Proc. Indian Acad. Sci. (Math. Sci.), Vol. 95, No. 2, December 1986, pp. 127–132.

Computing the number of ways of representing primes by a norm form

RAJAT TANDON
School of Mathematics, University of Hyderabad, Hyderabad 500 134, India

MS received 11 September 1986; revised 12 February 1987

Abstract. Formulae for the number of different integral solutions of $a^2+b^2+c^2+d^2+ac+bd=p$ are given where p is a prime and the solution satisfies certain natural congruence conditions. Similar formulae are given for the case of the quadratic form $a^2+b^2+2c^2+2d^2+ac+bd$.

Keywords. Integral solutions; natural congruence.

The purpose of this note is to show how the results in [6] may be extended to the norm forms of other definite quaternion algebras ramifying at a single prime. The crucial extra information required is provided by [5]. The character formulas given in [5] enable us to "match" the representations of the idele group of the quaternion algebra and representations of $GL(2, \mathbf{A_Q})$ with the same L-functions. The method is exemplified by considering definite quaternion algebras ramifying only at 3 and at 7. In determining the various representations, this paper incorporates an idea mentioned in [6] but not used. The notation used is of that in [6].

We will describe our quaternion algebra D in standard form. D is generated as a vector space over $\mathbf{Q}$ by $1, i, j, ij$ where $j^2=-1$, $i^2=-3$ and $ij=-ji$. This has one maximal order $\mathbf{Z}+\mathbf{Z}_j+\mathbf{Z}[\frac{1}{2}(1+i)]+\mathbf{Z}[\frac{1}{2}(1+i)]j$ (see [5]). The class number is 1. The order has twelve units $\{\pm 1, \pm j, \frac{1}{2}(\pm 1+i), \frac{1}{2}(\pm j \pm ij)\} = U$. The norm of any element of the form $a+bj+c[(1+i)/2]+[d(1+i)j]/2$ is $a^2+b^2+c^2+d^2+ac+bd$, denoted by $N(a,b,c,d)$.

Suppose p is an odd prime. Then it has been known for a long time that the number of integral solutions of $N(a,b,c,d)=p$ is $12(p+1)$ (see [2]).

We denote by D_A the adele ring of D and by D_v the completion of D at v (v is a place). U_v denotes the corresponding group of units in the ring of integers or the maximal compact subgroup of $GL(2, \mathbf{Q}_v)$ depending on whether D is ramified at v or not. Since D has class number one, we have

$$D_{\mathbf{A}}^* = D^* D_{\mathbf{R}}^* \prod_{v<\infty} U_v.$$

Suppose $U_3 = \cup a_i(1+P_3^2)$ where P_3 is the maximal ideal in the ring of integers in D_3.

Then $D_{\mathbf{A}}^* = \cup D^* g_i D_{\mathbf{R}}^* \prod_{v<\infty} U_v'$ where $U_v' = U_v$ if $v \neq 3$ and $U_v' = 1+P_3^2$

if $v = 3$ and g_i is the idele which has a_i in the third place and ones everywhere else.

In fact if we factor out units, then

$$D_{\mathbf{A}}^* = \bigcup_{i=1}^{6} D^* g_i D_{\mathbf{R}}^* \prod_{v<\infty} U_v',$$

where $g_i = (1, 1, b_i, 1, \ldots)$ and the b_i's are coset representative such that $U_3 = \bigcup_{i=1}^{6} U(1+P_3^2)b_i$.

