Thus we are left with the case where $r \leqslant e-2$ and $l \leqslant r$.

Since $l \leqslant r \leqslant e-2$, $l < e$, so $a_1 \equiv \pm 3 \pmod 8$ and using this and applying 2.2 and 2.6 we see that (**) cannot hold in this case.

References

[1] Maria Acosta de Orozco and William Yslas Vélez, *The lattice of subfields of a radical extension*, J. Number Theory 15 (1982), 388–405.
[2] — — *The torsion group of a field defined by radicals*, ibid. 19 (1984), 283–294.
[3] David Gay and William Yslas Vélez, *The torsion group of a radical extension*, Pacific J. Math. 92 (1981), 317–327.
[4] Irving Gerst, *On the theory of n-th power residues and a theorem of Kronecker*, Acta Arith. 17 (1970), 121–139.
[5] Kenkichi Iwasawa, *On the ring of valuation vectors*, Ann. of Math. 57 (1953), 331–356.
[6] Eliot Jacobson and William Yslas Vélez, *On the adèle rings of radical extensions of the rationals*, Archiv der Mathematik 45 (1985), 12–20.
[7] Warren May, *Fields with free multiplicative groups modulo torsion*, Rocky Mountain J. Math. 10 (1980), 599–604.
[8] Andrzej Schinzel, *On linear dependence of roots*, Acta Arith. 28 (1975), 161–175.
[9] William Yslas Vélez, *On normal binomials*, ibid. 36 (1980), 113–124.
[10] — *Several results on radical extensions*, Archiv der Mathematik 45 (1985), 342–349.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ARIZONA
Tucson, Arizona 85721

Received on 21.5.1986 (1640)

ACTA ARITHMETICA
LI (1988)

An arithmetic problem on the sums of three squares

by

A. Arenas (Barcelona)

Introduction. As is well known, any positive integer $n \neq 4^a(8b+7)$ can be expressed as a sum of three integer squares. In general, given a decomposition of n, $n = x_1^2 + x_2^2 + x_3^2$, very little is known about the integers x_i. C. F. Gauss proved that n admits a primitive representation as a sum of three squares if and only if $n \not\equiv 0, 4, 7 \pmod 8$ (cf. [5], Art. 291). Catalan showed that if $n = 3^\nu$, the three summands could be chosen to be prime to 3 (cf. [3]).

Special representations of integers as a sum of three squares have recently appeared in connection with the determination of some Stiefel–Whitney classes (see [11]). Let ξ_n be the real bundle over the classifying space BA_n associated to the standard representation of the alternating group A_n into $SO_n(\boldsymbol{R})$. Let $w^*(\xi_n) \in H^*(BA_n, Z/2Z) = H^*(A_n, Z/2Z)$ be its Stiefel–Whitney class. Since $w^1(\xi_n) = 0$, $w^2(\xi_n)$ is the nontrivial element of $H^2(A_n, Z/2Z) = Z/2Z$. It is shown in [11] (cf. also [7]), that if $n \equiv 3 \pmod 8$ admits a representation as a sum of three integer squares with $(x_1, n) = 1$ and $x_1^2 \leqslant (n+1)/3$, then there exists a continuous surjective representation $\varrho\colon \mathrm{Gal}(\overline{\boldsymbol{Q}(T)}/\boldsymbol{Q}(T)) \to A_n$ of the absolute Galois group of $\boldsymbol{Q}(T)$ such that its second Stiefel–Whitney class $\varrho^* w^2(\xi_n)$ is trivial.

Given an integer n, we consider in this paper the maximum value $l = l(n)$ such that n can be written as a sum of three integer squares with l summands prime to n. We call $l(n)$ the level of n.

Obviously, all integers having level 3 satisfy the preceding condition.

The problem of the determination of the level of an integer leads to compare numbers of representations of this integer by different ternary quadratic forms of a very special type.

Since the number of representation $r(n, f)$ of a given positive integer by a quadratic form cannot be determined in general, we approximate this number by the average value $r(n, \operatorname{gen} f)$, where $\operatorname{gen} f$ stands for the genus of f. By means of Siegel's Hauptsatz (see [9]) this average value can be calculated using p-adic densities.

For the forms we are dealing with, we have that $r(n, \operatorname{gen} f) = r(n, \operatorname{spn} f)$, where $\operatorname{spn} f$ denotes the spinorial genus of f.

