Cesàro asymptotics for the orders of $SL_k(\mathbb{Z}_n)$ and $GL_k(\mathbb{Z}_n)$ as $n \to \infty$

Alexey G. Gorinov$^1$ and Sergey V. Shadchin$^2$

$^1$Université Paris 7, U.F.R. de Mathématiques, 2 place Jussieu, F-75251, France
$^2$IHES, Bures-sur-Yvette, route de Chartres, F-91140, France

Abstract

Given an integer $k > 0$, our main result states that the sequence of orders of the groups $SL_k(\mathbb{Z}_n)$ (respectively, of the groups $GL_k(\mathbb{Z}_n)$) is Cesàro equivalent as $n \to \infty$ to the sequence $C_1(k)n^{k^2-1}$ (respectively, $C_2(k)n^{k^2}$), where the coefficients $C_1(k)$ and $C_2(k)$ depend only on $k$; we give explicit formulas for $C_1(k)$ and $C_2(k)$. This result generalizes the theorem (which was first published by I. Schoenberg) that says that the Euler function $\varphi(n)$ is Cesàro equivalent to $\frac{6}{\pi^2}n$. We present some experimental facts related to the main result.

$^1$e-mail: gorinov@math.jussieu.fr
$^2$e-mail: chadtchi@ihes.fr
1 Introduction

The article is organized as follows: in section 2 we introduce some notation and formulate our main result. Then, in section 3 we prove this result. Finally, in section 4 we discuss some interesting related facts, in particular, some experimental facts.

The authors wish to thank V. I. Arnold for proposing this interesting problem and for useful discussions.

2 The main theorem

Two sequences of real numbers \((x_n)_{n \in \mathbb{N}}\) and \((y_n)_{n \in \mathbb{N}}\) are said to be Cesàro equivalent, if

\[
\lim_{n \to \infty} \frac{x_1 + \cdots + x_n}{y_1 + \cdots + y_n} = 1.
\]

For any finite set \(X\) we shall denote by \(#(X)\) the cardinality of \(X\). We shall use the symbol \(\prod_p\) to denote the product over all prime numbers.

Our main result is the following theorem.

**Theorem 2.1** For any fixed integer \(k > 0\) the sequence \((#(SL_k(\mathbb{Z}_n)))_{n \in \mathbb{N}}\) (respectively, the sequence \((#(GL_k(\mathbb{Z}_n)))_{n \in \mathbb{N}}\)) is Cesàro equivalent as \(n \to \infty\) to \(C_1(k)n^{k^2-1}\) (respectively, \(C_2(k)n^{k^2}\)), where \(C_1(1) = 1, C_2(1) = \prod_p \left(1 - \frac{1}{p^2}\right)\), and for any \(k > 1\) we have

\[
C_1(k) = \prod_p \left(1 - \frac{1}{p} \left(1 - \prod_{i=2}^{k} \left(1 - \frac{1}{p^i}\right)\right)\right),
\]

\[
C_2(k) = \prod_p \left(1 - \frac{1}{p} \left(1 - \prod_{i=1}^{k} \left(1 - \frac{1}{p^i}\right)\right)\right).
\]

**Remark.** In particular, \(#(GL_1(\mathbb{Z}_n))\) and \(#(SL_2(\mathbb{Z}_n))\) are Cesàro equivalent to \(\frac{n}{\zeta(2)}\) and \(\frac{n^3}{\zeta(3)}\) respectively. We do not know if the asymptotics given by Theorem 2.1 can be expressed in terms of values of the Riemann zeta-function (or any other remarkable function) at algebraic points in any of the other cases.

To the best of our knowledge, the fact that the Euler function \(\varphi(n) = #(GL_1(\mathbb{Z}_n))\) is Cesàro equivalent to \(n \frac{\phi}{\pi^2}\) was first published in [1] by I.
Schoenberg, who attributes the result to J. Schur. This result was probably already known to Gauss. An explicit formula for the cumulative distribution function of the sequence \( \left( \frac{\phi(n)}{n} \right)_{n \in \mathbb{N}} \) is given in [2] by B. A. Venkov.

3 Proof of Theorem 2.1

Let us first recall the explicit formulas for \( \#(SL_k(\mathbb{Z}_n)) \) and \( \#(GL_k(\mathbb{Z}_n)) \). For any positive integer \( k \) denote by \( \hat{\phi}_k \) the map \( \mathbb{N} \to \mathbb{R} \) given by the formula

\[
\hat{\phi}_k(p_1^{l_1} \cdots p_m^{l_m}) = \left(1 - \frac{1}{p_1^k}\right) \cdots \left(1 - \frac{1}{p_m^k}\right)
\]

(here \( p_1, \ldots, p_m \) are pairwise distinct primes).

