Canad. Math. Bull. 2024, pp. 1–15
http://dx.doi.org/10.4153/S0008439524000365

Counting elements of the congruence subgroup

Kamil Bulinski and Igor E. Shparlinski

Abstract. We obtain asymptotic formulas for the number of matrices in the congruence subgroup

$$\Gamma_0(Q) = \{A \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod Q\},$$

which are of naive height at most X. Our result is uniform in a very broad range of values Q and X.

1 Introduction and the main result

Given an integer $Q \geq 1$, we consider the congruence subgroup

$$\Gamma_0(Q) = \{A \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod Q\},$$

where

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

We are interested in counting matrices $A \in \Gamma_0(Q)$ with entries of size at most

$$\|A\|_\infty = \max\{|a|, |b|, |c|, |d|\} \leq X. \tag{1.1}$$

The question is a natural generalization of the classical counting result of Newman [10] concerning matrices $A \in \mathrm{SL}_2(\mathbb{Z})$ with

$$\|A\|_2 = a^2 + b^2 + c^2 + d^2 \leq X, \tag{1.2}$$

and of Krieg [9] who counts matrices $A \in \mathrm{SL}_2(\mathbb{Z})$ with respect to the L^∞-norm as (1.1). We note that both of these results correspond to $Q = 1$.

We note that while we can also use the L^2-norm as in (1.2) to measure the "size" of $A \in \mathrm{SL}_2(\mathbb{Z})$, for us it is more convenient to use the L^∞-norm as in (1.1). However, our main purpose to have an asymptotic formula in a broad range of uniformity with respect to the size of Q compared to X.

Let

$$\Gamma_0(Q, X) = \{A \in \Gamma_0(Q) : \|A\|_\infty \leq X\}.$$

Received by the editors February 1, 2024; revised May 16, 2024; accepted May 17, 2024.
Published online on Cambridge Core May 22, 2024.
During the preparation of this work, the authors were supported in part by the Australian Research Council Grants DP230100530 and DP230100534.
AMS subject classification: **11C20, 15B36, 15B52.**
Keywords: $\mathrm{SL}_2(\mathbb{Z})$ matrices, congruence subgroup, modular hyperbola.

The question of investigating the cardinality $\#\Gamma_0(Q,X)$ has been raised in [3], where it is also shown that for $Q \le X$, we have

$$\#\Gamma_0(Q,X) = X^{2+o(1)}Q^{-1}.$$

We are interested in obtaining an asymptotic formula for the cardinality $\#\Gamma_0(Q,X)$ in a broad range of Q and X. Furthermore, our bound on error term relies on some results of Ustinov [14], which go beyond standard techniques.

We first give an asymptotic formula for $\#\Gamma_0(Q,X)$ with the main term expressed via sums of some standard arithmetic functions. For this, we also define

$$F(Q,X) = 8\left(F_1(Q,X) + F_2(Q,X)\right),$$

where

$$F_1(Q,X) = \sum_{1\le c\le X/Q} \frac{\varphi(cQ)}{cQ},$$
$$F_2(Q,X) = Q^{-1} \sum_{\substack{Q<x\le X\\ \gcd(x,Q)=1}} \frac{\varphi(x)}{x},$$

where as usual $\varphi(k)$ denotes the Euler function.

Theorem 1.1 *Uniformly over an integer $Q \ge 1$ and a positive real $X \ge Q$, we have*

$$\#\Gamma_0(Q,X) = XF(Q,X) + O\left(X^{5/3+o(1)}Q^{-1} + X\right).$$

Next, we study the function $F(Q,X)$. As indicated to us by one the referees, the sum $F_2(Q,X)$ has already been computed in [13]. When Q is fixed a much more general result is given in [11, Theorem 5.5A.1]. We have not, however, been able to locate references for an asymptotic formula for $F_1(Q,X)$ with the desired level of uniformity in Q, so we derive one in this paper (see 4.4). For this, we first recall the definition of the Dedekind function

$$\psi(Q) = Q \prod_{\substack{p\mid Q\\ p \text{ prime}}} \left(1 + \frac{1}{p}\right).$$

Theorem 1.2 *Uniformly over an integer $Q \ge 1$ and a positive real $X \ge Q$, we have*

$$F(Q,X) = \frac{96}{\pi^2} \cdot \frac{X}{\psi(Q)} + O\left(Q^{o(1)} \log X\right).$$

Combining Theorems 1.1 and 1.2, we obtain the following asymptotic formula.