Denoted by N_{b_k}, the number of integral solutions of $N(a,b,c,d) = p$ such that

$$a + bj + \tfrac{1}{2}[c(1+i)] + \tfrac{1}{2}[d(1+i)j] \in b_k(1+P_3^2).$$

In $\mathbf{Q}_3$, -2 has a square root which lies in $1+(3)$. We denote this square root by $\sqrt{-2}$. Let $u = (1+j)/\sqrt{-2}$, $v = 1+iu$. Then the b_k's may be taken to be $1, u, v, v^2, uv, uv^2$. Then from Jacquet-Langlands Theory, we get the following:

THEOREM 1. If $p \equiv -1 \pmod 3$, then $N_1 = N_v = N_{v^2} = 0$,

$$N_u = N_{uv} = N_{uv^2} = \tfrac{1}{3}(p+1).$$

If $p \equiv 1 \pmod 3$, then $N_u = N_{uv} = N_{uv^2} = 0$, $N_1 = \frac{1}{3}[p+1+2(2x-y)]$, $N_v = N_{v^2} = \frac{1}{3}[p+1-(2x-y)]$ where (x,y) is a solution of $x^2 - xy + y^2 = p$ with $x \equiv 1 \pmod 3$, $y \equiv 0 \pmod 3$.

Remark. The fact that an integral solution of $N(a,b,c,d) = p$ contributes to N_{b_k} simply expresses some congruence condition on the solution. For instance a solution (a,b,c,d) contributes to N_1 simply means that $a + bj + \frac{1}{2}[c(1+i)] + \frac{1}{2}[d(1+i)j]$ is in $1+P_3^2$ or 9 divides the norm of $a - 1 + bj + \frac{1}{2}[c(1+i)] + \frac{1}{2}[d(1+i)j]$. This means that

$$9 \mid (a-1)^2 + b^2 + c^2 + d^2 + ac + bd - c.$$

Since $a^2 + b^2 + c^2 + d^2 + ac + bd = p$ we get the condition that $9 \mid p + 1 - 2a - c$.

Proof of theorem. Let $E = Q(\sqrt{-3})$. E has class number 1 so

$$E_A^* = E^* \mathbf{C}^* \prod_{v<\infty} \theta_v^*$$

where θ_v is the ring of integers in E_v. In fact because of six units in E we have

$$E_A^* = E^* \mathbf{C}^* U' \text{ where } U' = \theta_2^*(1+3\theta_3) \prod_{v \neq 2,3} \theta_v^*$$

define a Grossencharacter x on E_A^* so that it is trivial on E^* and U' and maps $z \to (z\bar{z})^{-1/2}\bar{z}$ for $z \in \mathbf{C}$. Then the representation (see [3]) π_∞ of $GL(2,\mathbf{R})$ is just $\sigma(|\,|^{1/2}, |\,|^{-1/2})$ (the irreducible subrepresentation obtained by inducing from the character

$$\begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} \to |a_1|^{1/2} |a_2|^{-1/2}.$$

The trivial representation of $D_{\mathbf{R}}^*$ is associated to $\sigma(|\,|^{1/2}, |\,|^{-1/2})$ by the Weil representation.

