ASYMPTOTICS OF SECOND-ORDER INTEGRAL MATRICES
LYING IN A GIVEN HYPERBOLIC REGION AND
BELONGING TO A GIVEN RESIDUE CLASS

A. M. Istamov

One obtains an asymptotic formula for the problem formulated in the title.

Let $N > 0$, $m > 0$ be integers and let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

be an integral matrix. Let $\Omega$ be a region on the four-dimensional surface

$$\frac{x_1 x_2}{r} = x_1 x_2 - x_1^2 x_2 = 1, \quad x_{ij} = x_{ij}/N \quad (i, j = 1, 2).$$

Let $\operatorname{mes} \Omega = \operatorname{mes} \tilde{\Omega}$ be the invariant measure (see [8, p. 353]). We investigate the number $R(N; \Omega; m, A)$ of integral matrices

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}, \quad x_{ij} \in \mathbb{Z}, \quad (i, j = 1, 2),$$

satisfying the conditions

$$X \in \Omega, \quad X \equiv A \pmod{m}.$$ 

THEOREM. Assume that $\tilde{\Omega} = \Omega/\sqrt{N}$ is a bounded region with a piecewise-smooth boundary. Let

$$\gcd (N, m) = 1,$$

and let

$$R(N; \Omega; m, A) = \frac{\text{mes} \tilde{\Omega}}{5(\tilde{\Omega})} R(N)(1 + O \left( N^{-\frac{1}{2}} \right)).$$

Then one can find a constant $\eta > 0$ such that for $N \to \infty$ and fixed $\tilde{\Omega}$ and $m$ one has

$$R_N(\Omega) = \sum_{d|N} \xi(m, \tilde{\Omega}) d \xi(m, \tilde{\Omega}) = \sum_{d|N} \xi(m, \tilde{\Omega}) \prod_{p|\frac{m}{d}} \left( 1 - \frac{1}{p^2} \right).$$

is the number of matrices $A \pmod{m}$ satisfying the congruence (4).

We outline the proof of the theorem, following the reasonings in [7] and mentioning only the necessary changes. For a preliminary communication of these results, see [1, 2].
1°. Without loss of generality, we can assume that for some constant \( c > 0 \) one has
\[
\bar{x}_{11} > c, \quad \text{if } (\bar{x}_{11}, \bar{x}_{12}, \bar{x}_{21}, \bar{x}_{22}) \in \bar{\mathcal{Q}}.
\]  
[otherwise we divide \( \mathcal{Q} \) into parts which satisfy conditions of the type (7)].

For the sake of the simplicity of the subsequent arguments, we shall assume that
\[
\gcd (a_{11}, m) = 1 \tag{8}
\]
Except for Lemma 2, the lemmas formulated below hold even without this assumption. In Lemma 2, in the general case, in the principal term of formula (17) one has to add a factor depending on \( \gcd (a_{11}, m) = 1 \). This factor disappears when from formula (17) one goes to formula (21). But for this, one does not make use of formula (22), which is valid under the assumption (8), but of the general version (see [6, p. 262]).

In the formulations of Lemmas 1-4 one assumes that the conditions (4), (5) of the theorem are satisfied.

2°. The proof of the theorem is based on the possibility of the parametrization of the problems regarding integral matrices \( X \) which satisfy the conditions (1), (3). A similar parametrization for \( m = 1 \) (and in a more general situation) is considered in [4, 7]. The case \( m = p \), where \( p \) is a prime number, is discussed in [4, 1]. The parametrization is described by the following proposition, proved by a straightforward verification.

**LEMMA 1.** 1) For any \( q > 0 \) satisfying the condition \( q = a_{11} \pmod{m} \) there exists a matrix
\[
X_q = \begin{pmatrix} q & x_1 \\ x_2 & x_3 \end{pmatrix}, \quad \det X_q = N, \quad X = A \pmod{m}, \quad \gcd (q, x_i) = 1.
\]

2) The collection of solutions \( X \) of system (1), (3) satisfying the conditions
\[
x_{11} = q, \quad \gcd (x_{11}, x_{12}) = 1
\]  
coincides with the set of matrices
\[
X = \begin{pmatrix} q & v_1 \\ v_2 & t \end{pmatrix},
\]
where
\[
\begin{aligned}
v_1 &= Z_1 x_1 + t_1 m q, \\
v_2 &= Z_2 x_2 + t_2 m q,
\end{aligned}
\]
here \( Z_1 \) runs through all integers satisfying
\[
1 \leq Z_1 \leq m, \quad \gcd (Z_1, m q) = 1, \quad Z_1 \equiv 1 \pmod{m} \tag{12}
\]
\( Z_2 \) is defined by the conditions
\[
1 \leq Z_2 \leq m, \quad Z_2 Z_1 \equiv 1 \pmod{m q},
\]
t_1 and t_2 run, independently from each other, through all the integers; \( t \) is defined by the condition \( q t - v_1 v_2 = N \).

3) To different triples \((Z_1, t_1, t_2)\) satisfying (12), there correspond different solutions (10) of system (1), (3).

3°. For a fixed integer \( q > 0 \) we denote by \( r(N; q, \omega; m, A) \) the number of integral matrices \( X \) satisfying the conditions (1), (3), (9) and the condition
\[
\omega = \omega (\xi_1, \xi_1', \xi_2, \xi_2') := \begin{cases} 
\xi_1' q < x_{12} \leq \xi_1' q, \\
\xi_2' q < x_{21} \leq \xi_2' q.
\end{cases}
\]

**LEMMA 2.** Let
\[
c_1 \frac{N^\frac{1}{m}}{q} \leq c_2 N^\frac{1}{m},
\]

1086