Corollary 1.3 *Uniformly over an integer $Q \ge 1$ and a positive real $X \ge Q$,*

$$\#\Gamma_0(Q,X) = \frac{96}{\pi^2} \cdot \frac{X^2}{\psi(Q)} + O\left(X^{5/3+o(1)}Q^{-1} + X\log X\right).$$

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

We remark that the appearance of the Dedekind function $\psi(Q)$ in the denominator of the asymptotic formula for $\#\Gamma_0(Q,X)$ in Corollary 1.3 is not surprising as function itself appears in as the index of $\Gamma_0(Q)$ in $\mathrm{SL}_2(\mathbb{Z})$, that is,

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(Q)] = \psi(Q)$$

(see [8, Proposition 2.5]).

Elementary estimates easily show that $\psi(Q) = Q^{1+o(1)}$. Thus, Corollary 1.3 is nontrivial in an essentially full range of Q and X, namely for $Q \le X^{1-\varepsilon}$ for a fixed $\varepsilon > 0$.

2 Preparations

2.1 Notation and some elementary estimates

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are equivalent to $|U| \leqslant cV$ for some positive constant c, which throughout this work, is absolute.

Furthermore, we write $U \asymp V$ to express that $V \ll U \ll V$.

We also write $U = V^{o(1)}$ if for all $\varepsilon > 0$, there exists a constant $c(\varepsilon) > 0$ such that $|U| \le c(\varepsilon)V^{\varepsilon}$ as $V \to \infty$.

The letter p always denotes a prime number.

For an integer $k \ge 1$, we denote by $\mu(k)$, $\tau(k)$, and $\varphi(k)$, the Möbius function, the number of integer positive divisors, and the Euler function of k, respectively, for which we use the well-known bound

$$\tau(k) = k^{o(1)} \qquad \text{and} \qquad \varphi(k) \gg \frac{k}{\log\log(k+2)}, \tag{2.1}$$

as $k \to \infty$ (see [6, Theorems 317 and 328]).

As usual, we define

$$\operatorname{sign} u = \begin{cases} -1, & \text{if } u < 0, \\ 0, & \text{if } u = 0, \\ 1, & \text{if } u > 0. \end{cases}$$

For positive integers u and v, using the Möbius function $\mu(e)$ and the inclusion–exclusion principle to detect the co-primality condition and then interchanging the order of summation, we obtain

$$\begin{aligned} \sum_{\substack{1\le c\le v \\ \gcd(c,u)=1}} 1 &= \sum_{e\mid u} \mu(e) \left\lfloor \frac{v}{e} \right\rfloor = v \sum_{e\mid u} \frac{\mu(e)}{e} + O\left(\sum_{e\mid u} |\mu(e)| \right) \\ &= v\frac{\varphi(u)}{u} + O\left(\tau(u)\right) = v\frac{\varphi(u)}{u} + O\left(u^{o(1)}\right) \end{aligned} \tag{2.2}$$

(see [6, Equation (16.1.3)]).

2.2 Modular hyperbolas

Here, we need some results on the distribution of points on the modular hyperbola

$$uv \equiv 1 \pmod q, \tag{2.3}$$

where $q \geq 1$ is an arbitrary integer.

We start with a very well-known case counting the number $N(q; U, V)$ of solutions in a rectangular domain $(u, v) \in [1, U] \times [1, V]$. For example, such a result has been recorded in [12, Theorem 13] (we note that the restriction $U, V \leq q$ is not really necessary).

Lemma 2.1 *For any $U, V \geq 1$, we have*

$$N(q; U, V) = \frac{\varphi(q)}{q^2} UV + O\left(q^{1/2+o(1)}\right).$$

Next, we recall a result of Ustinov [14] on the number $T_f(q; Z, U)$ of points (u, v) on the modular hyperbola (2.3) with variables run through a domain of the form

$$Z < u \leq Z + U \qquad \text{and} \qquad 0 \leq v \leq f(u),$$

where f is a positive function with a continuous second derivative.

Namely, a special case of [14], where we have also used (2.1) to estimate various divisor sums, can be formulated as follows.

Let

$$\begin{aligned}\mathcal{T}_f(q, Z, U) = \{(u, v) \in \mathbb{Z}^2 :\ Z < u \leq Z + U,\ 0 < v \leq f(u),\\ uv \equiv 1 \pmod q\},\end{aligned}$$

and let

$$T_f(q, Z, U) = \#\mathcal{T}_f(q, Z, U).$$

Lemma 2.2 *Assume that the function $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ has a continuous second derivative on $[Z, Z + U]$ such that for some $L > 0$, we have*

$$|f''(u)| \asymp \frac{1}{L}, \qquad u \in [Z, Z + U].$$

Then we have the estimate

$$T_f(q; Z, U) = \frac{1}{q} \sum_{\substack{Z<u\leq Z+U\\ \gcd(u,q)=1}} f(u) + O\left(\left(UL^{-1/3} + L^{1/2} + q^{1/2}\right)(qU)^{o(1)}\right).$$

For other results on the distribution of points on modular hyperbolas, we refer to the survey [12] and also more recent works [1, 2, 4, 5, 7, 15].