If n is square-free, the above considerations allow to estimate the error $r(n,f)-r(n, \text{gen} f)$ by applying recent results of Schulze-Pillot about the growth of Fourier coefficients of cusp forms of weight 3/2 (cf. [6]).

We conclude, under the assumption of Ramanujan–Petersson's conjecture for modular forms of weight 3/2, that if $n \not\equiv 7 \pmod 8$ is a square-free positive integer sufficiently large (see Sect. 4), then:

(i) $l(n) = 2$, if g.c.d. $(n, 10) \neq 1$,

(ii) $l(n) = 3$, if g.c.d. $(n, 10) = 1$.

The nonsquare-free case is considered in [2].

I wish to express my thanks to Professor P. Bayer for her valuable help.

1. The level of a positive integer.

DEFINITION. For a positive integer n we define the *level* $l(n)$ of n as the maximum value of l such that there exists an integral representation of n as a sum of three squares, $n = x_1^2+x_2^2+x_3^2$, with l summands prime to n.

We agree that $l(n) = -1$ if $n = 4^a(8b+7)$. If $4|n$ and $n \neq 4^a(8b+7)$, then it is clear that $l(n) = 0$. So we shall assume that $n \not\equiv 0, 4, 7 \pmod 8$.

If 2 or 5 divides n, then we have $l(n) < 3$.

By elementary methods, some families of integers with a given level can be constructed (see [1]).

For a given positive definite ternary quadratic integral form $f(x_1, x_2, x_3)$ we write, as usual

$$r(n,f) = \#\{(x_i) \in \mathbf{Z}^3 \mid f(x_1, x_2, x_3) = n\},$$

$$r_m(n,f) = \#\{(x_i) \in (\mathbf{Z}/m\mathbf{Z})^3 \mid f(x_1, x_2, x_3) \equiv n \pmod m\},$$

and we denote by $r(n, \text{gen} f)$ the average value of representations of n by all the forms in the genus of f (see [9]).

Siegel's Hauptsatz (see [9]) asserts that $r(n, \text{gen} f)$ may be evaluated by means of p-adic densities $\partial_p(n,f)$, with p prime or ∞, as follows

$$r(n, \text{gen} f) = \partial_\infty(n,f) \prod_p \partial_p(n,f),$$

where

$$\partial_p(n,f) = \begin{cases} \dfrac{2\pi n^{1/2}}{(\det f)^{1/2}}, & \text{if } p = \infty, \\ \dfrac{r_{p^{2\alpha}}(n,f)}{p^{2\alpha}}, & \text{for all } \alpha \geq 2\beta+1, \text{ where } p^\beta \| 2n, \text{ if } p \text{ is prime.} \end{cases}$$

We write $\langle a_1^2, a_2^2, a_3^2 \rangle$ for a diagonal quadratic form and $I_3 = \langle 1, 1, 1 \rangle$ for the identity. As usual, we denote by μ the Möbius function, and by [ ] the integral part function.

In order to evaluate $l(n)$ we first introduce the following alternating sums:

$$s_i(n) = \varrho_i \sum_{(1)} (-1)^i \mu(a_1)\mu(a_2)\mu(a_3) r(n, \langle a_1^2, a_2^2, a_3^2 \rangle),$$

for $i = 1, 2, 3$. The sum (1) is taken over those square-free positive integers a_j, $j = 1, 2, 3$, such that $1 < a_j | n$ for $j \leq i$ and $a_j = 1$ for $j > i$. We take $\varrho_i = 3-2[i/3]$.

We introduce the functions

$$g_1(n) = \frac{s_3(n)}{r(n, I_3)}, \quad g_2(n) = \frac{s_2(n)-2s_3(n)}{r(n, I_3)}, \quad g_3(n) = \frac{s_1(n)-s_2(n)+s_3(n)}{r(n, I_3)}.$$

The next proposition establishes a criterion for the determination of the value of $l(n)$.

PROPOSITION 1. *$l(n) \geq i$ if and only if $g_i(n) < 1$.*

Proof. One needs only to observe that the sums $s_i(n)$, $i = 1, 2, 3$, count the number of integral solutions of $X_1^2+X_2^2+X_3^2 = n$ with at least i summands not prime to n.

