ACTA ARITHMETICA
LIV (1990)

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 ${}^tX$, and ${}^tXSX$ by $S[X]$ if it is defined. Now suppose that $S[X] = T$ is soluble over $\mathbf{Z}_p$ for all primes. It is known ([1], [2], [4]) that if $m \geqslant 7$ and $\min T = \min T[x]$ $(\mathbf{Z}^2 \ni x \neq 0)$ is sufficiently large, then $S[X] = T$ is soluble over $\mathbf{Z}$. Let us consider the case of $m = 6$. In [6] we showed that if $T = aT_0$, where T_0 is fixed, and a is a sufficiently large integer relatively prime to det S, then $S[X] = aT_0$ is soluble over $\mathbf{Z}$. For $T = aT_0$, $\det T \asymp (\min T)^2$ is evident. Here we show, in particular, that if $\det T > (\min T)^{32.2}$ and $\min T$ is sufficiently large, then $S[X] = T$ is soluble over $\mathbf{Z}$. Let us consider the problem from a view of getting an asymptotic formula of the number of solutions. Let

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

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 $\min T > \varkappa$ (= an absolute constant)

$$a(T) = O\Big(\big((\min T)^{a/2-1/4+\varepsilon} + (\min T)^{-1}\log((\det T)^{0.5}/(\min T))\big)(\det T)^{1.5}\Big)$$

under an assumption of the estimate of some exponential sums, where $0 \leqslant a < 0.5$ and ε 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 $\mathrm{Sp}(2, \mathbf{Z})$, of the Farey dissection. If $a(B) = O((\min B)^{-1-\varepsilon}\cdot(\det B)^{0.5})$ holds for some positive ε, then we have an asymptotic formula for the number of integral solutions of $S[X] = T$, since the expected main term is

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

for any positive $\varkappa$, where p runs over a finite set of primes where the

Witt index of S is equal to 1, and $\alpha_p(T, S)$ is the local density.

We denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{Z}_p$ and $\boldsymbol{Q}_p$ 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 $\boldsymbol{Z}_p$ with $\operatorname{rk} M = 2n+2$, $\operatorname{rk} N = n \geq 2$, respectively, and assume that M is $2\boldsymbol{Z}_p$-maximal and N is represented by M. Then for any given regular primitive submodule N_0 of N with $\operatorname{rk} N_0 = n-1$, there exists an isometry u: $N \to M$ such that $u(N_0)$ is also primitive in M.*

Proof. Put $N = N_0 + \boldsymbol{Z}_p x$ and let $N_0 = \perp_{i=1}^{h} N_i$ where $\operatorname{rk} N_i = 1$ or 2, and $\operatorname{rk} N_i = 2$ only if $p = 2$ and $N_i = \langle 2^a \begin{pmatrix} 2d & 1 \\ 1 & 2d \end{pmatrix} \rangle$ $(d = 0$ or $1)$. Since M is $2\boldsymbol{Z}_p$-maximal, M is isometric to $\perp_{n-1} \langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle \perp M'$ where M' is $2\boldsymbol{Z}_p$-maximal and $\operatorname{rk} M' = 4$. Hence we may put $M = \perp_{i=1}^{h} H_i \perp M'$ where $H_i = \perp_r \langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$ for $r = \operatorname{rk} N_i$.

(1) Suppose $\operatorname{rk} N_i = 1$ and $N_i = \boldsymbol{Z}_p[x_i]$. Put $H_i = \boldsymbol{Z}_p[e, f]$ $(Q(e) = Q(f) = 0$, $B(e, f) = 1)$; then $v_i := e + 2^{-1} Q(x_i) f \in H_i$ satisfies that v_i is primitive in H_i with $Q(v_i) = Q(x_i)$, and $B(v_i, w_i) = B(x_i, x)$ and $Q(w_i) = 0$ for $w_i = B(x_i, x) f \in H_i$. Then $u(x_i) = v_i$ gives an isometry from N_i to H_i.