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

3 Proof of Theorem 1.1

3.1 Separating contributions to the main term and to the error term

It is easy to see that there are only $O(X)$ matrices in $\mathrm{SL}_2(\mathbb{Z};X)$ with $abcd = 0$. We now consider the following eight sets for different choices of the signs of a, c, and d:

$$\Gamma_0^{\alpha,\gamma,\delta}(Q,X) = \{A \in \Gamma_0(Q,X):\ \operatorname{sign} a = \alpha,\ \operatorname{sign} c = \gamma,\ \operatorname{sign} d = \delta\},$$

with $\alpha,\gamma,\delta \in \{-1,1\}$.

Now observe that $\Gamma_0(Q,X)$ is preserved under the bijections

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} -a & b \\ c & -d \end{bmatrix}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}.$$

This means

$$\#\Gamma_0^{1,1,1}(Q,X) = \#\Gamma_0^{\alpha,\gamma,\alpha}$$

and

$$\#\Gamma_0^{-1,1,1}(Q,X) = \#\Gamma_0^{-\alpha,\gamma,\alpha}$$

for all pairs $\alpha,\gamma \in \{-1,1\}$.

Thus

$$\#\Gamma_0(Q,X) = 4\cdot\left(\#\Gamma_0^{1,1,1}(Q,X) + \#\Gamma_0^{1,1,-1}(Q,X)\right) + O(X). \tag{3.1}$$

3.2 Preliminary counting of $\Gamma_0^{1,1,1}(Q,X)$

Writing cQ instead of c, we need to count the number of solutions to the equation

$$ad = 1 + bcQ, \qquad 1 \le a, |b|, d \le X,\ 1 \le c \le X/Q.$$

We first do this for a fixed c and then sum up over all $c \le X/Q$.

First, we consider the values $a \le cQ$. We note that setting

$$b = \frac{ad-1}{cQ}$$

for a solution (a,d) to the congruence

$$ad \equiv 1 \pmod{cQ} \qquad 1 \le a \le cQ,\ 1 \le d \le X,$$

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

we have $b \le X$. Hence, we see from Lemma 2.1 (and then recalling that $cQ \le X$) that for every $c \in [1, X/Q]$, there are

$$(3.2) \qquad \begin{aligned} G_1(c) &= \frac{\varphi(cQ)}{(cQ)^2} cQX + O\left((cQ)^{1/2+o(1)}\right) \\ &= \frac{\varphi(cQ)}{cQ} X + O\left(X^{1/2+o(1)}\right) \end{aligned}$$

such matrices

$$\begin{bmatrix} a & b \\ cQ & d \end{bmatrix} \in \Gamma_0^{1,1,1}(Q, X).$$

Next, we count the contribution $G_2(c)$ from matrices $A \in \Gamma_0^{1,1,1}(Q, X)$ with $a > cQ$. To do this, we recall the notation of Section 2.2 and then parameterize this set using a modular hyperbola as follows.

Lemma 3.1 *Fix $1 \le c \le X/Q$, $0 < U \le X - cQ$ and define*

$$f_c(x) = \frac{cQX + 1}{x}.$$

Then the map

$$\mathcal{T}_{f_c}(cQ, cQ, U) \to \Gamma_0^{1,1,1}(Q, X)$$

given by

$$(x, y) \mapsto \begin{bmatrix} x & (xy-1)/cQ \\ cQ & y \end{bmatrix}$$

is well-defined, injective and its image is exactly the set of those $A \in \Gamma_0^{1,1,1}(Q, X)$ with $cQ < a \le cQ + U$ and bottom left entry equal to cQ.

Proof For $(x, y) \in \mathcal{T}_{f_c}(cQ, cQ, U)$, we have that $(xy-1)/cQ \in \mathbb{Z}$ and

$$0 < y \le f_c(X),$$

which is equivalent to

$$\frac{-1}{cQ} < (xy-1)/cQ \le X.$$

As $x > cQ \ge 1$ and $y > 0$, this is actually equivalent to

$$1 \le (xy-1)/cQ \le X.$$

We also need to check that $1 \le y \le X$. This follows since

$$0 < y \le f_c(x) = \frac{cQX+1}{x} < \frac{cQX+1}{cQ} = X + \frac{1}{cQ} \le X + 1.$$

Thus, indeed, (x, y) is mapped to an element of $\Gamma_0^{1,1,1}(Q, X)$ with the desired properties. Conversely, suppose that $A \in \Gamma_0^{1,1,1}(Q, X)$ with $a > cQ$ and bottom left entry

