A note on representation of positive definite binary quadratic forms by positive definite quadratic forms in 6 variables

by

YOSHIYUKI KITAOKA (Nagoya)

Let $S$ and $T$ be positive definite even integral matrices of degree $m$ and 2, respectively. We denote the transpose of a matrix $X$ by $'X'$, and $'XSX'$ by $S[X]$ if it is defined. Now suppose that $S[X] = T$ is soluble over $\mathbb{Z}_p$ for all primes. It is known ([1], [2], [4]) that if $m \geq 7$ and $\min T = \min T[x]$ ($Z^2 \ni x \neq 0$) is sufficiently large, then $S[X] = T$ is soluble over $\mathbb{Z}$. Let us consider the case of $m = 6$. In [6] we showed that if $T = a T_0$, where $T_0$ is fixed, and $a$ is a sufficiently large integer relatively prime to det $S$, then $S[X] = a T_0$ is soluble over $\mathbb{Z}$. For $T = a T_0$, det $T := (\min T)^3$ is evident. Here we show, in particular, that if $\det T > (\min T)^{32/3}$ and $\min T$ is sufficiently large, then $S[X] = T$ is soluble over $\mathbb{Z}$. Let us consider the problem from a view of getting an asymptotic formula of the number of solutions. Let

$$f(Z) = \sum a(B) \exp(2\pi i tr(BZ))$$

be a Siegel modular form of degree 2, weight 3, whose constant term of Fourier expansion vanishes at every cusp. We showed (Theorem 1.5.13 on p. 99 in [2]) that for $T > 0$ and $\min T > \varepsilon$ (= an absolute constant)

$$a(T) = O\left((\min T)^{-1/4 + \varepsilon} + (\min T)^{-1}\log((\det T)^{0.5}/(\min T)) (\det T)^{1.5}\right)$$

under an assumption of the estimate of some exponential sums, where $0 < \varepsilon < 0.5$ and $\varepsilon$ is any positive number. Our result above may suggest that the second term on the right-hand side of the estimate of $a(T)$ is superfluous. But the appearance of such a troublesome factor seems to come from the generalization, by using the symplectic modular group $Sp(2, \mathbb{Z})$, of the Farey dissection. If $a(B) = O((\min B)^{-1-\varepsilon}(\det B)^{0.5})$ holds for some positive $\varepsilon$, then we have an asymptotic formula for the number of integral solutions of $S[X] = T$, since the expected main term is

$$\gg (\min T)^{-\varepsilon}(\det T)^{0.5} \prod_p \alpha_p(T, S) \gg (\min T)^{-1-\varepsilon}(\det T)^{0.5}$$

for any positive $\varepsilon$, where $p$ runs over a finite set of primes where the
Witt index of $S$ is equal to 1, and $\sigma_p(T, S)$ is the local density.

We denote by $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_p$ and $\mathbb{Q}_p$, the ring of integers, the field of rational numbers and their completions in the $p$-adic metric, respectively.

Terminology and notation on quadratic forms are generally those from [7].

**Lemma 1.** Let $M$ and $N$ be regular quadratic lattices over $\mathbb{Z}_p$ with $\text{rk } M = 2n + 2, \text{rk } N = n \geq 2$, respectively, and assume that $M$ is $2\mathbb{Z}_p$-maximal and $N$ is represented by $M$. Then for any given primitive submodule $N_0$ of $N$ with $\text{rk } N_0 = n - 1$, there exists an isometry $u: N \to M$ such that $u(N_0)$ is also primitive in $M$.

**Proof.** Put $N = N_0 + \mathbb{Z}_p x$ and let $N_0 = \bigoplus_{i=1}^{n} N_i$, where $\text{rk } N_i = 1$ or 2, and $\text{rk } N_2 = 2$ only if $p = 2$ and $N_i = \langle 2a \rangle (d = 0 \text{ or } 1)$. Since $M$ is $2\mathbb{Z}_p$-maximal, $M$ is isometric to $\bigoplus_{i=1}^{n} \langle 0, 1 \rangle \oplus \langle 1, 0 \rangle$ where $M'$ is $2\mathbb{Z}_p$-maximal and $\text{rk } M' = 4$. Hence we may put $M = \bigoplus_{i=1}^{n} H_i \oplus M'$ where $H_i = \bigoplus_{i=1}^{n} \langle 0, 1 \rangle \oplus \langle 1, 0 \rangle$ for $r = \text{rk } N_r$.

1. Suppose $\text{rk } N_1 = 1$ and $N_1 = \mathbb{Z}_p x$. Put $H_1 = \mathbb{Z}_p e, f) (Q(e) = Q(f) = 0, B(e, f) = 1)$; then $v_i = e + 2^{-1} Q(x_i) f, e_i \in H_1$ satisfies that $v_i$ is primitive in $H_1$ with $Q(v_i) = Q(x)$, and $B(v_i, w) = B(x_i, x)$. Then $u(x) = v_i$ gives an isometry from $N_1$ to $H_1$.