The character χ_2 of $\mathbf{Q}_2$ is unramified. Moreover $\chi_2(2) = \chi_2(2(-\frac{1}{2}, -1, -\frac{1}{2}, -\frac{1}{2}, \ldots)) = -1$. Hence $\chi_2 = \eta_2 \cdot N_{E_2/\mathbf{Q}_2}$ where η_2 is an unramified character of $\mathbf{Q}_2^*$ and $N_{E_2/\mathbf{Q}_2}$ is the norm map from E_2 to $\mathbf{Q}_2$. Hence π_{χ_∞} is the representation of $GL_2(\mathbf{Q}_2)$ obtained by inducing from two unramified characters applied to the upper triangular group and so is of class 1 (see [1]). Hence there exists a vector e_2 in the space $\mathfrak{B}_2$ on which π_{χ_2} acts which is fixed by $GL_2(\mathbf{Z}_2)$. Moreover 2 remains a prime in E_2 so that $L_2(s,\chi)$ is of the form $1/[1-\chi_2(2)2^{-2s}]$. Let $a_2 = 0$. Similarly if $p \equiv -1(3)$, then p remains a prime in E_p. We let $a_p = 0$. χ_p is unramified, $\chi_p(p) = -1$ so $\chi_p = \eta_p \cdot N_{E_p/\mathbf{Q}_p}$, η_p being unramified. Again there exists a vector e_p in the space $\mathfrak{B}_p$ on which π_{χ_p} acts, fixed by $GL_2(\mathbf{Z}_p)$. If $p \equiv 1(3)$, $p\theta_E = (\mathfrak{p}\bar{\mathfrak{p}})$ where $\mathfrak{p}$, $\bar{\mathfrak{p}}$ are two distinct conjugate ideals in the ring of integers in E. If $\mathfrak{p} = (x+\zeta y)$ where $\zeta = \frac{1}{2}(-1+\sqrt{-3})$, then $\bar{\mathfrak{p}} = (x+\bar{\zeta}y)$ and $p = x^2 - xy + y^2$. Moreover if we choose (x,y) such that $x \equiv 1 \pmod 3$ and $y \equiv 0 \pmod 3$, then both $x+\zeta y$ and $x+\bar{\zeta}y$ when viewed as elements in E_3 lie in $1+3\theta_3$. In this case $\pi_{\chi_p} = \pi(\chi_{\mathfrak{p}}, \chi_{\bar{\mathfrak{p}}})$. $\chi_{\mathfrak{p}}$, $\chi_{\bar{\mathfrak{p}}}$ are unramified so the representation is class 1. Moreover

$$L_p(s,\chi) = 1/[1-\chi_{\mathfrak{p}}(\mathfrak{p})p^{-s}]\,1/[1-\chi_{\bar{\mathfrak{p}}}(\bar{\mathfrak{p}})p^{-s}]$$

$$= 1/[1-(\chi_{\mathfrak{p}}(\mathfrak{p})+\chi_{\bar{\mathfrak{p}}}(\bar{\mathfrak{p}}))p^{-s}+\chi_{\mathfrak{p}}(\mathfrak{p})\chi_{\bar{\mathfrak{p}}}(\bar{\mathfrak{p}})p^{-2s}]$$

$$\chi_{\mathfrak{p}}(\mathfrak{p})+\chi_{\bar{\mathfrak{p}}}(\bar{\mathfrak{p}}) = p^{-1/2}(2x-y).$$

Put $a_p = 2x-y$. Finally we have $\chi_3(\sqrt{-3}) = i$, $\chi_3(-\zeta) = -\zeta$ and χ_3 is trivial on $1+3\theta_3$. The second relationship tells us that χ_3 is not of the form $\eta_3 \cdot N_{E_3/\mathbf{Q}_3}$. Hence π_{χ_3} is supercuspidal. Let l be the smallest integer greater than zero such that χ_3 is trivial on $E_3' \cap (1+(\sqrt{-3})^{2l+1}\theta_3)$, E_3' being the norm one group. Here $l = 1$. Let π_3' be a representation of D_3^* such that the associated Weil representation of $GL_2(\mathbf{Q}_3)$ is π_{χ_3}. Then Proposition 3 of [5] tells us that dim $\pi_3' = (q+1)q^{l-1} = 4$ where q is the number of elements in the residue of $\mathbf{Q}_3$. Moreover, if χ_3' is the character of π_3' and α is that of π_{χ_3}, then $-\chi_3' =$ character of π_{χ_3} where this is defined. But by [5]

$$\alpha(1-\sqrt{-3}) = \chi_3(\delta)\,\mathrm{sgn}_{E_3/\mathbf{Q}_3}(\delta) \sum_{\substack{x \in U^0/U' \\ x \neq g_1, \bar{g}_1}} \chi_3(x)\,\mathrm{sgn}_{E_3/\mathbf{Q}_3}(\mathrm{tr}(g_1 x))$$