2. The main term in the square-free case. As, in general, the value of $r(n,f)$ cannot be determined, we introduce the following average alternating sums:

$$S_i(n) = \varrho_i \sum_{(1)} (-1)^i \mu(a_1)\mu(a_2)\mu(a_3) r(n, \text{gen} \langle a_1^2, a_2^2, a_3^2 \rangle),$$

for $i = 1, 2, 3$. The sum (1) and ϱ_i are defined as in Section 1.

In order to estimate the value of $l(n)$, for n square-free, we next define the main term $G_i(n)$ in the determination of the level, as follows:

$$G_1(n) = S_3'(n), \quad G_2(n) = S_2'(n)-2S_3'(n), \quad G_3(n) = S_1'(n)-S_2'(n)+S_3'(n),$$

where $S_i'(n) = r(n, I_3)^{-1} S_i(n)$, $i = 1, 2, 3$.

From now on we will assume that $n \not\equiv 7 \pmod 8$ and that n is a square-free positive integer. We will always write $n = mt$ with $m = 2^\alpha p_1 \ldots p_r$, $\alpha = 0$ or 1, $p_i \equiv 1 \pmod 4$ and $t = q_1 \ldots q_s$ with $q_j \equiv 3 \pmod 4$.

PROPOSITION 2. *For $n = mt$, the alternating sums $s_i(n)$, $1 \leq i \leq 3$, can be written in the form:*

(i) $$s_i(n) = \sum_{(2)} (-1)^i \mu(a_1 a_2 a_3) r(n, \langle a_1^2, a_2^2, a_3^2 \rangle),$$

where the sum (2) is taken over the positive integers a_j such that $a_j | m$; g.c.d. $(a_j, a_k) = 1$, for $j \neq k$; $a_j \neq 1$ if $j \leq i$ and $a_j = 1$ if $j > i$.

(ii) *If n is even, we also have*

$$s_3(n) = 3\sum_{(3)} -\mu(2a_1 a_2)\, r(n, \langle a_1^2, a_2^2, 2^2\rangle),$$

$$s_2(n) = 6\sum_{(4)} -\mu(a)\, r(n, \langle a^2, 2^2, 1^2\rangle) + s_3(n),$$

$$s_1(n) = 3r(n, \langle 2^2, 1^2, 1^2\rangle) + s_2(n) - s_3(n),$$

where the sum (3) *is taken over the positive integers a_1, a_2, such that* g.c.d. $(a_1, a_2) = 1$ *and* $1 < a_j | 2^{-1} m$, *for* $j = 1, 2$. *The sum* (4) *is taken over the positive integers a with* $1 < a | 2^{-1} m$.

Proof. (i) The first expression is a consequence of the following two facts: First of all, since n is square-free, a prime p dividing n can appear only in one a_j. Secondly, if $q \equiv 3 \pmod 4$ is a prime dividing n, then $q \nmid a_j$, $j = 1, 2, 3$, for, otherwise, by reducing modulo q we would have $\left(\frac{-1}{q}\right) = 1$, which is impossible.

Observe that the last consideration also proves that if $m = 1$, then $l(n) = 3$.

(ii) In this case, one needs to distinguish in the formula given in (i) just the summands involving 2 from those not involving it.

LEMMA 1. *Let $n = mt$ be an odd square-free positive integer,*

$$n \not\equiv 7 \pmod 8.$$

Let $\langle a_1^2, a_2^2, a_3^2\rangle$ be a quadratic form with $a_i | m$, a_i square-free, for $i = 1, 2, 3$ and g.c.d. $(a_i, a_j) = 1$, *for* $i \neq j$. *Then*:

$$\text{(i)}\quad \partial_p(n, \langle a_1^2, a_2^2, a_3^2\rangle) = \begin{cases} (1-p^{-2})\left(1-\left(\frac{-n}{p}\right)p^{-1}\right)^{-1}, & \text{if } p \nmid n,\\ (1-p^{-2}), & \text{if } p | n \text{ and } p \nmid a_1 a_2 a_3,\\ 2(1-p^{-1}), & \text{if } p | a_1 a_2 a_3 \end{cases}$$

for $p \neq 2$.

$$\text{(ii)}\quad \partial_2(n, \langle a_1^2, a_2^2, a_3^2\rangle) = \begin{cases} 3/2, & \text{if } n \equiv 1, 5 \pmod 8,\\ 1, & \text{if } n \equiv 3 \pmod 8. \end{cases}$$

Proof. (i) The first two equalities of (i) follow immediately from [10], Hilfssatz 16.

