IJMMS 25:5 (2001) 289–292
PII. S0161171201005294
http://ijmms.hindawi.com

KAPLANSKY'S TERNARY QUADRATIC FORM

JAMES KELLEY

(Received 26 February 1998 and in revised form 17 May 2000)

ABSTRACT. This paper proves that if N is a nonnegative eligible integer, coprime to 7, which is not of the form $x^2+y^2+7z^2$, then N is square-free. The proof is modelled on that of a similar theorem by Ono and Soundararajan, in which relations between the number of representations of an integer np^2 by two quadratic forms in the same genus, the pth coefficient of an L-function of a suitable elliptic curve, and the class number formula prove the theorem for large primes, leaving 3 cases which are easily numerically verified.

2000 Mathematics Subject Classification. Primary 11E25.

1. Introduction. A *quadratic form* is a homogeneous polynomial of degree 2 in several variables. It is useful to consider the symmetric n-by-n matrix, A, associated with a *quadratic form* in n variables, that is, $f(x_1,x_2,\ldots,x_n)=\mathbf{x}^\top A\mathbf{x}$, where $\mathbf{x}=(x_1,x_2,\ldots,x_n)$. As such, we define the *automorphs* of f to be the matrices, T, in $\mathrm{SL}_n(\mathbb{Z})$ such that $T^{-1}AT=A$. We say that a *quadratic form* in n variables, f *represents* t if there exists an $\mathbf{x}\in\mathbb{Z}^n$ such that $t=\mathbf{x}^\top A\mathbf{x}$. We call $\mathbf{x}$ *primitive* if $\gcd(x_1,x_2,\ldots,x_n)=1$. Automorphs are significant because $\mathbf{x}^\top A\mathbf{x}=n$ implies that $T\mathbf{x}$ and $T^{-1}\mathbf{x}$ also satisfy this equation.

We say a nonnegative integer t is *eligible* with respect to a form f if there are no modularity conditions preventing f from representing n. Note that this does not imply that f represents n.

In [5], Kaplansky studied the quadratic form $\phi_1=x^2+y^2+7z^2$, and proved that certain subsets of the eligible numbers are always represented. First, we have to know what the eligible numbers are. Basic number theory shows that they are the nonnegative integers not of the form $7^{2m+1}r$, where r is not a quadratic residue modulo 7, that is, $r\equiv 3$, 5, or 6 (mod 7). Two of the subsets examined by Kaplansky, the set of eligible numbers congruent to 1 (mod 4) and the set of numbers congruent to 2 (mod 3) which are not the product of 14 and a perfect square, are not directly related to the results in this paper. However, Kaplansky also showed that all eligible integers divisible by 4 or 9 can be represented by ϕ_1, which brings up the question of whether this pattern holds true for other perfect squares. In general, we see that $k=f(x_1,x_2,\ldots,x_n)$ implies that $kp^2=f(px_1,px_2,\ldots,px_n)$, but knowing that kp^2 is represented by f does not imply that k is represented by f. So, for a given prime p, does ϕ_1 represent all eligible integers divisible by p^2? In almost all cases, we can answer the question affirmatively by proving the following theorem.

THEOREM 1.1. *If N is coprime to 7 and not of the form $x^2+y^2+7z^2$ with $x,y,z\in(\mathbb{Z})$, then N is square-free.*

2. Preliminary remarks. The form ϕ_1 is in a genus of two forms, the other one being $\phi_2 = x^2+2y^2+2yz+4z^2$. These two forms have the same set of eligible integers, and, as is the case with all genera of ternary quadratic forms, each eligible integer is represented by at least one of them. Let A_1 and A_2 denote the matrices representing the forms ϕ_1 and ϕ_2, respectively. We see that $A_1 = \left[\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&7\end{smallmatrix}\right]$ has eight automorphs: $\left[\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1&0&0\\0&-1&0\\0&0&-1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0&1&0\\1&0&0\\0&0&-1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0&1&0\\-1&0&0\\0&0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix} -1&0&0\\0&1&0\\0&0&-1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix} -1&0&0\\0&-1&0\\0&0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0&-1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0&-1&0\\-1&0&0\\0&0&-1\end{smallmatrix}\right]$, while $A_2 = \left[\begin{smallmatrix} 1&0&0\\0&2&1\\0&1&4\end{smallmatrix}\right]$ has two: $\left[\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1&0&0\\0&-1&0\\0&0&-1\end{smallmatrix}\right]$.

