Then necessarily, θ is integral but not rational. Let $g(X) = \mathrm{Irr}(\theta, Q) = X^m + c_{m-1}X^{m-1} + \ldots + c_1X + c_0$ be the minimal polynomial for θ in $\boldsymbol{Z}[X]$. Since the absolute norm

$$\|\theta\| = |c_0| = \|\mathfrak{p}\mathfrak{a}\| = \|\mathfrak{p}\|\cdot\|\mathfrak{a}\| = pa,$$

$$(p, a) = 1$$

and so

$$f(X) = p^{-1}g(pX)$$

is primitive with rational integral coefficients! Since we may choose $\mathfrak{a}$ prime to any prime $q \leqslant n$, the values $f(x)$ need not possess a non-trivial common divisor.

For any number field k with class number $h(k) > 1$, construct $f(X)$ as above. Then every value $f(x)$ has at least one non-principal prime divisor in k.

For θ/p is a root of $f(X) = 0$ and hence in $k[X]$,

$$f(X) = (pX - \theta)\frac{G(X)}{p}$$

where $F(X) = pX - \theta$ has non-principal content $\mathfrak{p}$.

Specializing, let $k = Q(\sqrt{-5})$, $p = 2$, and $\theta = 1 + \sqrt{-5}$. Then

$$f(X) = 2X^2 - 2X + 3$$

always has non-principal divisors in $Q(\sqrt{-5})$. This can be seen directly by translating Artin reciprocity for the class field $Q(\sqrt{5}, i)/Q(\sqrt{-5})$ into residues modulo 20.

Reference

[1] C. J. Parry, *On a problem of Schinzel concerning principal divisors in arithmetic progressions*, Acta Arith. 19 (1971), pp. 215–222.

MICHIGAN STATE UNIVERSITY

Received on 23. 2. 1970 (40)

ACTA ARITHMETICA
XIX (1971)

Primitive representation of a binary quadratic form as a sum of four squares

by

JOHN L. HUNSUCKER (Athens, Ga.)

1. If an integral binary quadratic form f of nonzero determinant is representable as a sum of four squares, i.e., in the form $(r_1x+s_1y)^2 + \ldots + (r_4x+s_4y)^2$ where $r_1, \ldots, s_4$ are integers, then f can be written as ef', where e is a positive integer, $f' = [a, 2t_0; b] = ax^2 + 2t_0xy + by^2$, $(a, t_0, b) = 1$, $a > 0$, $ab - t_0^2 > 0$. L. J. Mordell showed that such a form is representable as a sum of four squares if and only if $ab - t_0^2$ is not of the form $4^h(8n+7)$. H. Braun gave an expression for the number $r_4(f)$ of such representations, and G. Pall and O. Taussky found a simpler expression which showed that for fixed f' (with $r_4(f') \neq 0$), $r_4(ef')/r_4(f')$ is a factorable function of e. We will here prove a like result for $r_4'(ef')/r_4'(f')$, where $r_4'(\ldots)$ denotes the number of *primitive* representations, in which the g.c.d. of the six determinants $r_is_j - r_js_i$ is unity; and we will find simple formulas for $r_4'(f)$, and related results.

2. Let B_1 denote the matrix of ef', $c = ab - t_0^2$, $b_1 = e^2c$,

$$E = \operatorname{adj} B_1 = eR, \qquad R = \begin{bmatrix} b & -t_0 \\ -t_0 & a \end{bmatrix}. \tag{1}$$

Our work will be based on an algorithm due to G. Pall ([3], § 3). The algorithm is simplest for the study of primitive representations of a form in k variables by one in n variables, when $k = 1$ or $n-1$. In our case, $n = 4$ and $k = 2$, and we have to locate the integral symmetric positive-definite matrices G of determinant b_1 for which

$$KEK' \equiv -G \pmod{b_1} \tag{2}$$

has integral solution matrices K (of order 2). By (2) the g.c.d. e of the elements of E must divide the elements of G. But Pall's algorithm (see (13)–(14) of [3]) requires in the case where the determinant of the representing form is 1 that

$$L'GL \equiv -E \pmod{b_1} \tag{3}$$

be solvable for L. Hence the g.c.d. of the elements of G is also e.