Now, if $p | a_1 a_2 a_3$, say $p | a_1$, in order to calculate $\partial_p(n, \langle a_1^2, a_2^2, a_3^2\rangle)$ we first evaluate $r_{p^3}(n - a_1^2 x_1^2, \langle a_2^2, a_3^2\rangle)$ for each x_1 in $\boldsymbol{Z}/p^3\boldsymbol{Z}$. Letting now x_1 run over $\boldsymbol{Z}/p^3\boldsymbol{Z}$ and applying Siegel's formulae to the case of binary forms (cf. [9], Hilfssatz 16), we eventually get $\partial_p(n, \langle a_1^2, a_2^2, a_3^2\rangle) = 2(1-p^{-1})$.

(ii) As the a_i's are odd we have $\partial_2(n, \langle a_1^2, a_2^2, a_3^2\rangle) = \partial_2(n, I_3)$; and this reduces to the trivial calculation of $r_{2^3}(n, I_3)$, from which the assertion follows.

PROPOSITION 3. *Let $n = mt$ be a square-free positive integer,*

$$n \not\equiv 7 \pmod 8,$$

then: (i) *If n is odd, $a_i | m$ for $i = 1, 2, 3$, and* g.c.d. $(a_i, a_j) = 1$ *for* $i \neq j$, *then*

$$r(n, \text{gen}\langle a_1^2, a_2^2, a_3^2\rangle) = \frac{A(n)}{\pi} n^{1/2} L(1, \chi_{-4n}) \prod_{p | a_1 a_2 a_3} 2(1+p)^{-1},$$

with

$$A(n) = \begin{cases} 16 & \text{if } n \equiv 3 \pmod 8,\\ 24 & \text{if } n \equiv 1, 5 \pmod 8, \end{cases}$$

and $L(s, \chi_{-4n})$ being the L-series associated to the character χ_{-4n}.

(ii) *If n is even, $a_i | 2^{-1} m$ for $i = 1, 2$, and* g.c.d. $(a_1, a_2) = 1$, *then*

$$r(n, \text{gen}\langle a_1^2, a_2^2, a_3^2\rangle) = \frac{8}{\pi} n^{1/2} L(1, \chi_{-4n}) \prod_{p | a_1 a_2} 2(1+p)^{-1}.$$

Proof. (i) By Siegel's Hauptsatz and Lemma 1, we have:

$$r(n, \text{gen}\langle a_1^2, a_2^2, a_3^2\rangle) = \frac{2\pi n^{1/2}}{a_1 a_2 a_3} \partial_2(n, \langle a_1^2, a_2^2, a_3^2\rangle) \prod_{\substack{p \nmid n\\ p \neq 2}} (1-p^{-2})$$

$$\times \prod_{\substack{p \nmid n\\ p \neq 2}} \left(1-\left(\frac{-n}{p}\right)p^{-1}\right)^{-1} \prod_{\substack{p | n\\ p \nmid a_1 a_2 a_3}} (1-p^{-2}) \prod_{p | a_1 a_2 a_3} 2(1-p^{-1}).$$

So the first part of the proof follows from the observations that $\zeta(2)^{-1} = \prod_p (1-p^{-2})$ and that

$$\prod_{\substack{p \nmid n\\ p \neq 2}} \left(1-\left(\frac{-n}{p}\right)p^{-1}\right)^{-1} = \sum_{k \text{ odd}} \frac{\left(\frac{-n}{k}\right)}{k} = \sum_k \frac{\left(\frac{-4n}{k}\right)}{k} = L(1, \chi_{-4n}).$$

(ii) In this case $\partial_2(n, \langle a_1^2, a_2^2, a_3^2\rangle)$ can be easily calculated if we observe that

$$r_{2^{k+1}}(n, \langle a_1^2, a_2^2, a_3^2\rangle) = 2^2 r_{2^k}(n, \langle a_1^2, a_2^2, a_3^2\rangle), \quad \text{for } k \geq 3.$$

Using these formulae we immediately obtain

PROPOSITION 4. *Let $n = mt$. Then*

(i) *If n is odd,*

$$S_i'(n) = \varrho_i \sum_{(2)} (-1)^i \mu(a_1 a_2 a_3) \prod_{p | a_1 a_2 a_3} 2(1+p)^{-1},$$

for $i = 1, 2, 3$.

