D/h'}(n/h'^2)\psi_n(h'), \tag{37}$$

where $\varepsilon = 1$ if $v = 0$, $\varepsilon = 2$ if $v > 0$; and $\psi_n(h')$ is the factorable function defined as follows:

$$\begin{aligned}
\psi_n(2^r) &= 1 \text{ if } r = 0;\\
&= 3 \text{ if } r > 0;\\
\psi_n(5^r) &= (\zeta(5^r) + \zeta(5^{r-1}))/2, \quad \text{if } v\ (\geqq 2) \text{ is even and } r = v/2; \qquad (38)\\
&= \zeta(5^r) \text{ otherwise};\\
\psi_n(p^r) &= \zeta(p^r), \text{ for all odd primes different from 5.}
\end{aligned}$$

For any prime p, let p^a denote the power of p in $D = (s_0, s_1)$, and let p^{2a+b} denote the power of p in $n = N\sigma$. Then by the multiplicative properties of $g_k(q)$ and $\psi_n(h')$, $r_4(\sigma, 5)/(8\varepsilon)$ is the product for all p of

$$c_p = \sum_{r=0}^{a} g_{p^{a-r}}(p^{2a+b-2r})\psi_n(p^r). \tag{39}$$

The evaluation of c_p is straightforward, and gives the following results: If p is an odd prime different from 5, and $w = (5 \mid p)$,

$$c_p = \frac{p^{a+b+1} - w^{b+1}}{p - w} \cdot \frac{p^{a+1} - 1}{p - 1}. \tag{40}$$

If $p = 5$, then $v = 2a + b$, and, in all cases,

$$\varepsilon c_5 = (5^{v+1} - 1)/4. \tag{41}$$

If $p = 2$, then $a = u$ and $b = 0$, and, in all cases,

$$c_2 = 1 \text{ if } u = 0, \quad c_2 = 2^{2u+1} - 5 \text{ if } u > 0. \tag{42}$$

8. **Discussion of** h **and** l **when** $d = 8$. We use the notations in (25)–(26). Note that $b = (s_0 - t_0)/4$ is integral only by choice of sign of t_0 if $u = 0$, and is always integral if $u > 0$. Also, $e = (s_0, s_3, b)$, and $h = (t_1, t_2, t_3, e)$, hence

(43) $$h = (t_0, t_1, t_2, t_3, s_0, s_3, (s_0 - t_0)/4).$$

We choose $h' = (t_0, t_1, t_2, t_3, s_0, s_3)$. To construct a formula similar to (37), we must try to define $\psi_n(h')$ in connection with $r_4(lh)$ in such a manner that it compensates for the cases where h' and lh have different parities.

A curious situation appears when $u = 2$. Then $t_0 \equiv s_0 \equiv 2 \pmod 4$. If $m \equiv 1 \pmod 8$, s_3 is even, t_1, t_2, t_3 are even: hence h' is double-odd, while h is odd or double-odd according to the sign of t_0; but $l = 1$ since s_2 contains no higher power of 2 than s_3. If $m \equiv -1 \pmod 8$, s_3 is odd, and $h = h'$ (both odd); since $(s_0 - t_0)/4$ changes parity with the sign of t_0, l alternates between 1 and 2 with that sign. In both cases the exponent of 2 in h' is unique for all solutions of (7). To keep $\psi_n(h')$ factorable we can define $\psi_n(2^r) = 1$ $(r \geqq 0)$ when $u = 2$, and can compensate both for the present phenomenon and for the need to make b integral, by defining

(44) $\varepsilon = 1$ if n is odd; $\varepsilon = 4$ if $n \equiv 4 \pmod 8$, $\varepsilon = 2$ if $n \equiv 0 \pmod 8$.

We will prove for $u > 2$ that $h' \equiv lh \pmod 2$. First let $2^3 \parallel N\sigma$. Then s_3 is odd, hence h and h' are odd. Also $l = 2$ leads to a contradiction: then $(s_0 - t_0)/4$ is even, hence since 4 divides s_0 and t_0,

$$8(t_1^2 + t_2^2 + t_3^2) \equiv s_0^2 - t_0^2 - 8s_3^2 \equiv -8 \pmod{64}.$$

Second, if $16 \mid N\sigma$, then either $s_0 \equiv t_0 \equiv 0$ or $4 \pmod 8$, hence h and h' are even; or $s_0 \equiv t_0 + 4 \equiv 0$ or $4 \pmod 8$, hence $\pm 2 \equiv s_3^2 + t_1^2 + t_2^2 + t_3^2 \pmod 8$, hence h and h' are odd and $l = 1$.