We say that two representations of an integer by a form are essentially distinct if one cannot be written as the product of the other and an automorph of that form. Let $s_1(n)$ and $s_2(n)$ be the number of primitive representations of n by ϕ_1 and ϕ_2, respectively. If $r_1(n)$ and $r_2(n)$ are defined to be the total number of representations of n by ϕ_1 and ϕ_2, respectively, $G(N)$ denotes the number of essentially distinct primitive representations of square-free N by the genus in question, and no representations of N are fixed by multiplication by a non-trivial automorph, then

$$G(N) = \frac{r_1(N)}{8} + \frac{r_2(N)}{2}. \tag{2.1}$$

In particular, this holds when N is greater than 1 and is not represented by ϕ_1. Also note that $r_1(n)$ is the nth coefficient in the expansion of $\Theta(z)^2\Theta(7z)$, where $\Theta(n) = \sum_{n\in\mathbb{Z}} q^{n^2}$ and $q = e^{2\pi iz}$. Define

$$\begin{aligned} f(z) &= \frac{1}{2}\sum_{n=1}^{\infty} a(n)q^n = \frac{1}{2}\sum_{n=1}^{\infty}(r_1(n)-r_2(n))q^n \\ &= q+q^2-2q^3-q^4-2q^6+q^7-\cdots, \end{aligned} \tag{2.2}$$

where $q = e^{2\pi iz}$. By Shimura's general result in [7] pertaining to all quadratic forms with integral coefficients, $f \in S_{3/2}(28,\chi_{-28})$. Thus, $g(z)$, the Shimura lift of $f(z)$, is in $M_2(14,\chi_0)$, and from the first proposition in [2], the number of coefficients needed to recognize a modular form is

$$\frac{Nk}{12}\prod_{p|N}\left(1+\frac{1}{p}\right), \tag{2.3}$$

so by checking the first 4 coefficients, we see that

$$\begin{aligned} g(z) &= \eta(z)\eta(2z)\eta(7z)\eta(14z) \\ &= q\prod_{n=1}^{\infty}(1-q^z)\prod_{n=1}^{\infty}(1-q^{2z})\prod_{n=1}^{\infty}(1-q^{7z})\prod_{n=1}^{\infty}(1-q^{14z}) \\ &= q-q^2-2q^3+q^4+2q^6+q^7-\cdots = \sum_{n=1}^{\infty}A(n)q^n. \end{aligned} \tag{2.4}$$

From the theory of Eichler and Shimura summarized by Birch and Swinnerton-Dyer in [8], we know that g will be the inverse Mellin transform of $L(E,s)$, for some elliptic curve of conductor 14. We find an elliptic curve $E: y^2 = x^3+x^2+72x-368$ in [3] with

the appropriate conductor, and calculating the first four coefficients of its L-function, we see that E is indeed the curve in question. By Hasse-Weil's bound, for every prime p, $|A(p)| \le 2\sqrt{p}$. The main result of the paper is restricted to integers coprime to 7, but we can apply the following result to integers divisible by an even power of 7.

PROPOSITION 2.1. *ϕ_1 represents $7^{2m}n$ if and only if it represents n.*

PROOF. It is sufficient to prove the proposition for $m = 1$. If ϕ_1 represents n, it clearly represents $49n$. The other direction is simple algebra: $x^2+y^2+7z^2 = 49n \Rightarrow x^2+y^2 \equiv 0 \pmod 7 \Rightarrow (x,y) \equiv (0,0) \pmod 7$. Letting $x = 7a$, and $y = 7b$, $49a^2 + 49b^2 + 7z^2 = 49n \Rightarrow z^2 \equiv 0 \pmod 7$. Letting $z = 7c$, divide by 49 to obtain $a^2+b^2+7z^2 = n$. □

PROOF OF THEOREM 1.1. Our proof is modelled after Ono and Soundararajan's proof in [6] of a corresponding result for $\phi = x^2+y^2+10z^2$. Since f lies in $S_{3/2}(28,\chi_{-28})$, a one-dimensional space, it is an eigenform of all half-integral weight Hecke operators $T(p^2)$, so for every prime p and integer n, there exists a complex number $\lambda(p)$, depending only on p, such that

$$\lambda(p)a(n) = a(np^2) + \chi_{-28}(p)\left(\frac{-n}{p}\right)a(n) + \chi_{-28}(p^2)pa\left(\frac{n}{p^2}\right). \tag{2.5}$$