(ii) *If n is even,*

$$S'_1(n) = 1+S'_2(n)-S'_3(n),$$

$$S'_2(n) = 2\sum_{(4)} -\mu(a)\prod_{p|a} 2(1+p)^{-1}+S'_3(n),$$

$$S'_3(n) = \sum_{(3)} -\mu(2a_1 a_2) \prod_{p|a_1 a_2} 2(1+p)^{-1}.$$

Next we give the value of the main term.

THEOREM 1. *Let $n = mt$ be square-free, $n \not\equiv 7 \pmod 8$. Then*
(i) *If n is odd,*

$$G_1(n) = 1-3P_1(m)+3P_2(m)-P_3(m),$$

$$G_2(n) = 1-3P_2(m)+2P_3(m),$$

$$G_3(n) = 1-P_3(m).$$

(ii) *If n is even,*

$$G_1(n) = 1-2P_1(m)+P_2(m),$$

$$G_2(n) = 1-P_2(m),$$

$$G_3(n) = 1.$$

Here

$$P_j(m) = \prod_{i=1}^{r} \left(1-2j(1+p_i)^{-1}\right), \quad \text{for } j = 1, 2, 3.$$

Proof. (i) Let $x_i = 2(1+p_i)^{-1}$, $1 \leqslant i \leqslant r$, then

$$P_j = \prod_{i=1}^{r} (1-jx_i) = \prod_{k=0}^{r} (-j)^k \sigma_k(x_1, \ldots, x_r),$$

σ_k being the elementary symmetric polynomials of degree k in r variables. We have

$$1-3P_1+3P_2-P_3 = \prod_{k=3}^{r} (-1)^{k+1}(3-3\cdot 2^k+3^k)\sigma_k(x_1, \ldots, x_r).$$

Now we observe that each summand of $S'_3(n)$ is of the form

$$(-1)^{k+1} x_{i_1} \ldots x_{i_k} \quad (3 \leqslant k \leqslant r)$$

and that it appears in $S'_3(n)$ a number of times equal to

$$\sum_{\substack{k_i>0 \\ k_1+k_2+k_3=k}} \binom{k}{k_1}\binom{k-k_1}{k_2}\binom{k-k_1-k_2}{k_3} = \sum_{\substack{k_i>0 \\ k_1+k_2+k_3=k}} \frac{k!}{k_1!\,k_2!\,k_3!} = 3^k-3\cdot 2^k+3.$$

This shows that $S'_3(n) = 1-3P_1+3P_2-P_3$. Proceeding similarly we get $S'_2(n) = 3-6P_1+3P_2$ and $S'_1(n) = 3-P_1$. Recalling now the expressions of $G_i(n)$ in terms of $S'_i(n)$, we are done. Observe that if $5|n$, then $P_3(m) = 0$ and, consequently $G_3(n) = 1$.

(ii) In this case we have that $S'_3(n) = 1-2P_1+P_2$,

$$S'_2(n) = 2-2P_1, \quad S'_1(n) = 2-P_2.$$

Note that $G_i(n) = G_i(m)$ in all cases.

COROLLARY. *We have*
(i) $0 \leqslant G_1(n) \leqslant G_2(n) < G_3(n) = 1$, *if* g.c.d. $(n, 10) \neq 1$,
(ii) $0 \leqslant G_1(n) \leqslant G_2(n) \leqslant G_3(n) < 1$, *if* g.c.d. $(n, 10) = 1$.

Proof. From the definition it follows that $P_3 < P_2 < P_1$ and $P_j > 0$, for $j = 1, 2, 3$. Let us write $P_j = 1-y_j$, $j = 1, 2, 3$; then by induction on r we see that $y_3 \leqslant 2y_2-y_1$; $y_3 \geqslant 3(y_2-y_1)$, $y_2 \geqslant y_1$; $2y_1 \geqslant y_2$. Now, from these inequalities the assertion follows immediately.

3. The error term in the square-free case. We call error term in the determination of the level to the difference $g_i(n)-G_i(n)$ for $i = 1, 2, 3$.

Let $\theta(f, z)$ and $\theta(\operatorname{spn} f, z)$ be the theta series associated to f and $\operatorname{spn} f$ (spinorial genus of f). If $f = \langle a_1^2, a_2^2, a_3^2\rangle$ is a quadratic form with g.c.d. $(a_i, a_j) = 1$, for $i \neq j$, then $\theta(f, z)$ belongs to the space $M_0(3/2, 4a_1^2 a_2^2 a_3^2)$ of modular forms of weight 3/2 with respect to $\Gamma_0(4a_1^2 a_2^2 a_3^2)$.