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

equal to cQ. As $ad \equiv 1 \pmod{cQ}$, we have $1 \le x, y \le X$ such that

$$A = \begin{bmatrix} x & (xy-1)/cQ \\ cQ & y \end{bmatrix}.$$

Also by definition (the lower bound holds as $x > cQ \ge 1$)

$$1 \le \frac{xy-1}{cQ} \le X,$$

which means

$$0 < \frac{cQ+1}{x} \le y \le \frac{cQX+1}{x} = f_c(x)$$

and so indeed $(x, y) \in \mathcal{T}(f_c, cQ, U)$. ∎

We partition the interval $(cQ, X]$ into $I \ll \log X$ dyadic intervals of the form $(Z_i, Z_i + U_i]$ with

$$Z_i = 2^{i-1}cQ \qquad \text{and} \qquad U_i \le Z_i, \qquad i = 1, \dots, I,$$

(in fact $U_i = Z_i$, except maybe for $i = I$) and note that

$$2^I cQ \asymp X. \tag{3.3}$$

We now write

$$G_2(c) = \sum_{i=1}^{I} T_{f_c}(cQ, Z_i, U_i), \tag{3.4}$$

where $f_c(x)$ is as in Lemma 3.1.

Next, for each $i = 1, \dots, I$, we use Lemma 2.2 with $q = cQ$ and use that

$$|f''(x)| \asymp \frac{cQX}{Z_i^3} \asymp \frac{X}{2^{3i}(cQ)^2}$$

for $x \in (Z_i, Z_i + U_i]$. Therefore, we conclude that

$$T_{f_c}(cQ, Z_i, U_i) = M_i(c) + O\left(E_i(c)X^{o(1)}\right), \tag{3.5}$$

where

$$M_i(c) = \frac{1}{cQ} \sum_{\substack{Z_i < x \le Z_i + U_i \\ \gcd(x, cQ) = 1}} f_c(x),$$

$$E_i(c) = 2^i cQ \left(\frac{X}{2^{3i}(cQ)^2}\right)^{1/3} + \left(\frac{2^{3i}(cQ)^2}{X}\right)^{1/2} + X^{1/2}.$$

Combing the main terms $M_i(c)$, $i = 1, \dots, I$, together and recalling (3.4), we obtain

$$G_2(c) = \mathsf{M}(c) + O\left(\mathsf{E}(c)X^{o(1)}\right), \tag{3.6}$$

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

where

$$\mathsf{M}(c) = \frac{1}{cQ} \sum_{\substack{cQ<x\le X \\ \gcd(x,|c|Q)=1}} f_c(x)$$

and

$$\begin{aligned}\mathsf{E}(c) &= \sum_{i=1}^{I}\left(2^i cQ\left(\frac{X}{2^{3i}(cQ)^2}\right)^{1/3} + \left(\frac{2^{3i}(cQ)^2}{X}\right)^{1/2} + (cQ)^{1/2}\right)\\ &= \sum_{i=1}^{I}\left((cQX)^{1/3} + 2^{3i/2}cQX^{-1/2} + (cQ)^{1/2}\right)\\ &= \left((cQX)^{1/3} + 2^{3I/2}cQX^{-1/2} + (cQ)^{1/2}\right)X^{o(1)}.\end{aligned}$$

Recalling (3.3) and using $cQ \le X$, we obtain

$$\mathsf{E}(c) \le \left(X^{2/3} + (cQ)^{-1/2}X\right)X^{o(1)},$$

which after the substitution in (3.6) yields

$$G_2(c) = \mathsf{M}(c) + O\left(\left(X^{2/3} + (cQ)^{-1/2}X\right)X^{o(1)}\right). \tag{3.7}$$

3.3 Asymptotic formula for $\Gamma_0^{1,1,1}(Q,X)$

From the equations (3.2) and (3.7), we obtain

$$\#\Gamma_0^{1,1,1}(Q,X) = \sum_{1\le c\le X/Q}\left(G_1(c) + G_2(c)\right) = \mathbf{M} + O\left(\mathbf{E}\right), \tag{3.8}$$

where

$$\begin{aligned}\mathbf{M} &= \sum_{1\le c\le X/Q}\left(\frac{\varphi(cQ)}{cQ}X + \frac{1}{cQ}\sum_{\substack{cQ<x\le X \\ \gcd(x,cQ)=1}} f_c(x)\right)\\ &= XF_1(Q,X) + \sum_{1\le c\le X/Q}\frac{1}{cQ}\sum_{\substack{cQ<x\le X \\ \gcd(x,cQ)=1}} f_c(x)\end{aligned}$$

and

$$\mathbf{E} = \sum_{1\le c\le X/Q}\left(X^{2/3} + (cQ)^{-1/2}X\right)X^{o(1)} = X^{5/3+o(1)}Q^{-1}.$$