2. Suppose $N_1 = \mathbb{Z}_p x, y$ with $Q(x) = Q(y) = 0, B(x, y) = 2$. Put $H_1 = \mathbb{Z}_p e, f) (Q(e) = Q(f) = 0, B(e, f) = 1, j = 1, 2)$. Then $v_{ij} = e_i, v_{ij} = e_i + 2^{-1} f_j, e_{i+j}$ satisfy that $Z_{v_{ij}, v_{ij}}$ is primitive in $H_1$ and $\text{rk } N_1 = 2$.

3. Suppose $N_1 = \mathbb{Z}_p x, y$ with $Q(x) = Q(y) = 2, B(x, y) = 2$. Let $H_1 = \mathbb{Z}_p e, f) (Q(e) = Q(f) = 2, B(e, f) = 2)$. Then $v_{ij} = e_i + 2^{-1} f_j, v_{ij} + v_{ij} + 2^{-1} f_j$ satisfy that $Z_{v_{ij}, v_{ij}}$ is a primitive lattice in $H_1$ isometric to $N_1$.

We can take an element $w \in M'$. Then there is a natural number $x$ such that $u(N') = x^i \mathbb{Z}_p x$ and we can extend the above isometry $u: N_0 \to M$ by putting $u(x) = \sum_{i=1}^{n} w_i \to x$ and $u(N_0) < x$.

**Proof.** We may suppose that the scale $sM$ of $M$ is in $\mathbb{Z}_p$. We choose and fix a $2\mathbb{Z}_p$-maximal sublattice $M'$ of $M$ for some natural number $k$ once and for all. Suppose, first, that $sN$ is contained in $2\mathbb{Z}_p$. Since $M'$ is $2\mathbb{Z}_p$-maximal and $\text{rk } M' - \text{rk } N = n + 2 - 3 > 0$, it is known that $N$ is represented by $M'$ and hence applying Lemma 1 with scaling by $p^{-1}$ there is an isometry $u: N \to M'$ such that $u(N)$ is primitive in $M'$. Hence we have

$$[M \cap \mathbb{Q}_p u(N) : u(N)] = [M \cap \mathbb{Q}_p u(N) : M' \cap \mathbb{Q}_p u(N)] \leq [M : M']$$

Next consider the case of $sN > 2\mathbb{Z}_p$ and let $N = N_1 \oplus N_2$ where $N_1$ is a modular lattice with $\text{rk } N_1 > 2\mathbb{Z}_p$. $N_2$ may happen to be $0$, and put $S = \{ K \subset M : K \text{ is modular with } sK > 2\mathbb{Z}_p \}$.

It is known that the number of equivalence classes by $O(M)$ in $S$ is finite. We fix a finite number of representatives $(K_j)$. Since $N$ is represented by $M$, $M$ has an isometry $u: N \to M$ such that $u(N_1) = K_j$ for some $j$. Because of $u(N_2) \subset K_j$ and $rk K_j - (2\mathbb{Z}_p N_2 + 3) = rk N_1 - 1 > 0$, there is a submodule $N_2'$ of $K_j$ which is isometric to $N_2$ and $[Q_2, N_2 \cap K_j : N_2] < x'$ for some positive number $x'$ dependent only on $K_j$ by virtue of Theorem 2 in [3], and hence we may suppose that $[Q_2, N_2 \cap K_j : N_2] < x'$. Thus we have

$$[M \cap \mathbb{Q}_p u(N) : u(N)]$$

which depends only on $M$. Since $x'$ is primitive in $N$, $u(N)$ is also primitive in $u(N)$ and we take a natural number $x'$ such that $u(N) > x' (M \cap \mathbb{Q}_p u(N))$. It is easy to see that $u(N) > x' (M \cap \mathbb{Q}_p u(N))$ and hence $[M \cap \mathbb{Q}_p u(N) : u(N)] \leq (x')^{-t}$. We can take max $[(M : M'), (x')^{-t}]$ as $x$ in Theorem.
THEOREM. Let $M$ be a lattice on a positive definite quadratic space over $\mathcal{Q}$ with $\text{rk} M = 2n + 2 \geq 6$. Let $N = \mathbb{Z}[e_1, \ldots, e_n]$ be a lattice on a positive definite quadratic space over $\mathcal{Q}$ so that $(B(e_i, e_j))$ is reduced in the sense of Minkowski and $N$ is represented by $M$, for all primes. If the assumption $\ast$ in Lemma 3 holds and $Q(e_i) > (Q(e_i) \cdots Q(e_{i-1}))^{n+4}$ where $x$ is some constant depending only on $n$, then $N$ is represented by $M$. 