9. **The formula for** $r_4(\sigma, 8)$. In much the same way as in §1, we have

(45) $$r_4(\sigma, 8) = 8\varepsilon \sum_{h' \mid D} g_{D/h'}(n/h'^2)\psi_n(h') = 8\varepsilon c_2 \prod_{p \text{ odd}} c_p,$$

where $D = (s_0, s_3)$, $n = N\sigma$, ε is defined in (44), ψ_n is the factorable function such that $\psi_n(p^r) = \zeta(p^r)$ for odd primes p, $\psi_n(2^r) = 1$ if $8 \nmid n$, and

(46) $$\psi_n(2^r) = 1 \text{ or } 3 \text{ according as } r = 0 \text{ or } r > 0, \text{ if } 8 \mid n.$$

The evaluation of the factors c_p is straightforward: c_p is given by (40) with $w = (2 \mid p)$ if p is any odd prime, and εc_2 has the value

(47) $$1 \text{ if } u = 0; \quad 4 \text{ if } u = 2; \quad 6(2^{u-2} - 1) \text{ if } u > 2.$$

10. **Discussion of** h **and** l **when** $d = 12$. We use (28), $e = (s_0, s_3, j)$, where $f = (s_0 - t_0)/6$, $le = (s_0, 2s_3, j)$,

(48) $$h = (h', j), \text{ where } h' = (t_0, \cdots, t_3, s_0, s_3).$$

The integrality of j depends on the sign of t_0 if $(n, 3) = 1$.

We prove for n odd that $h = h'$ and $l = 1$. For, since s_0 is odd, h' and h are odd, and $l = 1$. If $(n, 3) = 1$, s_0, h', and h are prime to 3, hence $h = h'$. If $3 \mid n$,

we assume (cf. Theorem 7) that v is odd. Let $3^b \| (t_0, \cdots, t_3)$. Then $2b+1 \leqq v$, $3^b \mid (s_0, s_3)$, $3^{b+1} \mid s_0$, $3^{2b+1} \mid t_0^2$, $3^{b+1} \mid t_0$, $3^b \mid j$, $h = h'$.

Case n even. We can set $s_0 = 2s_2$, $t_0 = 2t_0''$, and have $j = (s_2 - t_0'')/3$,

$$2^{u-2}3^v m = s_2^2 - 3s_3^2 = t_0''^2 + 3(t_1^2 + t_2^2 + t_3^2). \tag{49}$$

Denote by 2^a, 3^b the powers of 2 and 3 in (t_0, t_1, t_2, t_3). If $2^{a-1} \| t_0''$, then $u = 2a$, $s_2 = 2^{a-1}3^b s_4$, $s_3 = 2^{a-1}3^b s_5$, and $s_4^2 - 3s_5^2$ is odd. If $2^a \mid t_0''$, $u \geqq 2a+2$, $s_2 = 2^a 3^b s_4$, $s_3 = 2^a 3^b s_5$. Also, $v \geqq 2b$; and if $v = 2b$, $(s_4, 3) = 1$.

We prove that h and h' contain the same power of 2. Indeed, if s_5 is odd, the power of 2 in s_3 divides both s_2 and t_0''. If s_5 is even, then if $2^a \mid t_0''$, $2^a \mid j$; and if $2^{a-1} \| t_0''$, $3j = 2^{a-1}(\text{odd}) - 2^{a-1}(\text{odd}) \equiv 0 \pmod{2^a}$.

We prove next that h is odd and $l = 2$ if and only if

$$s_2 \text{ even}, \quad s_3 \text{ odd}, \quad (t_0, t_1, t_2, t_3) \text{ odd}. \tag{50}$$

For if h is odd, s_3 or (t_1, t_2, t_3) is odd. By (49), s_3 even and j even imply that $4 \mid (t_1, t_2, t_3)$. Hence if h is odd and s_3 is even, j is odd and $l = 1$. Thus, if h is odd and $l = 2$, then j must be even; also, s_2 must be even, since otherwise (49) implies $t_1^2 + t_2^2 + t_3^2 \equiv -1 \pmod 8$. Finally, notice that if s_2 is even and s_3 is odd, then j is even (hence $l = 2$) if and only if (t_1, t_2, t_3) is odd.