We also note that

$$\begin{aligned}\frac{1}{cQ}\sum_{\substack{cQ<x\le X \\ \gcd(x,cQ)=1}} f_c(x) &= \sum_{1\le c\le X/Q}\sum_{\substack{cQ<x\le X \\ \gcd(x,cQ)=1}}\frac{cQX+1}{cQx}\\ &= X\sum_{1\le c\le X/Q}\sum_{\substack{cQ<x\le X \\ \gcd(x,cQ)=1}}\frac{1}{x} + O\left(X^{o(1)}\right).\end{aligned}$$

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

Change the order of summation, we write

$$\sum_{\substack{1\le c\le X/Q}} \sum_{\substack{cQ<x\le X\\ \gcd(x,cQ)=1}} \frac{1}{x} = \sum_{\substack{Q<x\le X\\ \gcd(x,Q)=1}} \frac{1}{x} \sum_{\substack{c<x/Q\\ \gcd(x,c)=1}} 1.$$

Hence, recalling (2.2), we derive that

$$\begin{aligned}\sum_{1\le c\le X/Q} \frac{1}{cQ} \sum_{\substack{cQ<x\le X\\ \gcd(x,cQ)=1}} f_c(x) &= Q^{-1} \sum_{\substack{Q<x\le X\\ \gcd(x,Q)=1}} \frac{\varphi(x)}{x} + O\left(X^{o(1)}\right)\\ &= F_2(Q,X) + O\left(X^{o(1)}\right).\end{aligned}$$

Thus, we see from (3.8) that

$$\#\Gamma_0^{1,1,1}(Q,X) = X\left(F_1(Q,X) + F_2(Q,X)\right) + O\left(X^{5/3+o(1)}Q^{-1}\right). \tag{3.9}$$

3.4 Counting $\Gamma^{-1,1,1}(Q,X)$

Recalling (3.1), we see that it remains to count $\Gamma_0^{-1,1,1}(Q,X)$. One can use a similar argument, but in fact, we show that

$$\#\Gamma^{-1,1,1}(Q,X) = \#\Gamma^{1,1,1}(Q,X) + O\left(\mathbf{E} + X\right), \tag{3.10}$$

where the error term $\mathbf{E} = O(X^{5/3+o(1)}Q^{-1})$ is the same as obtained above.

Thus, we wish to count matrices of the form

$$A = \begin{bmatrix} x & (xy-1)/cQ \\ cQ & y \end{bmatrix},$$

where $xy \equiv 1 \pmod{cQ}$, $-X \le x \le -1$, $1 \le y \le X$, $1 \le cQ \le X$ and $-X \le (xy-1)/cQ \le -1$.

Without loss of generality, we can assume that $X \notin \mathbb{Z}$. Then, we consider the following two cases.

Case I: $x > -cQ$. Note that for any x, y with $xy \equiv 1 \pmod{cQ}$, $-cQ < x \le -1$ and $1 \le y \le X$, we have

$$\frac{-cQX-1}{cQ} < \frac{xy-1}{cQ} \le \frac{-2}{cQ},$$

and so

$$\le \frac{xy-1}{cQ} \le -1.$$

Thus, indeed, the corresponding A is in $\Gamma_0^{-1,1,1}(Q,X)$. Note that since $0 < x + cQ \le cQ$ and $-X \le (xy-1)/cQ + y \le X$, we have that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} A = \begin{bmatrix} x+cQ & (xy-1)/cQ + y \\ cQ & y \end{bmatrix} \in \Gamma_0^{1,1,1}(Q,X).$$

So in fact, the number of such matrices A is exactly $G_1(c)$ as computed in (3.2) in the $\Gamma_0^{1,1,1}(Q,X)$ case.

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

Case II: $-X < x \le -cQ$. Let

$$\widetilde{f_c}(x) = \frac{-cQX+1}{x}.$$

We now need an analogue of Lemma 3.1. While the argument is very similar to that of the proof of Lemma 3.1, there are some differences, so we prefer to present it in full detail.

Lemma 3.2 *Fix* $1 \le c \le X/Q$, $0 < U \le X - cQ$. *Then the map*

$$\mathcal{T}_{\widetilde{f_c}}(cQ, -X, U) \to \Gamma_0^{-1,1,1}(Q, X)$$

given by

$$(x, y) \mapsto A = \begin{bmatrix} x & (xy-1)/cQ \\ cQ & y \end{bmatrix}$$

is well-defined, injective and its image is exactly the set of those $A \in \Gamma_0^{-1,1,1}(Q, X)$ *with* $-X < x \le -X + U$ *and bottom left entry equal to* cQ.

