ILLINOIS JOURNAL OF MATHEMATICS
Volume 32, Number 3, Fall 1988

AN ASYMPTOTIC RESULT FOR SUBGROUPS OF SL(2, Z) OF LEVEL 2

BY

MORRIS NEWMAN

In memoriam Irving Reiner

Introduction

Let $\Gamma = SL(2, Z)$. Let E stand for the euclidean matrix norm, so that if

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma,$$

then

$$E(A)^2 = a^2 + b^2 + c^2 + d^2.$$

In a previous paper [2] the author considered the problem of determining the number of solutions $N(\Gamma, x)$ of the inequality $E(A)^2 \le x$, $A \in \Gamma$. It was shown in [2] that $N(\Gamma, x) \sim 6x$; that is, $N(\Gamma, x)/x$ approaches 6 as x approaches ∞. This result also appears as Exercise 8, p. 267, of [3]. Furthermore, the following conjecture was made in [2]:

Conjecture. Let G be a subgroup of Γ of finite index μ. Let $N(G, x)$ be the number of solutions of the inequality $E(A)^2 \le x$, $A \in G$. Then $N(G, x) \sim (6/\mu)x$.

The purpose of this note is to prove the conjecture for all subgroups of Γ of level 2; that is, for all subgroups of Γ containing the principal congruence subgroup $\Gamma(2)$, which consists of all matrices $A \in \Gamma$ such that $A \equiv I \bmod 2$. $\Gamma(2)$ is a normal subgroup of Γ of index 6, and $\Gamma/\Gamma(2)$ is isomorphic to the symmetric group S_3. Thus if G is any proper subgroup of Γ containing $\Gamma(2)$, $G/\Gamma(2)$ is either the trivial group, the cyclic group C_2, or the cyclic group C_3.

Received July 6, 1987.

The principal analytic result required is a theorem of T. Estermann [1], which we state as a lemma:

LEMMA 1 (Estermann). *For any positive ε and any positive integer k,*

(1)
$$\sum_{1 \le h \le n} r(h) r(h+k) = c_k n + O(n^{\alpha} \log^{\beta} n), \quad \alpha = 11/12, \beta = 17/6 + \varepsilon,$$

where

$$c_k = 8 \sum_{d \mid k} (-1)^{d+k} d/k. \tag{2}$$

Here $r(n)$ is the number of representations of n as the sum of 2 squares, and is the coefficient of x^n in the power series for $\theta^2(x)$, where $\theta(x)$ is the theta-function $\theta(x) = \Sigma_{-\infty}^{\infty} x^{n^2}$. We also require the function $r^*(n)$, which is the coefficient of x^n in the power series for $\theta(x)\theta(-x)$. This function satisfies

$$r^*(n) = 0,\ n \text{ odd}, \quad -r(n), n \equiv 2 \bmod 4, \quad r(n/4), n \equiv 0 \bmod 4. \tag{3}$$

We also note that

$$r(4n) = r(n), \quad r(4n+2) = r(2n+1), \quad r(n) = 0 \text{ if } n \equiv 3 \bmod 4. \tag{4}$$

The full error term of (1) will not be required; all that is needed is the fact that it is $o(n)$.

The theorem and its proof

We will prove:

THEOREM. *Let G be a subgroup of Γ of level 2 and index μ. Let $N(G, x)$ denote the number of solutions of $E(A)^2 \le x$, $A \in G$. Then $N(G, x) \sim (6/\mu)x$.*

Note that $6/\mu$ is the order of $G/\Gamma(2)$.

Proof. We break the proof up into cases, depending on the value of μ. The case $\mu = 3$ is the hardest, and depends (in part) on the case $\mu = 6$, so this will be done last.

(i) $\mu = 1$. Then $G = \Gamma$, and the theorem has already been proved in [2] for this case.