We prove finally that $h = h'$ except that when v is even and positive, and $3^{v/2} \| (t_0, t_1, t_2, t_3)$, then $h = h'$ for one sign of t_0, $h = h'/3$ for the other. First, if $v = 0$, h' is prime to 3, hence $h = h'$. If $v > 0$, (49) can be divided by the powers of 2 and 3 dividing (t_0'', t_1, t_2, t_3), and gives

$$s_4^2 - t_0'^2 = 3 \text{ times an integer}. \tag{51}$$

If here $v > 2b$, then $3 \mid (s_4, t_0')$ and $h = h'$. But if $v = 2b, (s_4, 3) = 1$, hence only one of $s_4 + t_0'$ and $s_4 - t_0'$ is divisible by 3, and $h = h'$ or $h'/3$ correspondingly.

11. **Proof of Theorem 7; evaluation of $r_4(\sigma, 12)$ in certain cases.** To compensate for the final result of §10 is easy: simply define

$$\begin{aligned} \psi_n(3^b) &= \zeta(3^b) && \text{if } 2b < v \text{ or } b = 0, \\ &= (\zeta(3^b) + \zeta(3^{b-1}))/2 && \text{if } 2b = v > 0. \end{aligned} \tag{52}$$

If $p > 3$, we let $\psi_n(p^b) = \zeta(p^b)$. And if $p = 2$, we let $\psi_n(2^b) = 1$ if $b = 0$, $\psi_n(2^b) = 3$ if $b > 0$. This does not represent the needs of the case $u = 2$ (cf. (50)), but this case will be handled separately below.

We proceed with the proof of Theorem 7, and refer to the paragraph of (27).

LEMMA 1. *If $n = 4q$, q integral, then $F_1(n) = F_2(n)$.*

Proof. $4q = t_0^2 + 12(t_1^2 + t_2^2 + t_3^2)$ reduces to $q = t_0''^2 + 3(t_1^2 + t_2^2 + t_3^2)$. In (27), $3t_1^2 + \cdots - 2t_1t_2 - \cdots = (t_2 + t_3 - t_1)^2 + \cdots + (t_1 + t_2 - t_3)^2$. Now 4 divides a sum of three squares only if they are even. Finally,

$$t_2 + t_3 - t_1 = 2x_1, \cdots, t_1 + t_2 - t_3 = 2x_3,$$

gives $t_1 = x_2 + x_3, \cdots, t_3 = x_1 + x_2$, and replaces $\frac{1}{4}F''_{12}$ *by* $t_0^2 + 3(x_1^2 + x_2^2 + x_3^2)$.

Besides multiples of 4, F_{12} and F''_{12} represent only odd numbers of the form $4q + 1$. Consider now the equation

$$4q + 1 = t_0''^2 + 3(t_1^2 + t_2^2 + t_3^2). \tag{53}$$

LEMMA 2. *There is a one-to-one association between the solutions of* (53) *with* t_0'' *respectively odd and even, and the representations of* $4q + 1$ *by* F_{12} *and* F''_{12}.

Proof. *If* t_0'' is odd, $t_1\, t_2, t_3$ are even. If t_0'' is even, then t_1, t_2, t_3 are odd and integers u_j can be chosen so that $u_2 + u_3 - u_1 = t_1, \cdots, u_1 + u_2 - u_3 = t_3$.

Some comments will now be made on the cases $N\sigma$ odd or quadruple-odd.

In formulae (54)–(57), σ will designate a number $s_0 + 2s_3\omega$ with s_0 odd; σ', one with s_0 divisible by 4 and s_3 odd; σ'', one with s_0 double-odd, s_3 even. The odd part of the divisor (s_0, s_3) will be assumed to be the same for all three. If we wish, we can take $\sigma'' = 2\sigma$, $\sigma' = 2\theta\sigma$, where θ is the unit $2 + 3^{1/2}$; $N\sigma = k$, $N\sigma' = N\sigma'' = 4k$, $k = 4q + 1$.

Let $D = (s_0, s_3)$, $k = 4q + 1$, and for any divisor j of D, let $F_{i,j}(k/j^2)$ denote the number of solutions of (53) with $t_0'' \equiv i \pmod 2$, $(2t_0'', t_1, t_2, t_3, D) = j$.