Lemma 3.1 We have

\[
\#(GL_1(\mathbb{Z}_n)) = n\hat{\phi}_1(n),
\]

and for any integer \( k > 1 \) we have

\[
\#(SL_k(\mathbb{Z}_n)) = n^{k^2-1}\hat{\phi}_2(n) \cdots \hat{\phi}_k(n),
\]

\[
\#(GL_k(\mathbb{Z}_n)) = n^{k^2}\hat{\phi}_1(n) \cdots \hat{\phi}_k(n).
\]

Proof of Lemma 3.1 If \( p \) is prime, then

\[
\#(GL_k(\mathbb{Z}_p)) = (p^k - 1)(p^k - p) \cdots (p^k - p^{k-1}).
\]

The formula for \( \#(GL_k(\mathbb{Z}_n)) \) follows from the existence of the homomorphisms

\[
GL_k(\mathbb{Z}_p^l) \rightarrow GL_k(\mathbb{Z}_p^{l-1})
\]

(for any prime \( p \) and for any positive integer \( l \)), and from the fact that

\[
GL_k(\mathbb{Z}_{nm}) = GL_k(\mathbb{Z}_n) \times GL_k(\mathbb{Z}_m),
\]

if \( m \) and \( n \) are positive coprime integers. The formula for \( \#(SL_k(\mathbb{Z}_n)) \) is obtained from the formula for \( \#(GL_k(\mathbb{Z}_n)) \) using the determinant homomorphism.\( \diamond \)

\( ^{3} \)This notation can be explained as follows: the function \( \hat{\phi}_k \) generalizes the function \( n \mapsto \frac{\varphi(n)}{n} = \hat{\phi}_1(n) \).
Now let us calculate the limits of the averages of the sequences $(\tilde{\varphi}_1(n) \cdots \tilde{\varphi}_k(n))_{n \in \mathbb{N}}$ and $(\tilde{\varphi}_2(n) \cdots \tilde{\varphi}_k(n))_{n \in \mathbb{N}}$. More generally, let $\ell$ be a finite (nonempty) ordered collection of positive integers: $\ell = (i_1, \ldots, i_l)$. For any $n \in \mathbb{N}$ set

$$\tilde{\varphi}_\ell(n) = \tilde{\varphi}_{i_1}(n) \cdots \tilde{\varphi}_{i_l}(n).$$

For any sequence $x = (x_n)_{n \in \mathbb{N}}$ denote by $\langle x \rangle$ the Cesàro limit of $x$, i.e.,

$$\lim_{n \to \infty} \frac{1}{n} \sum_{m=1}^{n} x_m = \langle x \rangle.$$

**Theorem 3.2** For any $\ell = (i_1, \ldots, i_l)$ the limit $\langle \tilde{\varphi}_\ell \rangle$ exists and is equal to

$$\prod_p f_\ell \left( \frac{1}{p} \right),$$

where

$$f_\ell(t) = 1 - t(1 - \prod_{j=1}^{l} (1 - t^{i_j})).$$

*Sketch of a proof of Theorem 3.2.* We shall first give an informal proof of the theorem; we shall then show what changes should be made to make our informal proof rigorous.

The idea of the proof of Theorem 3.2 is to give a probabilistic interpretation to some complicated expressions (such as $\frac{1}{n} \sum_{m=1}^{n} \tilde{\varphi}_\ell(m)$). This idea goes back to Euler.

Let us note that for any positive integer $q$ the “probability” that a “random” positive integer is not a multiple of $q$ is

$$1 - \frac{1}{q}.$$

If $q_1$ and $q_2$ are coprime integers, the events “$r$ is not divisible by $q_1$” and “$r$ is not divisible by $q_2$” ($r$ being a “random” positive integer) are independent, which implies that for any positive integers $m, k$ the expression $\tilde{\varphi}_k(m)$ is the “probability” that a “randomly chosen” positive integer is not divisible by $k$-th powers of the prime divisors of $m$.

Analogously, for any fixed positive integer $m$ the expression $\tilde{\varphi}_\ell(m)$ can be seen as the “probability” to find an element

$$(x_1, \ldots, x_l) \in \mathbb{N}^l$$
that satisfies the following conditions: $x_1$ is not divisible by the $i_1$-th powers of the prime factors of $m$, $x_2$ is not divisible by the $i_2$-th powers of the prime factors of $m$ etc.