where $\mathrm{sgn}_{E_3/\mathbf{Q}_3}$ is the character of $\mathbf{Q}_3$ determined by the quadratic extension E_3, $\delta \in \mathbf{Q}_3$ is such that $(1-\sqrt{-3})/\delta$ has norm 1 and trace $(1-\sqrt{-3})/\delta \equiv 2 \pmod 3$, $g_1 = (1-\sqrt{-3})/\delta$. Here, $\mathbf{Q}_3(\sqrt{-3})$ has been imbedded in $GL_2(\mathbf{Q}_3)$ and the elements of $\mathbf{Q}_3(\sqrt{-3})$ identified with their images. Finally $U^i = E_3' \cap (1+\sqrt{-3})^{2i+1}\theta_3)$. Now

$$E_3' \cap ((1+\sqrt{-3})^3\theta_3) = E_3' \cap ((1+\sqrt{-3})^2\theta_3).$$

Moreover by Serre [4] we can see that

$$\frac{E_3' \cap (1+\sqrt{-3}\theta_3)}{E_3' \cap (1+\sqrt{-3})^2\theta_3} \cong \frac{1+\sqrt{-3}\theta_3}{1+3\theta_3}$$

and so has 3 elements, 1, g_1, $\bar{g}_1$. Hence

$$\alpha(1-\sqrt{-3}) = \chi_3(-2)\,\mathrm{sgn}_{E_3/\mathbf{Q}_3}(-2)\,\mathrm{sgn}_{E_3/\mathbf{Q}_3}\left(\mathrm{tr}\left(\frac{1-\sqrt{-3}}{-2}-1\right)\right) = -1. \quad (*)$$

The central character of π_3' is the same as that of π_{χ_3} which is $\chi_3 \cdot \mathrm{sgn}_{E_3/\mathbf{Q}_3}$. Hence $\pi_3'(-1) = \mathrm{I}$. Hence π_3' is a four-dimensional representation of $U_3/[\langle \pm 1\rangle(1+P_3^2)]$. This is a group of order 36 which has the following presentation: $\langle a, b, c;\ b^3 = 1,\ c^3 = 1,\ a^4 = 1,\ aba^{-1} = c,\ bc = cb,\ aca^{-1} = b^2\rangle$. It has 4 one-dimensional representations and two irreducible four-dimensional representations. If ρ_1 denotes the character of the subgroup generated by b and c which map $b \mapsto \omega$, $c \mapsto 1$ (ω a complex primitive cube root of 1) and ρ_2 the character which maps $b \mapsto \omega$, $c \mapsto \omega$, then the induced representations are inequivalent, irreducible four-dimensional representations. Denote their characters by χ and χ'. Then $\chi(b^2) = 1$, $\chi(bc) = -2$ and $\chi'(b^2) = -2$, $\chi'(bc) = 1$. Now (*) tells us that $\chi(b^2) = -1$. Hence $\chi_3' = \chi$. Here we have identified a, b, c with the cosets of u, $1+i$ and $1+ji$ respectively.

If V is the space on which π_3' acts, then

$$\pi' = \pi_{\chi_3} \otimes \pi_2' \otimes \bigotimes_{p>3} \pi_p \text{ acts on } \mathfrak{B}_2 \otimes V \otimes \bigotimes_{p>3} \mathfrak{B}_p$$

(restricted tensor product). However, by Jacquet-Langlands, π' occurs in the space $\mathscr{A}'$ of automorphic forms for $D_{\mathbf{A}}$ so there is an intertwining operator T: $\mathfrak{B}_2 \otimes V \otimes \bigotimes_{p>3} \mathfrak{B}_p \mapsto \mathscr{A}'$ which commutes with the $D_{\mathbf{A}}^*$ action. The image of the vectors $e_2 \otimes v \otimes \bigotimes_{p>3} e_p$, $v \in V$ lie in the space of functions on $D_{\mathbf{A}}^*$ which are left invariant by D^* and right invariant by $D_{\mathbf{R}}^* U_2(1+p_3^2) \prod_{p>3} U_p$. This space $\mathscr{F}$, we have seen in the beginning, is six-dimensional and contains a four-dimensional subspace on which the right regular action, restricted to D_3^*, is equivalent to π_3'. Let ϕ_x denote the characteristic function of the double coset

$$D^*(1,\ 1,\ x^{-1},\ 1, \ldots) D_{\mathbf{R}}^* \coprod_{v<\infty} U_v',\ x \in U_3.$$