Since $N\sigma = k$ is odd, the factors of D are odd, $l = 1$, and hence

$$r_4(\sigma, 12) = 4\varepsilon \sum_{j \mid D} F_{1,j}(k/j^2) \cdot \psi_k(j), \tag{54}$$

with $\varepsilon = 1$ or 2 according as k is or is not prime to 3.

Consider now σ'. In deriving (50) we noticed that h' is odd, and that $l = 2$ if t_0'' is even (corresponding, we now recognize, to a representation of k by F''_{12}), and $l = 1$ if t_0'' is odd (corresponding to a representation of k by F'_{12}). Accordingly,

$$r_4(\sigma', 12) = 4\varepsilon \sum_{j \mid D} \{3F_{1,j}(k/j^2) + F_{0,j}(k/j^2)\} \cdot \psi_n(j). \tag{55}$$

In the case of σ'', h' odd means that (t_1, t_2, t_3) is odd, corresponding to a representation of k by F''_{12}. And h' even means t_1, t_2, t_3 even, corresponding to a representation of k by F_{12}. Hence:

$$r_4(\sigma'', 12) = 4\varepsilon \sum_{j \mid D} \{F_{1,j}(k/j^2) + 3F_{0,j}(k/j^2)\}\psi_n(j). \tag{56}$$

Since k is odd, a simplifying expression for $F_{i,j}(k/j^2)$ is not in general available. However, since as noted following (28), $F_2(n) + F_1(n) = 2g(n)$, we have $F_{0,j}(k/j^2) + F_{1,j}(k/j^2) = 2g_{D/j}(k/j^2)$, and hence

$$\{r_4(\sigma',12)+2r_4(\sigma,12)\}/3 = r_4(\sigma'',12) - 2r_4(\sigma,12)$$

$$= 4\varepsilon \sum_{j \mid D} \{F_{0,j}(k/j^2)+F_{1,j}(k/j^2)\}\psi_k(j)$$

$$= 8\varepsilon \sum_{j \mid D} g_{D/j}(k/j^2)\psi_k(j) \tag{57}$$

$$= 8\varepsilon \prod_{p \text{ odd}} c_p,$$

where c_p is given by (40) with $w = (3 \mid p)$ if $p > 3$, and $c_3 = (3^{v+1}-1)/2$ if $3^v \parallel k$. From (57) also follows that $r_4(\sigma',12) + r_4(\sigma'',12) = 32\varepsilon \prod c_p$.

Let $G_i(n)$ denote the number of solutions of

$$n = 3x_0^2 + x_1^2 + x_2^2 + x_3^2, x_0 \equiv i \pmod 2, \tag{58}$$

$(i = 1,2)$. Clearly $F_i(3n) = G_i(n)$ for any integer n.

LEMMA 3. *If* $n \equiv 5 \pmod 6$, $G_2(n) = G_1(n)$.

Proof. In (58), two of x_1, x_2, x_3 are prime to 3, hence exactly half the solutions satisfy $3 \mid x_1 + x_2 + x_3$. The self-inverse substitution

$$y_0 = (x_1 + x_2 + x_3)/3,\ y_1 = x_0 + (2x_1 - x_2 - x_3)/3, \cdots, \cdots, \tag{59}$$

under which $3x_0^2 + \sum x_j^2 = 3y_0^2 + \sum y_j^2$, carries x_0 into y_0 of the opposite parity.

LEMMA 4. *If* n *is odd, and* $\phi(n)$ *denotes the number of solutions of*

$$n = y_0^2 + y_1^2 + 2y_2^2 + 2y_2y_3 + 2y_3^2, \tag{60}$$

then

$$G_i(3n) + 3F_i(n) = 2\phi(n) \quad (i = 1,2), \tag{61}$$

hence

$$F_2(9n) + 3F_2(n) = F_1(9n) + 3F_1(n).$$

Proof. In $3n = 3x_0^2 + x_1^2 + x_2^2 + x_3^2$, either $x_3 \equiv \pm x_1 \equiv \pm x_2 \pmod 3$ for exactly one of the four combinations of signs, or 3 divides (x_1, x_2, x_3). The discussion for $x_1 \equiv -x_2 \equiv x_3$ will be typical. Then $x_0 = u_0$, $x_1 = u_1$, $x_2 = 3u_2 - u_1$, $x_3 = 3u_3 + u_1$, $3n = 3u_0^2 + 3u_1^2 + 9u_2^2 - 6u_1u_2 + 9u_3^2 + 6u_1u_3$, or

$$n = u_0^2 + (u_1 - u_2 - u_3)^2 + 2u_2^2 + 2u_2u_3 + 2u_3^2.$$

Thus $G_i(3n) = F_i(n) + 4\{\phi_i(n) - F_i(n)\}$ $(i = 1,2)$, where $\phi_i(n)$ denotes the number of solutions of (60) with $y_0 \equiv i \pmod 2$. But since n is odd, y_0 is odd or even equally often in (60), $2\phi_i(n) = \phi(n)$.