(2) Suppose $N_i = \boldsymbol{Z}_2[x_{i,1}, x_{i,2}]$ $(Q(x_{i,1}) = Q(x_{i,2}) = 0$, $B(x_{i,1}, x_{i,2}) = 2^a)$. Put $H_i = \boldsymbol{Z}_2[e_1, f_1] \perp \boldsymbol{Z}_2[e_2, f_2]$ $(Q(e_j) = Q(f_j) = 0$, $B(e_j, f_j) = 1$, $j = 1, 2)$; then $v_{i,1} := e_1$, $v_{i,2} := e_1 + 2^a f_1 - 2^a e_2 + f_2$ satisfy that $\boldsymbol{Z}_2[v_{i,1}, v_{i,2}]$ is primitive in H_i and isometric to N_i by $u(x_{i,j}) = v_{i,j}$ $(j = 1, 2)$ and for $w_i = B(x_{i,1}, x) f_1 + B(x_{i,2} - x_{i,1}, x) e_2$, $B(v_{i,j}, w_i) = B(x_{i,j}, x)$ holds for $j = 1, 2$ and $Q(w_i) = 0$ is clear.

(3) Suppose $N_i = \boldsymbol{Z}_2[x_{i,1}, x_{i,2}]$ $(Q(x_{i,1}) = Q(x_{i,2}) = 2^{a+1}$, $B(x_{i,1}, x_{i,2}) = 2^a)$. Let H_i, e_j, f_j be the same as in (2); then $v_{i,1} := e_1 + 2^a f_1$, $v_{i,2} := 2^a f_1 + e_2 + 2^a f_2$ satisfy that $\boldsymbol{Z}_2[v_{i,1}, v_{i,2}]$ is a primitive lattice in H_i isometric to N_i by $u(x_{i,j}) = v_{i,j}$ $(j = 1, 2)$ and for $w_i = B(x_{i,1}, x) f_1 + B(x_{i,2}, x) f_2$, $B(v_{i,j}, w_i) = B(x_{i,j}, x)$ holds for $j = 1, 2$ and $Q(w_i) = 0$ is obvious.

We can take an element $w \in M'$ with $Q(w) = Q(x)$ and we can extend the above isometry u: $N_0 \to M$ by putting $u(x) = \sum w_i + w$ to an isometry from N to M. □

LEMMA 2. *Let M and N be regular quadratic lattices over $\boldsymbol{Z}_p$ with $\operatorname{rk} M = 2n+2$, $\operatorname{rk} N = n \geq 2$, respectively, and suppose that N is represented by M. Then there is a natural number $\varkappa$ dependent only on M such that for any given primitive submodule N' of N with $\operatorname{rk} N' = n-1$, there is an isometry u: $N \to M$ with*

$$[M \cap \boldsymbol{Q}_p u(N') : u(N')] < \varkappa.$$

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

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

Next consider the case of $\mathfrak{s}N \supset 2p^k\boldsymbol{Z}_p$ and let $N = N_1 \perp N_2$ where N_1 is a modular lattice with $\mathfrak{s}N_1 \supset 2p^k\boldsymbol{Z}_p$ (N_2 may happen to be $\{0\}$), and put

$$S = \{K \subset M \mid K \text{ is modular with } \mathfrak{s}K \supset 2p^k\boldsymbol{Z}_p\}.$$

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

$$\begin{aligned}
&[M \cap \boldsymbol{Q}_p u(N) : u(N)] \\
&\quad = [M \cap \boldsymbol{Q}_p u(N) : (K_i \perp K_i^\perp) \cap \boldsymbol{Q}_p u(N)][(K_i \perp K_i^\perp) \cap \boldsymbol{Q}_p u(N) : u(N)] \\
&\quad \leq [M : K_i \perp K_i^\perp][K_i^\perp \cap \boldsymbol{Q}_p u(N_2) : u(N_2)] \qquad (\text{by } u(N_1) = K_i) \\
&\quad < \max_i [M : K_i \perp K_i^\perp] \cdot \varkappa',
\end{aligned}$$