(ii) $\mu = 2$. Then $G/\Gamma(2)$ is isomorphic to C_3 and $G = \Gamma^2$, the subgroup of Γ generated by the squares of all elements of Γ. Γ^2 is a normal subgroup of Γ

(in fact, a fully invariant subgroup of Γ), and

$$\Gamma = \Gamma^2 + T\Gamma^2, \quad T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

is a left coset decomposition for Γ modulo Γ^2. If we now note that for any matrix $A \in \Gamma$, $E(A) = E(TA)$, the result is a consequence of case (i), since the number of solutions of $E(A)^2 \leq x$, $A \in \Gamma^2$, is the same as the number of solutions of $E(A)^2 \leq x$, $A \in T\Gamma^2$; and both together constitute the number of solutions of $E(A)^2 \leq x$, $A \in \Gamma$. It follows that

$$N(\Gamma^2, x) = N(\Gamma, x)/2 \sim 3x,$$

the desired result.

(iii) $\mu = 6$. Then $G = \Gamma(2)$. Let $S(G, n)$ denote the number of solutions of $E(A)^2 = n$, $A \in G$. Then $S(\Gamma(2), n)$ is just the number of solutions of

$$a^2 + b^2 + c^2 + d^2 = n, \quad ad - bc = 1, b, c \text{ even}. \tag{5}$$

As in [2], put $A = a + d$, $D = a - d$, $B = b + c$, $C = b - c$. Then

$$A^2 + C^2 = n + 2, \quad B^2 + D^2 = n - 2, \quad A, B, C, D \text{ even}. \tag{6}$$

Conversely, if A, B, C, D satisfy (6) then

$$a = (A + D)/2, \quad b = (B + C)/2, \quad c = (B - C)/2, \quad d = (A - D)/2$$

are integers satisfying (5). Since A, B, C, D are even, we may write

$$A = 2A_0, B = 2B_0, C = 2C_0, D = 2D_0,$$

so that

$$a = A_0 + D_0, b = B_0 + C_0, c = B_0 - C_0, d = A_0 - D_0.$$

Then (6) becomes

$$A_0^2 + C_0^2 = (n + 2)/4, \quad B_0^2 + D_0^2 = (n - 2)/4, \quad B_0 + C_0 \text{ even}, \quad A_0 + D_0 \text{ odd}.$$

Thus for solutions to exist at all, $n = 4N + 2$.

Since $A_0 + D_0$ odd follows from the facts that $B_0 + C_0$ is even and

$$A_0^2 + B_0^2 + C_0^2 + D_0^2 = n/2 = 2N + 1,$$

we need the number of solutions

$$A_0^2 + C_0^2 = N + 1, \quad B_0^2 + D_0^2 = N, \quad B_0 \equiv C_0 \bmod 2.$$

This is the coefficient of $x^{N+1}y^N$ in the power series

$$\sum_{a,b,c,d} \tfrac{1}{2}\left(1 + (-1)^{b+c}\right)x^{a^2+c^2}y^{b^2+d^2}$$
$$= \tfrac{1}{2}\{\theta^2(x)\theta^2(y) + \theta(x)\theta(-x)\theta(y)\theta(-y)\}.$$

This readily implies that the number of solutions $S(\Gamma(2), n) = S(\Gamma(2), 4N + 2)$ is given by

$$\tfrac{1}{2}\{r(N+1)r(N) + r^*(N+1)r^*(N)\}.$$

But $r^*(N+1)r^*(N) = 0$, since one of $N, N+1$ is odd (formula (3)). It follows that the number of solutions is $\frac{1}{2}(r(N+1)r(N))$. Hence

$$\begin{aligned} N(\Gamma(2), x) &= \tfrac{1}{2} \sum_{4N+2 \le x} r(N+1)r(N) \\ &= \tfrac{1}{2} \sum_{N \le (x-2)/4} r(N+1)r(N) \\ &= \tfrac{1}{2}c_1 x/4 + o(x) \\ &= x + o(x), \end{aligned}$$

by Lemma 1. This completes the proof in this case.