COROLLARY. $F_2(k) = F_1(k)$ *if* $k = 3^h m$ $(m \equiv 5 \bmod 6, h > 0)$, *hence if* k *is a norm divisible by* 3 *to an odd exponent.*

Proof. If $n \equiv 2 \pmod 3$, Lemma 3 shows that $F_2(3n) = F_1(3n)$, and hence by (61), $F_2(3^{2h+1}n) = F_1(3^{2h+1}n)$ $(n \equiv 5 \mod 6,\ h \geqq 0)$. Also, by (61), since $F_2(n) = F_1(n) = 0$ if $n \equiv 2 \pmod 3$, also $F_2(3^{2h+2}n) = F_1(3^{2h+2}n)$ if $n \equiv 5 \pmod 6$ and $h \geqq 0$.

LEMMA 5. *Let p denote an odd prime such that $(3|p) = 1$. There are $p - (-1|p)$ matrices R of determinant $v \pmod p$ which satisfy $R'ER \equiv -3I \pmod p$, where*

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ and } R \text{ can be designated as } \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{62}$$

and where v denotes a fixed solution of $v^2 \equiv 3 \pmod p$. Consider the $p-(-1|p)$ formulae

$$x_0 \equiv ax_2 + bx_3,\ x_1 \equiv cx_2 + dx_3 \pmod p. \tag{63}$$

Trivially, if $x_2 = x_3 = 0$, (63) gives the null solution $x_0 = x_1 = x_2 = x_3 = 0$ of

$$x_0^2 + 3x_1^2 + 3x_2^2 + 3x_3^2 \equiv 0 \pmod p. \tag{64}$$

As x_2, x_3 range over the $p^2 - 1$ pairs not 0, 0, the $p - (-1|p)$ formulae (63) give distinct solutions of (64). Every solution of (64) is so given if $p \equiv 3 \pmod 4$. But if $p \equiv 1 \pmod 4$, there are exactly $2(p^2 - 1)$ additional non-null solutions of (64) which satisfy

$$x_0 \equiv uvx_1,\ x_2 \equiv ux_3 \pmod p, \text{ where } u^2 \equiv -1 \pmod p. \tag{63'}$$

Proof. First notice that (63) and (63') do provide solutions of (64). For example, $R'ER \equiv -3I \pmod p$ expands into

$$a^2 + 3c^2 \equiv -3,\ b^2 + 3d^2 \equiv -3,\ ab + 3cd \equiv 0 \pmod p. \tag{65}$$

Notice also that $|R|^2 \equiv 3 \pmod p$, so that $|R| \equiv v$ or $-v \pmod p$. Also, if $|R| = v$, then multiplying the third member of (65) by a or b, and using all of (65), we see that

$$a \equiv -dv,\ b \equiv cv \pmod p. \tag{65'}$$

Now it is well known that (64) has exactly $1 + (p + 1)(p^2 - 1)$ solutions. The lemma then asserts that if $\mathfrak{x}$ is a non-null column vector $\{x_2, x_3\}$, and R_1, R_2 are distinct solutions of $R'ER \equiv -3I$ with the same determinant v, then $R_1\mathfrak{x}$ and $R_2\mathfrak{x}$ are distinct vectors. This follows from the fact that $|R_1 - R_2| \neq 0$. To prove the last fact, notice first that $R'ER \equiv -3I$ has at least one solution (solve $b^2 + 3d^2 \equiv -3$ and use (65')), and that if R is one solution then every solution is given by RV, where V ranges over the solutions of $V^2V \equiv I \pmod p$. Now the last congruence has exactly the $2\{p - (-1|p)\}$ solutions

(66) $$\begin{pmatrix} y & z \\ -z & y \end{pmatrix} \text{ and } \begin{pmatrix} y & z \\ z & -y \end{pmatrix}, \text{ where } y^2 + z^2 \equiv 1.$$

For (66_1) evidently $|V - I| = y^2 - 2y + 1 + z^2 = 2 - 2y \neq 0$ unless $V = I$. Hence also $|RV - R| \neq 0$ unless $V = I$. (On the other hand it is seen using the same machinery that if the determinants of R_1 and R_2 are different, then $R_1 - R_2$ is always singular, and that therefore no new solutions are obtained by using $-v$ in place of v!)