which depends only on M. Since N' is primitive in N, $u(N')$ is also primitive in $u(N)$ and we take a natural number $\varkappa''$ such that $u(N) \supset \varkappa''(M \cap \boldsymbol{Q}_p u(N))$. It is easy to see that $u(N') \supset \varkappa''(M \cap \boldsymbol{Q}_p u(N'))$ and hence $[M \cap \boldsymbol{Q}_p u(N') : u(N')] \leq (\varkappa'')^{n-1}$. We can take $\max\{[M : M'], (\varkappa'')^{n-1}\}$ as $\varkappa$ in Theorem. □

LEMMA 3. *Let M and N be lattices on positive definite quadratic spaces over $\boldsymbol{Q}$ with $\operatorname{rk} M = 2n+2$, $\operatorname{rk} N = n \geq 2$, respectively, and suppose that N_p is represented by M_p for all primes p. We take and fix a basis $\{e_i\}$ of N such that $(B(e_i, e_j))$ is reduced in the sense of Minkowski. Then there is a constant $c(M)$ satisfying: if $Q(e_1) > c(M)$, then there exist $v_1, \ldots, v_{n-1}$ in M and an isometry u_p: $N_p \to M_p$ with $u_p(e_i) = v_i$ $(1 \leq i \leq n-1)$ for all primes p, provided*

$(*)$: *Let H and K be lattices on positive definite quadratic spaces over $\boldsymbol{Q}$ with $\operatorname{rk} H = h := n-1$, $\operatorname{rk} K = k$, respectively, and suppose that $k \geq 2h+3$ and H_p is represented by K_p for all primes p. Let a be a natural number and S a finite set of rimes containing all prime divisors of a and such that K_p is even unimodular for $p \notin S$. For every collection $\{f_p\}$ of isometries f_p: $H_p \to K_p$, there is an isometry*

$f\colon H \to K$ *satisfying*

$$f(x) \equiv f_p(x) \bmod aK_p \quad \text{for } x \in H_p \text{ and for } p \in S$$

and

$$f(H_p) \text{ is primitive in } K_p \text{ for } p \notin S$$

if $\min H := \min Q(x)$ $(0 \neq x \in H)$ *is larger than some constant dependent only on* a, S, K.

Proof. Recall the following fact:

Let $\sigma\colon W_1 \to W_2$ be an isometry of primitive submodules of M_p ($\sigma(W_1) = W_2$). If M_p is even unimodular, or if σ is sufficiently near to the identity mapping, then σ can be extended to an isometry of M_p.

Put $N' = \mathbf{Z}[e_1, \ldots, e_{n-1}]$. By virtue of Lemma 2, there are an integer c_p dependent only on M_p and an isometry $u'_p\colon N_p \to M_p$ with $[M_p \cap \mathbf{Q}_p u'_p(N'_p) : u'_p(N'_p)] < c_p$. Moreover, we may assume, by Lemma 1, that $u'_p(N'_p)$ is primitive in M_p if M_p is even unimodular. In the assumption $(*)$, we put $H = N'$, $K = M$, $f_p = u'_p$ and $S = \{p \mid M_p \text{ is not even unimodular}\}$. a should be a large number such that prime divisors of a are in S and a makes the above fact hold for $p \in S$. If $Q(e_1) = \min N'$ is sufficiently large, then there is an isometry $u\colon N' \to M$ such that u and u'_p are sufficiently near on N'_p for $p \in S$ and that $u(N'_p)$ is primitive in M_p for every $p \notin S$. We put $v_i = u(e_i)$. If $p \notin S$, then M_p is even unimodular, and hence from the above fact it follows that there is an isometry u''_p of M_p such that $u = u''_p u'_p$ on N'. Therefore, we can put $u_p = u''_p u'_p$. If $p \in S$, then $[M_p \cap \mathbf{Q}_p u'_p(N') : \mathbf{Z}_p u'_p(N')] < c_p$, and u and u'_p are sufficiently near. Noting that c_p depends only on M_p, the same conclusion holds. □

Remark. The assumption $(*)$ is true for $n = 2$ and 3 [5].