Proof Let $(x, y) \in \mathcal{T}_{\widetilde{f_c}}(cQ, -X, U)$. Thus, by definition,

$$0 < y \le \frac{-cQX+1}{x}.$$

As $x < -cQ$, we have that

$$\frac{-cQX+1}{x} = \frac{cQX-1}{-x} \le \frac{cQX-1}{cQ} < X$$

and so indeed $y \le X$. Moreover, as $x < 0$, we have

$$1 \ge \frac{1}{cQ} > \frac{xy-1}{cQ} \ge -X.$$

So indeed this mapping has range inside $\Gamma_0^{-1,1,1}(Q, X)$. Conversely, suppose

$$A = \begin{bmatrix} x & b \\ cQ & y \end{bmatrix}$$

is in $\Gamma_0^{-1,1,1}(Q, X)$ with $-X < x \le -X + U$. Then $-X \le b \le 0$ is an integer, thus $xy \equiv 1 \pmod{cQ}$ and

$$\le \frac{xy-1}{cQ} \le 0.$$

Thus, as $x < 0$, we have

$$\frac{-cQX+1}{x} \ge y.$$

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

Thus

$$0 < y \le \widetilde{f}_c(x)$$

and so indeed $(x, y) \in \mathcal{T}_{\widetilde{f}_c}(cQ, -X, U)$ as desired. ■

We now fix c with $1 \le c \le X/Q$ and observe now that by Lemma 3.2, for any $Z \in [-X, 0)$ and $0 < U \le |Z|$, we have that $T_{\widetilde{f}_c}(cQ, Z, U)$ has the main term

$$\begin{aligned}
\frac{2}{cQ} \sum_{\substack{Z < x \le Z+U \\ \gcd(x,q)=1}} \widetilde{f}_c(x) &= \frac{2}{cQ} \sum_{\substack{Z < x \le Z+U \\ \gcd(x,q)=1}} \frac{-cQX+1}{x} \\
&= \frac{2}{cQ} \sum_{\substack{-Z-U \le x < -Z \\ \gcd(x',q)=1}} \frac{cQX-1}{x} \\
&= \frac{2}{cQ} \sum_{\substack{-Z-U \le x < -Z \\ \gcd(x,q)=1}} f_c(x) \\
&= \frac{2}{cQ} \sum_{\substack{|Z|-U \le x < |Z| \\ \gcd(x,q)=1}} f_c(x),
\end{aligned}$$

where we recall $f_c(x) = (cQX-1)/x$ as used in Lemma 3.1. But this is precisely the same main term as for $T_{f_c}(cQ, |Z| - U, U)$ except for the boundary terms $(x = -Z - U, -Z)$ which contribute only $O(X)$ (uniformly in Q as $|(cQX-1)/x \le (cQX-1)/cQ \le X)$. Thus, recalling (3.4), (3.5), and (3.6), we see that for each admissible c, we obtain the contribution to $\#\Gamma^{-1,1,1}(Q, X)$, which is asymptotic to $G_2(c)$. Now observe that $\widetilde{f}_c(x) = -f_c(x)$ and so $|\widetilde{f}_c''(x)| = |f_c''(-x)|$ which means that the error terms we obtain from applying Lemma 2.2 to $\widetilde{f}_c$ are the same as those obtained for f_c (we have $x \in [-X, -cQ]$ and before we had $x \in [cQ, X]$). Thus, if we sum over c and proceed as before, we see that the error term is at most $O(\mathbf{E} + X)$ which implies (3.10).

3.5 Concluding the proof

Substituting (3.10) in (3.1) implies

$$\#\Gamma_0(Q, X) = 8\#\Gamma_0^{1,1,1}(Q, X) + O(X^{5/3+o(1)}Q^{-1} + X).$$

Recalling (3.9), we conclude the proof.

4 Proof of Theorem 1.2

4.1 Approximating $F_1(Q, X)$

For convenience, we let

$$G(Q, X) = \sum_{1 \le n \le X} \frac{\varphi(Qn)}{Qn}.$$

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

So

$$F_1(Q,X) = G(Q,Q^{-1}X). \tag{4.1}$$

We now define the function

$$h(n) = \mu(n)/n.$$

Lemma 4.1 *We have*

$$G(Q,X) = \frac{\varphi(Q)}{Q} \sum_{\substack{n\le X\\ \gcd(n,Q)=1}} h(n) \left\lfloor \frac{X}{n} \right\rfloor.$$

Proof Observe that for any integer $n \ge 1$,

$$\varphi(Qn) = Qn \prod_{p \mid Qn} \left(1 - p^{-1}\right) \qquad \text{and} \qquad \varphi(Q)n = Qn \prod_{p\mid Q} \left(1-p^{-1}\right).$$

Hence

$$\frac{\varphi(Qn)}{\varphi(Q)n} = \prod_{\substack{p\mid n\\ \gcd(p,Q)=1}} \left(1-p^{-1}\right).$$