All solutions of (64) are thus accounted for if $p \equiv 3 \pmod 4$. But if $p \equiv 1 \pmod 4$, we are short $2(p^2 - 1)$ solutions in using (63). These are provided by the $4(p - 1)$ solutions satisfying (63′) with exactly one of the pairs x_0, x_1 and x_2, x_3 null; and the $2(p-1)^2$ solutions satisfying (63′) with neither pair null. There is no overlapping with the solutions satisfying (63), since (63) and (63′) together imply that $x_0 = x_1 = x_2 = x_3 = 0$. The lemma follows.

Consider now the equation

(67) $$pn = x_0^2 + 3(x_1^2 + x_2^2 + x_3^2).$$

We assume (63), the treatment of (63′) being similar. We can thus set

(68) $$x_0 = py_0 + ay_2 + by_3,\ x_1 = py_1 + cy_2 + dy_3,\ x_2 = y_2,\ x_3 = y_3,$$

and so have $p - (-1 \mid p)$ substitutions each of determinant p^2. For each of these the resulting form in $y_0, \cdots, y_3$ may be designated as pg^*. Thus g^* is integral, has determinant $3^3(p^2)^2/p^4 = 3^3$, and has first coefficient p.

Now there are two genera of determinant 3^3 which have the same ordinal structure as regards the primes 2 and 3 as $f = x_0^2 + 3x_1^2 + 3x_2^2 + 3x_3^2$. One is that of f, and the other is that of

(69) $$f' = 2z_0^2 + 2z_0z_1 + 2z_1^2 + 3z_2^2 + 3z_3^2.$$

Clearly, g^* belongs to the genus of f or f' according as $p \equiv 1$ or $2 \pmod 3$: in other words, since $(3 \mid p) = 1$, according as $p \equiv 1$ or $-1 \pmod{12}$. Both genera are known to consist of one class.

Consider the case $p = 12q - 1$. Then there exists a linear transformation of integral matrix $T = (t_{ij})$ $(i, j = 0, \cdots, 3)$ and determinant p^2 which replaces f by pf'. Hence

$$2p = t_{00}^2 + 3t_{10}^2 + 3t_{20}^2 + 3t_{30}^2.$$

If t_{00} could be odd, $(2p - t_{00}^2)/3$ would be congruent to 7 (mod 8) and could not be a sum of three squares. Hence t_{00} and, likewise, t_{01} are even. Both t_{02} and t_{03} cannot be even since $|T|$ is odd; also, both cannot be odd, since

$$3p = t_{02}^2 + 3(t_{12}^2 + t_{22}^2 + t_{32}^2),\ 3p = t_{03}^2 + 3(t_{13}^2 + t_{23}^2 + t_{33}^2),$$

then requires that $t_{12}, t_{22}, t_{32}, t_{13}, t_{23}, t_{33}$ are even, and this contradicts

$$0 = t_{02}t_{03} + 3(t_{12}t_{13} + t_{22}t_{23} + t_{32}t_{33}).$$

Hence $t_{02} \not\equiv t_{03} \pmod 2$.

It follows that in $x_0 = t_{00}z_0 + t_{01}z_1 + t_{02}z_2 + t_{03}z_3$, x_0 is congruent (mod 2) to a definite one of z_2 and z_3. Hence, the number of representations of an odd number by f' with z_2 odd being half the total number $f'(n)$, we have, if n is odd and $p \equiv -1 \pmod{12}$,

$$F_i(pn) = F_i(n/p) + (p+1)\{\tfrac{1}{2}f'(n) - F_i(n/p)\}, \qquad (i = 1, 2),$$

or

$$F_i(pn) + pF_i(n/p) = \tfrac{1}{2}(p+1) \cdot f'(n), \qquad (i = 1, 2). \tag{70}$$

COROLLARY 1. *If* $(n, p) = 1$ *and* $p \equiv -1 \pmod{12}$, $F_1(pn) = F_2(pn)$. *Also,* $F_1(p^{2h+1}n) = F_2(p^{2h+1}n)$.