We put $G = eQ$ with Q primitive, and so reduce (2) and (3) to

$$(4) \qquad KRK' \equiv -Q, \quad L'QL \equiv -R \pmod{ec}.$$

We denote the form of matrix Q by g. If (4) holds, R and $-Q$ represent the same residues modulo ec, and hence $(g|p) = (-f'|p)$ for each odd prime factor p of c. However, the conditions imposed on the generic characters of g by the solvability of (4) may conflict with the product relation the generic characters must satisfy (which, as Gauss showed, ensures the existence of a corresponding form). If f_0 is a positive-definite primitive binary quadratic form of discriminant $-2^h m = -2^h p_1 \dots p_r$ (where the p_i are odd primes, not necessarily distinct), the Gaussian product relation may be given the form

$$(5) \qquad a(f_0) = \beta(f_0),$$

$$\text{where } a(f_0) = (f_0|p_1)\dots(f_0|p_r),\ \beta(f_0) = (2|a)^h(-1)^{\frac{a-1}{2}\cdot\frac{m+1}{2}},$$

where a is any odd number represented by f_0. We will prove:

THEOREM 1. *The form f is primitively representable as a sum of four squares if and only if*

$$(6) \qquad \text{(i) } e^2c \equiv 3 \pmod 8, \text{ or (ii) } c \equiv 1 \text{ or } 2 \pmod 4 \text{ and } e \text{ is odd or double-an-odd}.$$

These are exactly the cases in which g can be chosen to make (4) solvable. The forms g which thus work for a given f constitute a single genus characterized by the property that $(g|p) = (-f'|p)$ for odd prime factors p of c and the following: in case (i), one of f' and g is p.p. (properly primitive), the other i.p. (improperly primitive); in case (ii), f' and g are p.p. and the generic character $\beta(g)$ is determined by (5).

Proof. We cannot have f' and g i.p., since then $m \equiv 3 \pmod 4$, $\beta(\frac12 g) = \beta(\frac12 f') = 1$, $a(\frac12 f')/a(\frac12 g) = (-1|m) = -1$. If $2|ec$, (4) shows that f' and g are alike i.p. or p.p.; hence both are p.p. If f' is i.p. and g is p.p. [or vice versa], $a(g)/a(\frac12 f') = (-2|c)$, $\beta(g) = \beta(\frac12 f') = 1$, hence g works only if $c \equiv 3 \pmod 8$. Only cases with f' and g both p.p. remain. Then $c \equiv 3 \pmod 4$ is excluded since $a(f')/a(g) = (-1|c) = -1$, and $\beta(f')/\beta(g) = 1$. In case (ii), the generic character $\beta(g)$ can be uniquely chosen to satisfy (5). If $4|e$, and f' represents the odd number a, then by (4) either g represents $-a \pmod 8$, or h is even and g represents $-a \pmod 4$, hence $a(f')/a(g) = (-1)^{(m-1)/2}$, but

$$\beta(f')/\beta(g) = (-1)^{\frac{a-1}{2}\cdot\frac{m+1}{2}}\cdot(-1)^{\frac{-a-1}{2}\cdot\frac{m+1}{2}} = (-1)^{(m+1)/2}.$$