LEMMA 4. *Let M and N be lattices on positive definite quadratic spaces over $\mathbf{Q}$ with $\operatorname{rk} N = n$, $\operatorname{rk} M = m$, $\mathfrak{s}M$, $\mathfrak{s}N \subset \mathbf{Z}$, respectively. Suppose that there exist sublattices $N_0 \subset N$, $M_0 \subset M$ satisfying*

1) $1 \leqslant \operatorname{rk} N_0 < n$,

2) *there are isometries $\sigma\colon N_0 \to M_0$, $\eta\colon N_0^\perp \to M_0^\perp$ and $\sigma_p\colon N_p \to M_p$ for all primes,*

3) $\sigma_p|_{N_0} = \sigma$ *for all primes,*

4) *putting $k = [N : N_0 \perp N_0^\perp]$, $\eta(x) - \sigma_p(x) \in k(M_0^\perp)_p$ holds for all $x \in N_0^\perp$ and all primes $p \mid k$.*

Then N is represented by M.

Proof. Clearly, $u = \sigma \perp \eta$ is an isometry from $\mathbf{Q}N$ to $\mathbf{Q}M$. Take any element $x \in N$ and put $kx = x_1 + x_2$, $x_1 \in N_0$, $x_2 \in N_0^\perp$. Since $u(kx) = u(x_1) + u(x_2) = \sigma(x_1) + \eta(x_2) = \sigma_p(x_1) + \sigma_p(x_2) + \eta(x_2) - \sigma_p(x_2) = \sigma_p(kx) + \eta(x_2) - \sigma_p(x_2) \in kM_p$ for $p \mid k$, $u(x) \in M_p$ holds for $p \mid k$. For $p \nmid k$, $N_p = (N_0)_p \perp (N_0^\perp)_p$ and hence $u(N_p) = \sigma(N_0)_p \perp \eta(N_0^\perp)_p \subset M_p$ holds. Thus we have $u(N) \subset M$. □

THEOREM. *Let M be a lattice on a positive definite quadratic space over $\mathbf{Q}$ with $\operatorname{rk} M = 2n+2 \geqslant 6$. Let $N = \mathbf{Z}[e_1, \ldots, e_n]$ be a lattice on a positive definite quadratic space over $\mathbf{Q}$ so that $(B(e_i, e_j))$ is reduced in the sense of Minkowski and N_p is represented by M_p for all primes. If the assumption $(*)$ in Lemma 3 holds and $Q(e_1)$ is sufficiently large and $Q(e_n) > (Q(e_1) \ldots Q(e_{n-1}))^{\varkappa(n+4)}$ where $\varkappa$ is some constant depending only on n, then N is represented by M.*

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

$$S = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix} \quad \text{where } S_1 \in M_{n-1}(\mathbf{Z}),\ S_2 = {}^tS_3 \in M_{n-1,1}(\mathbf{Z}),\ S_4 \in \mathbf{Z};$$

then we have

$$(B(e_i, e_j))\left[\begin{pmatrix} 1_{n-1} & -S_1^{-1}S_2 \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} S_1 & 0 \\ 0 & S_4 - S_1^{-1}[S_2] \end{pmatrix}.$$