Then $\mathscr{F}$ is generated by $\langle \phi_1, \phi_u, \phi_v, \phi_{v^2}, \phi_{uv}, \phi_{uv^2}\rangle$, u, v being defined as before. Then the four-dimensional subspace in $\mathscr{A}'$ is generated by

$$\langle \phi_1 + \zeta\phi_v + \zeta^2\phi_{v^2},\ \phi_1 + \zeta^2\phi_v + \zeta\phi_{v^2},\ \phi_u + \zeta\phi_{uv} + \zeta^2\phi_{uv^2},$$
$$\phi_u + \zeta^2\phi_{uv} + \zeta\phi_{uv^2}\rangle.$$

If p is an odd prime, then the corresponding Hecke operator commutes with the right regular action of U_3 on this space. Since this action is irreducible the Hecke operators act as scalars. The given functions are, therefore, eigenfunctions for the

T_p with eigenvalues a_p. By Jacquet-Langlands $a_p = a'_p$. We need to compute a'_p. We have

$$a'_p(\phi_1 + \zeta\phi_\nu + \zeta^2\phi_{\nu^2}) = T_p(\phi_1 + \zeta\phi_\nu + \zeta^2\phi_{\nu^2}).$$

Evaluating at 1 we get

$$\begin{aligned} a'_p &= [T_p(\phi_1 + \zeta\phi_\nu + \zeta^2\phi_{\nu^2})](1) \\ &= \sum_{x \in \mathbf{Z}/p\mathbf{Z}} \phi_1\left[\begin{pmatrix} p & x \\ 0 & 1 \end{pmatrix}\right] + \phi_1\left[\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\right] \\ &\quad + \zeta \sum_{x \in \mathbf{Z}/p\mathbf{Z}} \phi_\nu\left[\begin{pmatrix} p & x \\ 0 & 1 \end{pmatrix}\right] \\ &\quad + \zeta\phi_\nu\left[\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\right] + \zeta^2 \sum_{x \in \mathbf{Z}/p\mathbf{Z}} \phi_{\nu^2}\left[\begin{pmatrix} p & x \\ 0 & 1 \end{pmatrix}\right] + \zeta^2\phi_{\nu^2}\left[\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\right] \\ &= N_1 + \zeta^2 N_\nu + \zeta N_{\nu^2}; \text{ see [6].} \end{aligned}$$

Similarly evaluating at ν^2 we get $a'_p = N_1 + \zeta N_\nu + \zeta^2 N_{\nu^2}$.
Evaluating at u, $u\nu$ we get $0 = N_u + \zeta N_{u\nu} + \zeta^2 N_{u\nu^2} = N_u + \zeta^2 N_{u\nu} + \zeta N_{u\nu^2}$.
Suppose now $p \equiv -1(3)$. Then $a_p = a'_p = 0$ so we get

$$N_1 = N_\nu = N_{\nu^2},\ N_u = N_{u\nu} = N_{u\nu^2}.$$

Moreover, we claim that $N_1 = 0$. For if the solution (a, b, c, d) contributes to N_1, then $9/p + 1 - 2a - c$. Hence $3 \mid a - c$. But

$$\begin{aligned} p = a^2 + b^2 + c^2 + d^2 + ac + bd &= (a-c)^2 + (b-d)^2 + 3ac + 3bd \\ &\equiv (b-d)^2 \pmod 3. \end{aligned}$$