LEMMA 2. *Let us write $n = mt$, as usual, and $f = \langle a_1^2, a_2^2, a_3^2\rangle$ with $a_i|m$, a_i square-free, for $i = 1, 2, 3$, and* g.c.d. $(a_i, a_j) = 1$, *for $i \neq j$. Then*
(i) $r(n, \operatorname{spn} f) = r(n, \operatorname{gen} f)$,
(ii) *The validity of Ramanujan–Petersson's conjecture for modular forms of weight 3/2 implies that for every $\varepsilon > 0$*

$$r(n, f)-r(n, \operatorname{gen} f) = O_{\varepsilon,m,f}(t^{1/4+\varepsilon}).$$

Proof. (i) It suffices to apply th. 4.6 of [4] that assures that for our forms $\operatorname{gen} f = \operatorname{spn} f$.

(ii) By [6] we have that $\theta(f, z)-\theta(\operatorname{spn} f, z)$ lies in $U^{\perp}$, where $U^{\perp}$ is the orthogonal complement, in the space of cusp forms $S_0(3/2, 4a_1^2 a_2^2 a_3^2)$, of the space U spanned by Shimura's theta functions (cf. [8]). Since the growth of the Fourier coefficients $a(n)$, n square-free, of a cusp form g lying in $U^{\perp}$ is predicted by the Ramanujan–Petersson's conjecture for weight 3/2, in the sense that

$$a(n) = O_{\varepsilon,g}(n^{1/4+\varepsilon}), \quad \text{for every } \varepsilon > 0,$$

it suffices to apply this claim to our forms. Obviously, the final O-constant will be independent of t.

Under the assumption of Ramanujan–Petersson's conjecture for weight 3/2 we can state

THEOREM 2. *Let $n = mt$ be square-free, $n \not\equiv 7 \pmod 8$. For every $\varepsilon > 0$, we have*

$$g_i(n) - G_i(n) = O_{\varepsilon,m}(t^{-1/4+\varepsilon}), \quad \text{for } i = 1, 2, 3.$$

Proof. Let c_1 be the O-constant appearing in Lemma 2 and set

$$c_2 = c_2(\varepsilon, m) := \sum_{a_j | m} c_1(\varepsilon/2, m, \langle a_1^2, a_2^2, a_3^2 \rangle),$$

where obviously the a_j's considered are exactly the ones appearing in the definition of either g_i or G_i as alternating sums. Then, we may write, for every $\varepsilon > 0$,

$$|g_i(n) - G_i(n)| \leqslant c_2 \cdot t^{1/4+\varepsilon} \cdot r(n, I_3)^{-1}.$$

As, on the other hand, for every $\varepsilon > 0$, we have, with our hypothesis, that

$$r(n, I_3)^{-1} = O_\varepsilon(n^{1/2+\varepsilon/2})$$

(cf. [10]), we obtain

$$|g_i(n) - G_i(n)| \leqslant c_4 \cdot t^{-1/4+\varepsilon},$$

where $c_4 = c_4(\varepsilon, m) := c_2 \cdot c_3$, and c_3 being the O-constant appearing in $r(n, I_3)^{-1}$.

4. Asymptotic behaviour of $l(n)$. Taking into account the bound of the main term given in the Corollary of Theorem 1 together with the growth of the error term given in Theorem 2, we can state the following

THEOREM 3. *Let $n = mt$ be square-free, $n \not\equiv 7 \pmod 8$. The validity of Ramanujan–Petersson's conjecture for weight 3/2 implies that there exists a constant $c_5 = c_5(m)$ such that*

(i) $g_2(n) < 1$, *if* g.c.d. $(n, 10) \neq 1$,
(ii) $g_3(n) < 1$, *if* g.c.d. $(n, 10) = 1$,

for every $t > c_5$.

For each $m = 2^\alpha p_1 \ldots p_r$, $\alpha = 0$ or 1, $p_i \equiv 1 \pmod 4$, $i = 1, \ldots, r$, we introduce the family

$$F(m) := \{n \not\equiv 7 \pmod 8 \mid n = mt,\ t \text{ square-free containing no prime factors} \equiv 1 \pmod 4 \text{ in its factorization}\},$$

and the constant

$$c(m) := mc_5(m).$$

Using Proposition 1, Theorem 3 can be reformulated in terms of levels as follows.