3. Let us denote by p^ε and p^γ the precise powers of p in e and c. Supposing that G is such that (4) is solvable we will count the solutions $K \pmod{p^{\varepsilon+\gamma}}$ of

$$(7) \qquad KRK' \equiv -Q \pmod{p^{\varepsilon+\gamma}}.$$

We can replace f' and g by equivalent forms and can multiply both members by a residue prime to p. Thus, if p is odd, we can give both f' and $-g$ the residue $x^2+p^\gamma ty^2$, where t has the quadratic character of c/p^γ. Thus (7) reduces to

$$(8) \qquad k_1^2+p^\gamma tk_2^2 \equiv 1, \quad k_1k_3+p^\gamma tk_2k_4 \equiv 0, \quad k_3^2+p^\gamma tk_4^2 \equiv p^\gamma t, \quad \pmod{p^{\varepsilon+\gamma}},$$

and it follows easily that the number of solutions of (7) is

$$(9) \qquad \begin{array}{lll} 2p^{\varepsilon-1}[p-(-c|p)] & \text{if} & \varepsilon > 0 = \gamma; \\ 2p^{2\gamma} & \text{if} & \gamma > 0 = \varepsilon; \\ 4p^{\varepsilon+2\gamma} & \text{if} & \gamma > 0,\ \varepsilon > 0. \end{array}$$

For example in the last case we may take k_2 arbitrary ($p^{\varepsilon+\gamma}$ residues), and have two residues k_1 such that $k_1^2 \equiv 1-p^\gamma tk_2^2 \pmod{p^{\varepsilon+\gamma}}$; then, regarding k_3 as determined by $k_3 \equiv -p^\gamma tk_2k_4/k_1$, and substituting into the third congruence, we get $p^{2\gamma}tk_2^2k_4^2+p^\gamma tk_4^2k_1^2 \equiv p^\gamma tk_1^2 \pmod{p^{\varepsilon+\gamma}}$, or $k_4^2 \equiv k_1^2 \bmod p^\varepsilon$), $k_4 \equiv \pm k_1 \pmod{p^\varepsilon}$, or $2p^\gamma$ residues k_4: $p^{\varepsilon+\gamma}\cdot 2\cdot 2p^\gamma = 4p^{\varepsilon+2\gamma}$.

We have also to consider $p = 2$ in the cases (6). We can take R and $-Q$ to be the identity mod 2 if $c \equiv 1$, $e \equiv 2 \pmod 4$; to be S (see below) mod 2 if e and $c/2$ are odd; to be one or both of V and $W \pmod 4$ if $c/2$ and $e/2$ are odd. We count respectively two, four, and eight solutions K:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad V = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \quad W = \begin{bmatrix} -1 & 0 \\ & 0\ 2 \end{bmatrix}.$$

Now (7) is equivalent to

$$(10) \qquad KEK' \equiv -G \pmod{p^{2\varepsilon+\gamma}};$$

and, counting K to the modulus $p^{2\varepsilon+\gamma}$, the number of solutions of (10) is, if $p > 2$,

$$(11) \qquad \begin{array}{lll} 2p^{5\varepsilon-1}[p-(-c|p)] & \text{if} & \varepsilon > 0 = \gamma; \\ 2p^{2\gamma} & \text{if} & \gamma > 0 = \varepsilon; \\ 4p^{5\varepsilon+2\gamma} & \text{if} & \gamma > 0,\ \varepsilon > 0; \end{array}$$

and, if $p = 2$, 1 if ec is odd,

$$(12) \qquad 2^5 \text{ if } c \equiv 1, e \equiv 2, \quad 2^2 \text{ if } c \equiv 2,\ e \text{ odd}; \quad 2^7 \text{ if } c \equiv e \equiv 2 \pmod 4.$$

4. The form $x^2+y^2+z^2+w^2$ has $2^4(4!)/2 = 192$ unimodular automorph's. Pall's algorithm leads to a formula which reduces in the present case to

$$r_4'(f) = 192\sum_{j=1}^{n}\varrho(G_j)/u, \tag{13}$$

where $G_1, \ldots, G_n$ are representative matrices, one chosen from each class for which (2) is solvable, u is the number of unimodular automorphs of each G_j (the same for each since they belong to one genus), and $\varrho(G)$ (again the same for each G_j) is the number of solutions K of (2), with K counted not modulo b_1 but instead modulo B_1. Here two solutions K_1 and K_2 are called *congruent modulo* B_1 if K_1-K_2 has B_1 as a right divisor, i.e., $K_1-K_2 = XB_1$ for an integral matrix X. (Notice that if K is a solution of (2), so is $K+XB_1$).