(iv) $\mu = 3$. There are 4 subgroups of Γ of index 3; namely, $\Gamma_0(2)$, $\Gamma^0(2)$, K, Γ^3. Here $\Gamma_0(2)$ is the subgroup consisting of all elements $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of Γ such that $c \equiv 0 \bmod 2$; $\Gamma^0(2)$ is the subgroup consisting of all elements $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of Γ such that $b \equiv 0 \bmod 2$; K is the "theta subgroup", generated by

$$T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{and} \quad S^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix};$$

and Γ^3 is the fully invariant subgroup generated by the cubes of all elements of Γ. However, Γ^3 does not contain $\Gamma(2)$ as a subgroup, and so must be omitted. The remaining 3 are conjugate groups. The proof for $\Gamma^0(2)$ is precisely similar to the proof for $\Gamma_0(2)$, and will be omitted. It is thus only necessary to prove the result for $\Gamma_0(2)$ and K.

We start with K. K has the following coset decomposition modulo $\Gamma(2)$:

$$K = \Gamma(2) + T\Gamma(2), \quad T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

We now argue along the lines of case (ii). The number of solutions of $E(A)^2 \le x$, $A \in \Gamma(2)$, is the same as the number of solutions of $E(A)^2 \le x$, $A \in T\Gamma(2)$; and these together constitute the number of solutions of $E(A)^2 \le x$, $A \in K$. Since $N(\Gamma(2), x) = x + o(x)$ by case (iii), it follows that

$$N(K, x) = 2N(\Gamma(2), x) = 2x + o(x),$$

the desired result.

We now come to the last case: $G = \Gamma_0(2)$. We first prove:

LEMMA 2.

$$\sum_{n \le (x-1)/4} r(4n+1)r(4n+5) = 8x + o(x).$$

Proof. By Lemma 1, we have

$$f = \sum_{n \le x} r(n)r(n+4) = c_4 x + o(x) = 10x + o(x).$$

Considering n modulo 4, we find that $f = f_0 + f_1 + f_2 + f_3$, where

$$f_i = \sum_{n \le (x-i)/4} r(4n+i)r(4n+i+4), \quad i = 0, 1, 2, 3.$$

We have $f_0 = \sum_{n \le x/4} r(4n)r(4n+4) = \sum_{n \le x/4} r(n)r(n+1)$, because of (4). Hence $f_0 = c_1 x/4 + o(x) = 2x + o(x)$, by (1). Next, we have

$$f_1 = \sum_{n \le (x-1)/4} r(4n+1)r(4n+5),$$

$$f_2 = \sum_{n \le (x-2)/4} r(4n+2)r(4n+6) = \sum_{n \le (x-2)/4} r(2n+1)r(2n+3),$$

$$f_3 = \sum_{n \le (x-3)/4} r(4n+3)r(4n+7).$$

But one of $2n+1$, $2n+3$ must be congruent to 3 modulo 4, and $4n+3$ is congruent to 3 modulo 4. Hence because of (4), f_2 and f_3 are both 0. Thus

$$f = f_0 + f_1, \quad f_1 = f - f_0 = 10x + o(x) - \{2x + o(x)\} = 8x + o(x).$$

This completes the proof of the lemma.

Now let $S(\Gamma_0(2), n)$ be the number of solutions of $E(A)^2 = n$, $A \in \Gamma_0(2)$. This is just the number of solutions of

$$a^2 + b^2 + c^2 + d^2 = n, \quad ad - bc = 1, c \text{ even}.$$

As before, set $A = a + d$, $D = a - d$, $B = b + c$, $C = b - c$, so that

$$a = (A + D)/2, \quad b = (B + C)/2, \quad c = (B - C)/2, \quad d = (A - D)/2.$$

Then because a, d are odd and c is even, we have $B \equiv C \bmod 4$, and A and D even. Then arguing as before, $S(\Gamma_0(2), n)$ is just the number of solutions of

$$A^2 + C^2 = n + 2, B^2 + D^2 = n - 2, \quad B \equiv C \bmod 4, A, D \text{ even}.$$

We note that $C \equiv n \bmod 2$. Put $A = 2A_0$, $D = 2D_0$, so that

$$4A_0^2 + C^2 = n + 2, \quad B^2 + 4D_0^2 = n - 2.$$

There are 2 cases:

Case 1. n even. Then $C = 2C_0$, $B = 2B_0$,

$$A_0^2 + C_0^2 = (n + 2)/4, \quad B_0^2 + D_0^2 = (n - 2)/4, \quad B_0 \equiv C_0 \bmod 2.$$