THEOREM 3′. *Let $n \not\equiv 7 \pmod 8$ be a square-free positive integer and let $F(m)$ be the family to which n belongs. The validity of Ramanujan–Petersson's conjecture for weight 3/2 implies that if $n > c(m)$, then:*

(i) $l(n) = 2$, *if* g.c.d. $(n, 10) \neq 1$,
(ii) $l(n) = 3$, *if* g.c.d. $(n, 10) = 1$.

The following table, computed by P. Llorente, shows that the constants $c(m)$ are, in general, non-trivial. All positive square-free integers $n \leqslant 10^5$ not contained in the table have the level predicted in the Corollary of Theorem 1.

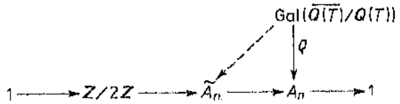
Table

$F(m)$	$n = 2^\alpha p_1 \ldots p_r q_1 \ldots q_s$	$l(n)$	$c(m) \geqslant$
$F(13)$	13	2	403
	$403 = 13 \cdot 31$	2	
$F(10)$	$30 = 2 \cdot 5 \cdot 3$	1	27190
	$70 = 2 \cdot 5 \cdot 7$	1	
	$210 = 2 \cdot 5 \cdot 3 \cdot 7$	1	
	$310 = 2 \cdot 5 \cdot 31$	1	
	$330 = 2 \cdot 5 \cdot 3 \cdot 11$	1	
	$430 = 2 \cdot 5 \cdot 43$	1	
	$670 = 2 \cdot 5 \cdot 67$	1	
	$790 = 2 \cdot 5 \cdot 79$	1	
	$1330 = 2 \cdot 5 \cdot 7 \cdot 19$	1	
	$2170 = 2 \cdot 5 \cdot 7 \cdot 31$	1	
	$2230 = 2 \cdot 5 \cdot 223$	1	
	$2530 = 2 \cdot 5 \cdot 11 \cdot 23$	1	
	$3070 = 2 \cdot 5 \cdot 307$	1	
	$27190 = 2 \cdot 5 \cdot 2719$	1	
$F(37)$	37	2	37
$F(13 \cdot 61)$	$793 = 13 \cdot 61$	2	793
$F(2 \cdot 5 \cdot 29)$	$870 = 2 \cdot 5 \cdot 29 \cdot 3$	1	870
$F(2 \cdot 5 \cdot 73)$	$2190 = 2 \cdot 5 \cdot 73 \cdot 3$	1	2190
$F(2 \cdot 5 \cdot 17)$	$3910 = 2 \cdot 5 \cdot 17 \cdot 23$	1	3910
$F(2 \cdot 5 \cdot 97)$	$6790 = 2 \cdot 5 \cdot 97 \cdot 7$	1	6790
$F(2 \cdot 5 \cdot 13 \cdot 41)$	$15990 = 2 \cdot 5 \cdot 13 \cdot 41 \cdot 3$	1	15990

Finally, we give an application which, in fact, motivated the study of the preceding problem.

COROLLARY. *Let $n = mt$ be square-free, $n \equiv 3 \pmod 8$, $n \not\equiv 0 \pmod 5$ and $n > c(m)$. Then every central extension of the alternating group A_n can be realized as a Galois group over $\mathbf{Q}$.*

Proof. Assuming the validity of Ramanujan–Petersson's conjecture for weight 3/2, we will get that all the integers above have level 3. This implies, as is shown in [11], (see also [7]), the existence of a continuous surjective representation $\varrho\colon \mathrm{Gal}(\overline{Q(T)}/Q(T)) \to A_n$ with a trivial second Stiefel–Whitney class $\varrho^* w_2(\xi_n) \in H^2(\mathrm{Gal}(\overline{Q(T)}/Q(T)), \boldsymbol{Z}/2\boldsymbol{Z})$. Here ξ_n denotes the real bundle over BA_n associated to the standard representation of the alternating group A_n into $SO_n(\boldsymbol{R})$. Since $\varrho^* w^2(A_n)$ can be viewed as the obstruction to the embedding problem given by the diagram



where $\tilde{A}_n$ denotes the universal central extension of A_n, the result follows.