Thus, we derive

$$\begin{aligned}\frac{Q}{\varphi(Q)} G(Q,X) &= \sum_{n\le X} \prod_{\substack{p\mid n\\ \gcd(p,Q)=1}} \left(1-p^{-1}\right) = \sum_{n\le X} \sum_{\substack{d\mid n\\ \gcd(d,Q)=1}} \frac{\mu(d)}{d}\\ &= \sum_{\substack{d\le X\\ \gcd(d,Q)=1}} \sum_{\substack{n\le X\\ d\mid n}} \frac{\mu(d)}{d} = \sum_{\substack{d\le X\\ \gcd(d,Q)=1}} \frac{\mu(d)}{d} \left\lfloor \frac{X}{d} \right\rfloor,\end{aligned}$$

which completes the proof. ∎

We now see from Lemma 4.1 that

$$\begin{aligned} G(Q,X) &= \frac{\varphi(Q)}{Q} X \sum_{\substack{n\le X\\ \gcd(n,Q)=1}} \frac{h(n)}{n} + O\left(\frac{\varphi(Q)}{Q} \sum_{n\le X} |h(n)| \right)\\ &= \frac{\varphi(Q)}{Q} X \sum_{\substack{n\le X\\ \gcd(n,Q)=1}} \frac{h(n)}{n} + O\left(\frac{\varphi(Q)}{Q} \log X \right).\end{aligned}$$

Using that

$$\sum_{n>X} \frac{|h(n)|}{n} \le \sum_{n>X} \frac{1}{n^2} = O\left(X^{-1}\right),$$

we write

$$G(Q,X) = \frac{\varphi(Q)}{Q} X \sum_{\substack{n=1\\ \gcd(n,Q)=1}}^{\infty} \frac{h(n)}{n} + O\left(\frac{\varphi(Q)}{Q} \log X \right). \tag{4.2}$$

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

Note that

$$\sum_{\substack{n\ge 1\\ \gcd(n,Q)=1}} \frac{h(n)}{n} = \prod_{\gcd(p,Q)=1}\left(1-\frac{1}{p^2}\right) = \prod_{p}\left(1-\frac{1}{p^2}\right)\prod_{p\mid Q}\left(1-\frac{1}{p^2}\right)^{-1}$$
$$= \frac{6}{\pi^2}\prod_{p\mid Q}\left(1-\frac{1}{p^2}\right)^{-1} = \frac{6}{\pi^2}\cdot\frac{Q}{\varphi(Q)}\cdot\frac{Q}{\psi(Q)}.$$

Thus, we see from (4.2) that

$$G(Q,X) = \frac{6Q}{\pi^2\psi(Q)}X + O\left(\frac{\varphi(Q)}{Q}\log X\right) \tag{4.3}$$

and so by (4.1), we derive

$$F_1(Q,X) = G(Q,Q^{-1}X) = \frac{6}{\pi^2\psi(Q)}X + O\left(\frac{\varphi(Q)}{Q}\log X\right). \tag{4.4}$$

4.2 Approximating $F_2(Q,X)$

We can now easily recover an estimate for $F_2(Q,X)$ originally derived in [13]. We do this for the sake of completeness as [13] is not easily available. Let

$$\delta_d(n) = \begin{cases} 1, & \text{if } d\mid n,\\ 0, & \text{if } d\nmid n,\end{cases}$$

be the characteristic function of the set of integer multiples of an integer $d\neq 0$. Then

$$\sum_{\substack{n\le X\\ \gcd(n,Q)=1}} \frac{\varphi(n)}{n} = \sum_{n\le X}\prod_{p\mid Q}\left(1-\delta_p(n)\right)\frac{\varphi(n)}{n} = \sum_{n\le X}\sum_{d\mid Q}\mu(d)\delta_d(n)\frac{\varphi(n)}{n}$$
$$= \sum_{d\mid Q}\mu(d)\sum_{n\le X/d}\frac{\varphi(dn)}{dn} = \sum_{d\mid Q}\mu(d)G(d,X/d).$$

We can now use (4.3) and then the multiplicativity of $\psi(d)$ to obtain

$$\sum_{\substack{n\le X\\ \gcd(n,Q)=1}} \frac{\varphi(n)}{n} = \frac{6}{\pi^2}X\sum_{d\mid Q}\mu(d)\frac{1}{\psi(d)} + O\left(\sum_{d\mid Q}|\mu(d)|\frac{\varphi(d)}{d}\log X\right)$$
$$= \frac{6}{\pi^2}X\prod_{p\mid Q}\left(1-\frac{1}{\psi(p)}\right) + O\left(2^{\omega(Q)}\log X\right)$$

since

$$\sum_{d\mid Q}|\mu(d)|\frac{\varphi(d)}{d} \le \sum_{d\mid Q}|\mu(d)| = 2^{\omega(Q)},$$

where $\omega(Q)$ is the number of prime divisors of Q.

https://doi.org/10.4153/S0008439524000365 Published online by Cambridge University Press