To count the number of solutions modulo B_1, notice that: *as X ranges over all 2-by-2 integral matrices, XB_1 gives rise to exactly b_1^2 incongruent matrix residues modulo b_1.* For, the result is unaltered if B_1 is multiplied on either side by unit-modular matrices, and hence we can diagonalize B_1. And if $rs = b_1$,

$$\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix} = \begin{bmatrix} x_1r & x_2s \\ x_3r & x_4s \end{bmatrix}$$

with, evidently, $(b_1/r)^2(b_1/s)^2 = b_1^2$ distinct residues $\bmod b_1$. We therefore have

THEOREM 2. *In the cases in* (6) *the number $r_4'(f)$ of primitive representations of f as a sum of four squares is equal to*

$$192(k/u)\prod_{p|b_1}\chi(p), \tag{14}$$

where $\chi(2) = 1$ if $e^2c \equiv 3 \pmod 8$, or e is odd and $c \equiv 2 \pmod 4$; $\chi(2) = 2$ if $e \equiv 2$, $c \equiv 1$ or $2 \pmod 4$; and if $p > 2$, $\chi(p)$ (obtained from (11)–(12) by dividing by $p^{4s+2\gamma}$) *is given by*

$$2p^{\varepsilon-1}[p-(-c|p)] \text{ if } \varepsilon > 0 = \gamma; \quad 2 \text{ if } \gamma > 0 = \varepsilon; \quad 4p^{\varepsilon} \text{ if } \gamma > 0,\ \varepsilon > 0. \tag{15}$$

Here k denotes the number of classes in the unique genus of G, and u is the number of unimodular automorphs of any form in that genus.

We recall from elementary number theory that if d denotes the discriminant of the primitive part of g (or f), $u = 6$ if $d = -3$, $u = 4$ if $d = -4$, $u = 2$ if $d < -4$. Also, f and g have equally many classes in their two genera, save that if $e^2c \equiv 3 \pmod 8$ and $e^2c > 3$, one of f' and g is i.p., the other p.p., and the p.p. genus has three times as many classes as the i.p. one.

THEOREM 3. *Assume that $r_4'(f') > 0$, i.e., $c \equiv 1, 2, 3, 5$, or $6 \pmod 8$. Then*

$$r_4'(f') = 192(k/u)2^q, \tag{16}$$

where q is the number of distinct odd prime factors of c. Also,

$$\frac{r_4'(ef')}{r_4'(f')} = \prod_{p|e}\chi_0(p) = e\cdot 2^s\cdot\prod_{\substack{p|e\\ p\nmid c,\, p>2}}[1-(-c|p)p^{-1}], \tag{17}$$

where $\chi_0(2) = 0$ if (6) does not hold, and $\chi_0(2)$ coincides with $\chi(2)$ in Theorem 1 otherwise; and if p is odd,

$$\chi_0(p) = \begin{cases} 2p^{s-1}[p-(-c|p)] & \text{if } p|e,\ p\nmid c; \\ 2p^{s} & \text{if } p|e,\ p|c; \end{cases}$$

where s denotes the number of distinct odd primes dividing e: obviously, for fixed f', a factorable function of e.

References

[1] H. Braun, *Ueber die Zerlegung quadratischer Formen in Quadrate*, Journ. Reine Angew. Math. 178 (1938), pp. 34–64.

[2] L. J. Mordell, *An application of quaternions to the representations of a binary quadratic form as the sum of four linear squares*, Oxford Quart. J. 8 (1937), pp. 58–61.

[3] G. Pall, *Representation by quadratic forms*, Canad. Journ. Math. 1 (1949), pp. 344–364.

[4] — and O. Taussky, *Application of quaternions to the representations of a binary quadratic form as the sum of four squares*, Proc. Roy. Irish Acad. 58 (1957), pp. 23–28.

Received on 10. 3. 1970 (57)