References

[1] A. Arenas, *Un problema aritmético sobre las sumas de tres cuadrados*, Tesis doctoral. Univ. de Barcelona, 1985.
[2] A. Arenas and P. Bayer, *Arithmetic behaviour of the sums of three squares*, J. Number Theory 27 (1987), 273–284.
[3] L. E. Dickson, *History of the theory of numbers*, vol. II. Chelsea Pub. Comp., 1971.
[4] A. J. Earnest and J. S. Hsia, *Spinor norms of local integral rotations II*, Pacific J. Math. 61 (1975), 71–86.
[5] C. F. Gauss, *Disquisitiones Arithmeticae*, Lipsiae, 1810. [English translation: Arthur A. Clarke, 1966, New Haven: Yale Univ. Press].
[6] R. Schulze-Pillot, *Thetareihen positiv definiter quadratischer Formen*, Invent. Math. 75 (1984), 283–299.
[7] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (4) (1984), 651–676.
[8] G. Shimura, *On modular forms of half integral weight*, Ann. of Math. 97 (1973), 440–481.
[9] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, ibid. 36 (1935), 527–606. Gesammelte Abhand., Band 1, Springer, 1966.
[10] — *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86. Gesammelte Abhand., Band 1, Springer, 1966.
[11] N. Vila, *On central extensions of* A_n *as a Galois group over* $\boldsymbol{Q}$, Arch. Math. 44 (1985), 424–437.

FACULTAT DE MATEMÀTIQUES
DPT. D'ÀLGEBRA I FONAMENTS
UNIVERSITAT DE BARCELONA
Gran Via de les Corts Catalanes 585
08007 Barcelona, Spain

Received on 17.6.1986
and in revised form on 5.2.1987 (1652)

ACTA ARITHMETICA
LI (1988)

Binäre quadratische Formen und Diederkörper

von

FRANZ HALTER-KOCH (Graz)

Gegenstand dieser Arbeit ist die Darstellung von Primzahlen durch ganzzahlige binäre quadratische Formen. Die Gauß'sche Theorie der Geschlechter gestattet es, zu entscheiden, ob eine Primzahl durch ein Geschlecht quadratischer Formen dargestellt wird oder nicht, aber sie erlaubt im allgemeinen keine Aussagen über die Darstellung durch individuelle Formen.

Die binären quadratischen Formen fester Diskriminante bilden bezüglich der Komposition eine zur Ringklassengruppe dieser Diskriminante isomorphe Gruppe, und jeder Satz über die Darstellung von Primzahlen durch eine Form dieser Diskriminante ist ein Satz über das Zerlegungsverhalten dieser Primzahl im Ringklassenkörper; umgekehrt ist auch jedes Zerlegungsgesetz für den Ringklassenkörper ein Darstellungssatz durch binäre quadratische Formen (auf Grund des Artin-Isomorphismus). Kann man nun auf andere als auf klassenkörpertheoretische Weise (etwa mittels einer Radikalerzeugung) ein Zerlegungsgesetz für den Ringklassenkörper herleiten, so hat man damit einen Darstellungssatz für Primzahlen durch binäre quadratische Formen hergeleitet. Auf diesem Prinzip beruhen viele der in den letzten Jahren publizierten Potenzrestkriterien für quadratische Einheiten, welche man auch als Darstellungssätze für Primzahlpotenzen durch binäre quadratische Formen deuten kann ([21], [15], [25], [14], [26], [12], [13]).

Verwendet man an Stelle des vollen Ringklassenkörpers nur einen Teilkörper desselben, so erhält man nicht mehr Darstellungssätze für individuelle Formen, aber doch noch Darstellungssätze für gewisse Mengen von Formenklassen, welche im Spezialfall absolut-abelscher Teilkörper gerade die Geschlechter sind. Eine in diesem Zusammenhang bereits mehrfach untersuchte Körperklasse ist die der Diederkörper 8. Grades ([21], [15], [20], [22]), da deren Radikalerzeugung leicht zu überblicken ist. Die daraus resultierenden Darstellungssätze für Primzahlen durch binäre quadratische Formen bestimmen die Klasse darstellender Formen bis auf 4. Potenzen in der Kompositionsklassengruppe ihrer Diskriminante.

In den zitierten Arbeiten wurden die Diederkörper 8. Grades immer nur in solchen Fällen verwendet, in denen die zugehörige Ringklassengruppe nur