Thus k is at most $\det S_1 = dN_0$. By virtue of Lemma 4, we have only to show that, putting $M_0 = \mathbf{Z}[v_1, \ldots, v_{n-1}]$, there is an element v in $M_0^\perp$ satisfying $Q(v) = Q(e)$ and $v - u_p(e) \in k(M_0^\perp)_p$ for all primes $p \mid k$. Take a basis $\{w_i\}$ of $M_0^\perp (\subset M)$ such that $A := (B(w_i, w_j))$ is reduced, and take $P = \sum f_i w_i \in M_0^\perp$ such that $P \equiv u_p(e) \bmod k(M_0^\perp)_p$ for all primes $p \mid k$ and $0 \leqslant f_i \leqslant k$. Identifying P and ${}^t(f_1, \ldots, f_{n+3})$, 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 $u_p(e) \in (M_0^\perp)_p$, it has an integral solution over $\mathbf{Z}_p$, and the equivalent diophantine equation $kA[X] + 2{}^tPAX = (Q(e) - A[P])/k$ has an integral solution over $\mathbf{Z}_p$. Since A is reduced, $A \asymp \operatorname{diag}(Q(w_1), \ldots, Q(w_{n+3}))$ holds and hence we have

$$A[P] \ll \sum f_i^2 Q(w_i) < k^2 \sum Q(w_i) \ll k^2 \det A = k^2 dM_0^\perp < k^2 dM dM_0 \ll k^2 dN_0.$$

Thus we have $Q(e) > \varkappa_1 k^2 Q(e_n)$, $A[P] < \varkappa_2 k^2 dN_0$ for some constants $\varkappa_1$, $\varkappa_2$ dependent only on M. Hence we have

$$\begin{aligned}(Q(e) - A[P])/k &> (\varkappa_1 k^2 Q(e_n) - \varkappa_2 k^2 dN_0)/k \\ &> Q(e_n) k(\varkappa_1 - \varkappa_2 dN_0/Q(e_n)) \gg k(dN_0)^{\varkappa(n+4)} \\ &\gg dN_0 (\det kA)^{\varkappa},\end{aligned}$$

if $Q(e_n) \gg (dN_0)^{\varkappa(n+4)}$, since $\det A = dM_0^\perp \leqslant dM dM_0 \ll dM_0 = dN_0$, $k \leqslant dN_0$ and degree of $A = n+3$. By virtue of [8], if $(Q(e) - A[P])/k \gg (\det kA^{\varkappa})$ for some $\varkappa$, which is given explicitly there, the diophantine equation has an integral solution. Since $dN_0 \gg (Q(e_1))^{n-1}$, we have only to take $Q(e_1)$ such that dN_0 exceeds a constant needed in [8].

Remark. As we noted, the assumption (*) is valid for $n = 2$ and 3, and $\varkappa$ 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

[1] J. S. Hsia, Y. Kitaoka, M. Kneser, *Representations of positive definite quadratic forms*, J. Reine Angew. Math. 301 (1978), 132–141.
[2] Y. Kitaoka, *Lectures on Siegel modular forms and representation by quadratic forms*, Tata Institute of Fundamental Research, Bombay; Springer, Berlin–Heildelberg–New York, 1986.
[3] — *Local densities of quadratic forms*; in: *Investigations in Number Theory*, Advanced Studies in Pure Math. 13, 1987, 433–460.
[4] — *Modular forms of degree n and representation by quadratic forms II*, Nagoya Math. J. 87 (1982), 127–146.
[5] — *Modular forms of degree n and representation by quadratic forms IV*, ibid. 107 (1987), 25–47.
[6] — *Modular forms of degree n and representation by quadratic forms V*, to appear in Nagoya Math. J.
[7] O. T. O'Meara, *Introduction to quadratic forms*, Springer, Berlin–Heidelberg–New York 1963.
[8] G. L. Watson, *Quadratic diophantine equations*, Philos. Trans. Roy. Soc. London Ser. A 253 (1960/61), 227–254.

DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
NAGOYA UNIVERSITY
Chikusa-ku, Nagoya, 464-01
Japan

Received on 2.5.1988
and in revised form on 25.8.1988 (1822)

ACTA ARITHMETICA
LIV (1990)

On Eisenstein's problem

by

NOBURO ISHII* (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

$$T^2 - DU^2 = +4 \tag{1.1}$$

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

$$V^2 - DW^2 = -1 \tag{1.2}$$

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 $l \equiv l^* \pmod 2$, 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.