We may assume that $Q(x) \in \mathbb{Z}$ for every $x \in M$. By virtue of Lemma 3, there exist $v_1, \ldots, v_n \in M$ and an isometry $u_p: N_p \to M_p$ such that $u_p(e_i) = v_i$, $i = 1, \ldots, n-1$ for all primes. Take $e \in N$ such that $Ze = N_0$ in $N$ where $N_0 = \mathbb{Z}[e_1, \ldots, e_{n-1}]$, and put $k = [N:N_0, \mathcal{Q}]$. Hence $Q(e) = k^2dN/dN_0 > 2kQ(e_i)$ since $S := (B(e_i, e_j))$ is reduced. Put 

$$S = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix}$$

where $S_1 \in M_{n-1}(Z), S_2 = S_3 \in M_{n-1,1}(Z), S_4 \in Z$; then we have 

$$B(e_i, e_j) = \begin{pmatrix} 1 & -S_1 & S_2 \\ S_1 & 0 & 1 \\ S_2 & 0 & S_4 - S_3 \end{pmatrix}.$$ 

Thus $k$ is at most $\text{det} S_1 = dN_0$. By virtue of Lemma 4, we have only to show that, putting $M_0 = Z[v_1, \ldots, v_n-1]$, there is an element $u$ in $M_0$ satisfying $Q(u) = Q(e)$ and $v = u(e)$ for all primes $p$. Take a basis $\{w_i\}$ of $\mathcal{Q}_k$ in $M_0$ such that $A := (B(w_i, w_j))$ is reduced, and take $P = \sum w_i M_0$ such that $P = u(e)$ mod $M_0$. Then $P = u(e)$ for all primes $p$ and $e_i$. Identifying $P$ and $\{e_i\}$, the existence of $v$, which is what we want to show, is equivalent to the existence of an integral solution $X$ of $A[P + kX] = Q(e)$. Since $u(e) \in M_0$, it has an integral solution over $Z$, and the equivalent diophantine equation 

$$ka[X] + 2PAX = (Q(e) - A[P])/k$$

has an integral solution over $Z$. Since $A$ is reduced, $A \cong \text{diag}(Q(w_1), \ldots, Q(w_n))$ holds and hence we have 

$$A[P] = k^2dN_0 < k^2dM_0 < k^2dM_0 < k^2dN_0.$$ 

Therefore we have $Q(e) > x_1^2Q(e_i), A[P] > x_2^2dN_0$ for some constants $x_1, x_2$ dependent only on $M$. Hence we have 

$$Q(e) - A[P]/k > x_1^2Q(e_i) - x_2^2dN_0/k$$

and 

$$dN_0(\text{det} A)^k / k > dN_0(\text{det} A)^k / k.$$ 

if $Q(e_i) > (dN_0)^{n+4}$, since $dN_0 = dM_0 \leq dM_0 < dM_0$, $k \leq dN_0$ and degree of $A = n+3$. By virtue of [8], if $Q(e_i) - A[P]/k > (\text{det} A)^{n+4}$ for some $x$, which is given explicitly there, the diophantine equation has an integral solution. Since $dN_0 > (Q(e_i))^{n+4}$, we have only to take $Q(e_i)$ such that $dN_0$ exceeds a constant needed in [8].
Remark. As we noted, the assumption (*) is valid for \( n = 2 \) and 3, and \( \chi \) in Theorem is 5.2, 8/3 for \( n = 2, 3 \), respectively [8]. Thus in the case of \( n = 2 \) the assumptions needed in Theorem are \( dN > (\min N)^{32:2} \) and the sufficient size of \( \min N \) as in the introduction.

References


On Eisenstein's problem

by

NOBURO ISHI* (Osaka), PIERRE KAPLAN** (Nancy) and KENNETH S. WILLIAMS*** (Ottawa)

1. Introduction. Let \( D \) be a positive nonsquare integer such that \( D \equiv 1 \pmod{4} \). In this paper we shall be concerned with the solvability or insolvability of the equation

\[ T^2 - DU^2 = 4 \]

in coprime integers \( T \) and \( U \) (equivalently in odd integers \( T \) and \( U \)). If there are odd integers \( T \) and \( U \) satisfying \( T^2 - DU^2 = 4 \) we say that (1.1) has odd solutions, and if there are no odd integers \( T \) and \( U \) satisfying \( T^2 - DU^2 = 4 \) we say that (1.1) has no odd solution. When \( D \equiv 1 \pmod{8} \) simple congruence considerations modulo 8 show that (1.1) has no odd solution. When \( D \equiv 5 \pmod{8} \) the equation (1.1) may \( (D = 5) \) or may not \( (D = 37) \) have odd solutions.

In 1844 Eisenstein [1] asked for a necessary and sufficient condition for (1.1) to have odd solutions. In fact Gauss in his Disquisitiones Arithmeticae (1801) (see [2], §256, VI) had already mentioned this problem, in a slightly different setting, and given the list of all \( D \equiv 5 \pmod{8} \), \( D < 1000 \), for which (1.1) has no odd solution.

When the equation

\[ V^2 - DW^2 = -1 \]

is solvable a necessary and sufficient condition for the solvability of (1.1) in odd integers was given recently by Kaplan and Williams [5], in terms of the lengths \( l \) and \( l^* \) of the continued fraction expansions of \( \sqrt{D} \) and \( (1+\sqrt{D})/2 \) respectively (see Theorem 0 below). It was known that \( l \equiv l^* \equiv 1 \pmod{2} \), and also that \( l \equiv l^* \equiv 1 \pmod{2} \) if, and only if, (1.2) is solvable.

* Research supported by the Government of Japan.

** Research supported by the Government of Canada.

*** Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.