A simple computation shows that

$$\prod_{p\mid Q}\left(1-\frac{1}{\psi(p)}\right)=\prod_{p\mid Q}\left(1-\frac{1}{p+1}\right)=\prod_{p\mid Q}\frac{1}{1+p^{-1}}=\frac{Q}{\psi(Q)}.$$

Therefore

$$\frac{1}{Q}\sum_{\substack{n\le X\\ \gcd(n,Q)=1}}\frac{\varphi(n)}{n}=\frac{6}{\pi^2}\frac{X}{\psi(Q)}+O\left(2^{\omega(Q)}Q^{-1}\log X\right).$$

Therefore, using that $2^{\omega(Q)}\le\tau(Q)=Q^{o(1)}$, we obtain

$$\begin{aligned} F_2(Q,X)&=\frac{6}{\pi^2}\frac{X-Q}{\psi(Q)}+O\left(Q^{-1+o(1)}\log X\right)\\ &=\frac{6}{\pi^2}\frac{X}{\psi(Q)}+O\left(1+Q^{-1+o(1)}\log X\right),\end{aligned}\tag{4.5}$$

whence $\psi(Q)\ge Q$.

4.3 Concluding the proof

Combining the bounds (4.4) and (4.5), we obtain the desired result.

5 Comments

We presented our result, Corollary 1.3 as a direct consequence of Theorems 1.1 and 1.2 of very different nature with error terms of different strength. This makes it apparent that Theorem 1.1 is the bottleneck to further improvements of Corollary 1.3.

The methods of this work can also be used for counting elements of bounded norm of other congruence subgroup such as

$$\Gamma(Q)=\left\{\begin{bmatrix} a & b\\ c & d\end{bmatrix}\in \mathrm{SL}_2(\mathbb{Z}):\ a,d\equiv 1 \pmod Q,\ b,c\equiv 0 \pmod Q\right\}$$

and

$$\Gamma_1(Q)=\left\{\begin{bmatrix} a & b\\ c & d\end{bmatrix}\in \mathrm{SL}_2(\mathbb{Z}):\ a,d\equiv 1 \pmod Q,\ c\equiv 0 \pmod Q\right\}.$$

One can also adjust our approach to counting matrices of restricted size with respect to other natural matrix norms.

Acknowledgments The authors would like to thank Régis de la Bretèche for his suggestion which has led to the proof of Theorem 1.2 with the current error term. The authors are also very grateful to the referees for the very careful reading of the manuscript and very useful comments.

References

[1] S. Baier, *Multiplicative inverses in short intervals*. Int. J. Number Theory **9**(2013), 877–884.
[2] T. D. Browning and A. Haynes, *Incomplete Kloosterman sums and multiplicative inverses in short intervals*. Int. J. Number Theory **9**(2013), 481–486.
[3] K. Bulinski, A. Ostafe, and I. E. Shparlinski, *Counting embeddings of free groups into $SL_2(\mathbb{Z})$ and its subgroups*. Ann. Sc. Norm. Pisa, (to appear).
[4] T. H. Chan, *Shortest distance in modular hyperbola and least quadratic non-residue*. Mathematika **62**(2016), 860–865.
[5] M. Z. Garaev and I. E. Shparlinski, *On the distribution of modular inverses from short intervals*. Mathematika **69**(2023), 1183–1194.
[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 2008.
[7] P. Humphries, *Distributing points on the torus via modular inverses*. Quart. J. Math. **73**(2022), 1–16.
[8] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics, 17, American Mathematical Society, Providence, RI, 1997.
[9] A. Krieg, *Counting modular matrices with specified maximum norm*. Linear Algebra Appl. **196**(1994), 273–278.
[10] M. Newman, *Counting modular matrices with specified Euclidean norm*. J. Combin. Theory Ser. A **47**(1988), 145–149.
[11] H. N. Shapiro, *Introduction to the theory of numbers*, Wiley, New York, 1983.
[12] I. E. Shparlinski, *Modular hyperbolas*. Jpn. J. Math. **7**(2012), 235–294.
[13] D. Suryanarayana, *The greatest divisor of n which is prime to k*. Math. Student **37**(1969), 147–157.
[14] A. V. Ustinov, *On the number of solutions of the congruence $xy \equiv \ell \pmod q$ under the graph of a twice continuously differentiable function*. St. Petersburg Math. J. **20**(2009), 813–836 (translated from *Algebra i Analiz*).
[15] A. V. Ustinov, *On points of the modular hyperbola under the graph of a linear function*. Math. Notes **97**(2015), 284–288 (translated from *Matem. Zametki*).

School of Mathematics and Statistics, University of New South Wales, Sydney, UNSW 2052, Australia
e-mail: k.bulinski@unsw.edu.au igor.shparlinski@unsw.edu.au