Therefore $(p/3) = 1$ which is a contradiction so $N_1 = 0$. Since the sum of the N's is $p+1$, we get

$$N_u = \tfrac{1}{3}(p+1).$$

On the other hand suppose $p \equiv 1 \pmod 3$, x, y being as before we get

$$\begin{aligned} 2x - y &= N_1 + \zeta^2 N_\nu + \zeta N_{\nu^2} = N_1 + \zeta N_\nu + \zeta^2 N_{u\nu^2} \\ 0 &= N_u + \zeta^2 N_{u\nu} + \zeta N_{u\nu^2} = N_u + \zeta N_{u\nu} + \zeta^2 N_{u\nu^2}, \end{aligned}$$

so $N_u = N_{u\nu} = N_{u\nu^2}$, $N_\nu = N_{\nu^2}$ and $2x - y = N_1 - N_\nu$. We claim that N_u is zero. For if (a, b, c, d) is a solution contributing towards N_u, then 9 divides $p + 2 - 2a - 2b - c - d$. Hence 3 divides $a + b - c - d$, i.e., $(a - c) = d - b \pmod 3$. But $p = (a-c)^2 + (d-b)^2 + 3ac + 3bd \equiv 2(a-c)^2 \pmod 3$ which is a contradiction. Hence $N_1 + 2N_\nu = p + 1$ and $N_1 - N_\nu = 2x - y$. This gives the required solution and completes the proof of the theorem.

The same argument may be repeated for definite quaternion algebras with discriminant 7, the essential conditions involved, namely that the class numbers of $\mathbf{Q}(\sqrt{-7})$ and the quaternion algebra are one, being the same. Such a quaternion algebra is generated over $\mathbf{Q}$ by $1, i, j, ij$ such that $i^2 = -7$ and $j^2 = -1$. The unique

maximal order is $Z+Zj+\frac{1}{2}[Z(1+i)]+\frac{1}{2}[Z(1+i)j]$ and the associated norm form $N(a, b, c, d) = a^2+b^2+2c^2+2d^2+ac+bd$. If U be the units in the maximal order and "a", a 48th root of unity in $Q_7(\sqrt{-7}) = Q_7(i)$ then $U_7 = \bigcup_{i=0}^{11} U\alpha^i(1+P_7)$. We denote as before by N_i the number of integral solutions of $N(a, b, c, d) = p$ such that $a+bj+\frac{1}{2}[c(1+i)]+\frac{1}{2}[d(1+i)j]$ is in $a^i(1+P_7)$. Making a closer use of the character tables in [5] we get

THEOREM 2. If $(p/7) = -1$, then $N_i = 0$ if i is even and $N_i = \frac{1}{2}(p+1)$ if i is odd.

If $(p/7) = 1$, then $N_i = 0$ if i is odd, $N_i = \frac{1}{2}[p+1+(2x+y)]$ if 4 divides i and $N_i = \frac{1}{2}[p+1-(2x+y)$ if i is even but not divisible by 4; here (x, y) is any solution of $x^2+xy+2y^2 = p$ such that $(2x+y)/p = 1$.

The notation $(/p)$ is used for the Legendre symbol.

References

[1] Gelbart S, Automorphic forms on adele groups, *Ann. Math. Stud.* No. 83 1975 (Princeton: University Press)

[2] Hecke E, Werke, *Vandenhoeck and Ruprecht*, Gottingen 1959

[3] Jacqet H and Langlands R P, Automorphic forms on $GL(2)$, *Lecture notes in mathematics* 114 (Berlin: Springer Verlag)

[4] Serre J P, *Corps Locaux* (Paris: Hermann)

[5] Shimizu H, Some examples of new forms, *J. Fac. Sci. Univ. Tokyo Sec. IA* **24** 97–113

[6] Tandon R, The Hecke theory of $GL(2)$ and quadratic forms, *J. Indian Math. Soc.* **40** (1976) 87–122