Thus $n = 4N - 2$ and

$$A_0^2 + C_0^2 = N, \quad B_0^2 + D_0^2 = N - 1, \quad B_0 \equiv C_0 \bmod 2.$$

The number of solutions is

$$\frac{1}{2} \sum_{a^2 + c^2 = N,\, b^2 + d^2 = N - 1} \left(1 + (-1)^{b+c}\right)$$
$$= \tfrac{1}{2}\{r(N)r(N-1) + r^*(N)r^*(N-1)\} = \tfrac{1}{2}r(N)r(N-1),$$

since one of N, $N - 1$ is odd.

Case 2. n odd. Then B and C are odd, which implies that $n = 4N - 1$. As before, put $A = 2A_0$, $D = 2D_0$. We have

$$4A_0^2 + C^2 = 4N + 1, \quad B^2 + 4D_0^2 = 4N - 3, \quad B \equiv C \bmod 4. \tag{7}$$

We note that

$$\begin{aligned} \tfrac{1}{4}\{1 + i^t + i^{2t} + i^{3t}\} &= 1 \quad \text{if } t \equiv 0 \bmod 4 \\ &= 0 \quad \text{otherwise} \end{aligned}$$

Using this, the number of solutions of (7) becomes

$$\begin{aligned} f &= \frac{1}{4} \sum_{\substack{4a^2+c^2=4N+1,\\ b^2+4d^2=4n-3}} \{1 + i^{b-c} + i^{2(b-c)} + i^{3(b-c)}\} \\ &= \tfrac{1}{4}(f_0 + f_1 + f_2 + f_3), \text{ say.} \end{aligned}$$

We have

$$f_0 = \sum_{\substack{4a^2+c^2=4N+1,\\ b^2+4d^2=4N-3}} 1 = \tfrac{1}{4}r(4N+1)r(4N-3),$$

since

$$\sum_{4u^2+v^2=2M+1} 1 = \tfrac{1}{2} \sum_{u^2+v^2=2M+1} 1.$$

Next,

$$f_1 = \sum_{\substack{4a^2+c^2=4N+1,\\ b^2+4d^2=4N-3}} i^{b-c} = \sum_{b^2+4d^2=4N-3} i^b \sum_{4a^2+c^2=4N+1} i^{-c}.$$

Since b is odd, it is readily seen that the contributions to the first factor for b positive and for b negative are negatives of each other, which implies that it is 0. Thus $f_1 = 0$ as well. A similar argument shows that f_3 is also 0. As for f_2, we have

$$\begin{aligned} f_2 &= \sum_{\substack{4a^2+c^2=4N+1,\\ b^2+4d^2=4N-3}} (-1)^{b-c} \\ &= \sum_{b^2+4d^2=4n-3} (-1)^b \sum_{4a^2+c^2=4N+1} (-1)^c \\ &= \tfrac{1}{4}r(4N-3)r(4N+1), \end{aligned}$$

since b and c are both odd. Hence $f = \frac{1}{4}\{f_0 + f_2\} = \frac{1}{8}r(4N-3)r(4N+1)$. Putting together cases 1 and 2, we finally get that the desired sum is

$$\frac{1}{2} \sum_{N \le (x+2)/4} r(N)r(N-1) + \frac{1}{8} \sum_{N \le (x+1)/4} r(4N-3)r(4N+1);$$

and by Lemmas 1 and 2, this becomes

$$\tfrac{1}{2} \cdot 8x/4 + \tfrac{1}{8} \cdot 8x + o(x) = 2x + o(x),$$

the desired result. This completes the proof.

REFERENCES

1. T. ESTERMANN, *An asymptotic formula in the theory of numbers*, Proc. London Math. Soc., Vol. 34 (1932), pp. 280–292.
2. M. NEWMAN, *Counting modular matrices with specified euclidean norm*, J. Combin. Theory Ser. A, to appear.
3. A. TERRAS, *Harmonic analysis on symmetric spaces and applications I*, Springer-Verlag, New York, 1985.

UNIVERSITY OF CALIFORNIA
SANTA BARBARA, CALIFORNIA