Since each $A(p)$ is an eigenvalue of T_p for $g(z)$, and the Hecke operators commute with the Shimura lift, $A(p)$ is also an eigenvalue of T_p for $f(z)$, and hence $\lambda(p) = A(p)$. If n is square-free, $a(n/p^2) = 0$, so by our definition of $a(n)$,

$$r_1(np^2) - r_2(np^2) = \left(A(p) - \chi_{-28}(p)\left(\frac{-n}{p}\right)\right)(r_1(n) - r_2(n)). \tag{2.6}$$

□

Let us assume that $n > 1$ is a square-free integer coprime to 7, and p is prime, but not 7. If $r_1(np^2) = 0$, then $r_1(n) = 0$, so

$$\frac{r_2(np^2)}{r_2(n)} = A(p) - \chi_{-28}(p)\left(\frac{-n}{p}\right) \le A(p) + 1. \tag{2.7}$$

But any non-primitive representation of np^2 has $\gcd(x,y,z) = p$, so

$$r_2(np^2) = s_2(np^2) + s_2(n) = s_2(np^2) + r_2(n). \tag{2.8}$$

Since $n \ne 1$, for any representation of n by ϕ_2 has $(x,y,z) \ne (x,-y,-z)$, so $2G(np^2) = s_2(np^2)$. Thus,

$$\frac{r_2(np^2)}{r_2(n)} = 1 + \frac{s_2(np^2)}{r_2(n)} = 1 + \frac{2G(np^2)}{2G(n)} = 1 + \frac{G(np^2)}{G(n)}. \tag{2.9}$$

By [4, Theorem 86], this equals $1 + h(-28np^2)/h(-28n)$, and applying the index formula for $h(-D)$ from [1], this simplifies to $1 + p - (\frac{-28n}{p}) \ge p$. Substituting into (2.7), $p \le A(p) + 1$. But since Hasse's bound yields $p \le 2\sqrt{p} + 1$, this is impossible for $p > 5$. For our exceptional cases; $p \le 5$, $A(p)$ is not positive, so we still obtain a contradiction. Thus, if n is coprime to 7, and p is a prime not equal to 7, ϕ_1 represents np^2, and thus ϕ_1 represents all non-square-free positive integers coprime to 7.

References

[1] D. A. Cox, *Primes of the Form $x^2 + ny^2$*. Fermat, class field theory and complex multiplication, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989. MR 90m:11016. Zbl 701.11001.

[2] G. Frey, *Construction and arithmetical applications of modular forms of low weight*, Elliptic Curves and Related Topics (H. Kisilevsky et al., ed.), CRM Proc. Lect. Notes, vol. 4, Amer. Math. Soc., Providence, RI, 1994, pp. 1–21. MR 95b:11042. Zbl 814.11027.

[3] K. James, *L-series with nonzero central critical value*, J. Amer. Math. Soc. **11** (1998), no. 3, 635–641. MR 98m:11040. Zbl 904.11015.

[4] B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, Carus Monograph Series, no. 10, The Mathematical Association of America, Buffalo, NY, 1950. MR 12,244a. Zbl 041.17505.

[5] I. Kaplansky, *The first nontrivial genus of positive definite ternary forms*, Math. Comp. **64** (1995), no. 209, 341–345. MR 95c:11048. Zbl 826.11015.

[6] K. Ono and K. Soundararajan, *Ramanujan's ternary quadratic form*, Invent. Math. **130** (1997), no. 3, 415–454. MR 99b:11036. Zbl 930.11022.

[7] G. Shimura, *On modular forms of half integral weight*, Ann. of Math. (2) **97** (1973), 440–481. MR 48#10989. Zbl 266.10022.

[8] H. P. F. Swinnerton-Dyer and B. J. Birch, *Elliptic curves and modular functions*, Modular Functions of One Variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, pp. 2–32. MR 52#5685.

James Kelley: Department of Mathematics, University of California at Berkeley, Berkeley, CA 94709, USA

E-mail address: kelley@math.psu.edu