This completes the proof of Theorem 7.

COROLLARY 2. *If* $N\sigma$ *is odd and is divisible by* 3 *or by some prime* $p = 12q - 1$ *to an odd exponent, then* $r_4(\sigma, 12)$ *is given by the same final expression* $8\varepsilon\prod c_p$ *as in* (57).

Among other deductions that can be easily made from (70), along with the formula for $F_1(n) + F_2(n)$ is the value of $F_1(p^{2h})$. In particular,

$$F_1(p^2) = (p^2 + 1)/2. \tag{70a}$$

Consider next the case where $2^u \parallel N\sigma = s_0^2 - 12s_3^2$, u ($\geqq 3$) odd. Then

$$s_0 = 2^{(u-1)/2}s_2, s_3 = 2^{(u-3)/2}s_5,$$

$s_2^2 - 3s_5^2 \equiv 2 \pmod 4$, hence s_2 and s_5 are odd. Hence h' can be divisible at most by $2^{(u-3)/2}$. Accordingly,

$$\begin{aligned} r_4(\sigma, d) &= 4\varepsilon \sum_{h' \mid D} g_{D/h'}(n/h'^2)\psi_n(h') \\ &= 4\varepsilon c_2 \prod c_p, \end{aligned} \tag{71}$$

where

$$\begin{aligned} c_2 &= \sum_{i=0}^{(u-3)/2} g_{2^{(u-3)/2-i}}(2^{u-2i}) \cdot \psi_n(2^i) \\ &= 6(2^{u-2} - 1), \ (u \text{ odd}, u \geqq 3). \end{aligned} \tag{72}$$

Finally, let $2^u \parallel s_0^2 - 12s_3^2$, u even, $u \geqq 4$. Write $D'' = (s_2, s_3)$, where $s_2 = s_0/2$. Then $2^{(u/2)-1} \parallel D''$, and if we define $h'' = (t_0, \cdots, t_3, s_2, s_3)$, evidently h'' and h' are alike even or odd. Hence

$$r_4(\sigma, d) = 4\varepsilon \sum_{h'' \mid D''} g_{D''/h''}(n/h''^2) \cdot \psi_n(h'')$$
$$= 4\varepsilon c_2 \prod c_p,$$

where c_p is of course the same as before, and c_2 is found to have the same final formula as in (72), with u even, $u \geqq 4$.

References

1. H. Cohn, *A numerical study of the representation of a totally positive integer as a sum of quadratic integral squares*, Numerische Math. **1** (1959), 121–134.

2. ———, *Decomposition into four integral squares in the fields of* $2^{1/2}$ *and* $3^{1/2}$, Amer. J. Math. **82** (1960), 301–322.

3. ———, *Cusp forms arising from Hilbert's modular functions for the field of* $3^{1/2}$, Amer. J. Math. **84** (1962), 283–305.

4. L. E. Dickson, *History of the theory of numbers*, Vol. III, Carnegie Institution, Washington, D. C., 1923, pp. 228–229.

4a. J. Dzewas, *Quadratsummen in reell-quadratischen Zahlkörpern*, Math. Nachr. **21** (1960), 233–284.

5. F. Götzky, *Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Verändlichen*, Math. Ann. **100** (1928), 411–437.

6. L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Z. **35** (1932), 1–15.

7. I. Niven, *Integers of quadratic fields as the sum of squares*, Trans. Amer. Math. Soc. **48** (1940), 405–417.

8. G. Pall, *The structure of the number of representations function in a binary quadratic form*, Trans. Amer. Math. Soc. **35** (1933), 491–509.

9. ———, *On the arithmetic of quaternions*, Trans. Amer. Math. Soc. **47** (1940), 487–500.

10. ———, *Representation by quadratic forms*, Canad. J. Math. **1** (1949), 344–364.

11. ———, *Sums of two squares in a quadratic field*, Duke Math. J. **18** (1951), 399–409.

12. G. Pall and O. Taussky, *Application of quaternions to the representation of a binary quadratic form as a sum of four squares*, Proc. Roy. Irish Acad. **58A** (1957), 23–28.

13. C. L. Siegel, *Lectures on the analytical theory of quadratic forms*, Mimeographed notes, Princeton, 1935.

University of Arizona,
Tucson, Arizona
Illinois Institute of Technology,
Chicago, Illinois