Using the total probability formula, we obtain that $\frac{1}{n} \sum_{m=1}^{n} \tilde{\varphi}_\ell(m)$ is the “probability” that a “random” element of the set

$$\{(x_0, x_1, \ldots, x_l)|x_0, \ldots, x_l \in \mathbb{N}, x_0 \leq n\}$$

satisfies the following condition: any $x_j, j = 1, \ldots, l$ is not divisible by the $i_j$-th powers of the prime divisors of $x_0$. So the limit $\langle \tilde{\varphi}_\ell \rangle$ is the “probability” of the limit event, which can be described as the intersection for all prime $p$ of the following events: “either ($x_0$ is not divisible by $p$), or (none of $x_j, j = 1, \ldots, l$ is divisible by $p^{i_j}$)”. These events are independent, and the “probability” of each of them is

$$f_\ell \left( \frac{1}{p} \right) = 1 - \frac{1}{p} \left( 1 - \prod_{j=1}^{l} \left( 1 - \frac{1}{p^{i_j}} \right) \right).$$

This gives the desired expression for $\langle \tilde{\varphi}_\ell \rangle$.

This idea is formalized as follows. Let $l$ be a positive integer, and let $A$ and $B$ be subsets of $\mathbb{N}^l$ such that there exists

$$\lim_{k \to \infty} \frac{\#(A \cap B \cap C_k)}{\#(B \cap C_k)},$$

where $C_k = \{(x_1, \ldots, x_l) \in \mathbb{N}^l|x_1 \leq k, \ldots, x_l \leq k\}$. This limit will be called the density of $A$ in $B$ and will be denoted by $p_B(A)$. For any $B \subset \mathbb{N}^l$ the correspondence $B \supset A \mapsto p_B(A)$ defines a measure on $B^4$.

Using the same argument as above (and replacing “probabilities” with “densities” and “events” with “sets”), we can represent $\frac{1}{n} \sum_{m=1}^{n} \tilde{\varphi}_\ell(m)$ as the density of a certain subset of the set

$$\{(x_0, x_1, \ldots, x_l)|x_0, \ldots, x_l \in \mathbb{N}, x_0 \leq n\}$$

This interpretation does not allow us to pass immediately to the limit as $n \to \infty$, but it enables us to write the following combinatorial formula for $\frac{1}{n} \sum_{m=1}^{n} \tilde{\varphi}_\ell(m)$. Define the sequence $(a_k)_{k \in \mathbb{N}}$ by the formula

$$\sum_{k=1}^{\infty} a_k t^k = 1 - \prod_{j} (1 - t^{i_j}).$$

Unfortunately, this measure is not $\sigma$-additive, which is why we prefer to speak rather of densities than of probabilities.
We have
\[
\frac{1}{n} \sum_{m=1}^{n} \tilde{\phi}_t(m) = 1 + \sum_{r=2}^{\infty} \frac{1}{r} (-1)^{pr(r)} a(r) b_{r,n},
\]
where for any \( r = p_{1}^{\alpha_1} \cdots p_{s}^{\alpha_s} \) we define
\[
pr(r) = s, \quad a(r) = a_{\alpha_1} \cdots a_{\alpha_s}, \quad b_{r,n} = \left[ \frac{n}{p_1 \cdots p_s} \right] \frac{1}{n}
\]
(in particular, \( a(r) = 0 \), if \( \max \{ \alpha_1, \ldots, \alpha_s \} > i_1 + \cdots + i_s \)). Now let us note that this expression has the form \( \sum_{k=1}^{\infty} b'_{k,n} c_r \), where \( c_k \) is the \( k \)-th term of the absolutely convergent series obtained by multiplying out the product
\[
\prod_{p} \left( 1 - \frac{1}{p} \left( 1 - \frac{l}{\prod_{j=1}^{l} \left( 1 - \frac{1}{p_{j}^{i_{j}}} \right)} \right) \right),
\]
and every \( b'_{k,n} \) has the form
\[
\frac{p_1 \cdots p_s}{n} \left[ \frac{n}{p_1 \cdots p_s} \right].
\]
We have \( 0 \leq b'_{k,n} \leq 1 \) for any \( k, n \), and the limit \( \lim_{n \to \infty} b'_{k,n} \) is equal to 1 for any \( k \). This implies Theorem 3.2.

Theorem 2.1 can be obtained from Theorem 3.2, from Lemma 3.1 and from the following lemma.

**Lemma 3.3** Let \( (x_n)_{n \in \mathbb{N}} \) be a sequence of real numbers, and suppose that \( \langle x \rangle \) exists. Then, for any nonnegative integer \( k \), we have
\[
\lim_{n \to \infty} \frac{x_1 + 2^k x_2 + \cdots + n^k x_n}{1 + 2^k + \cdots + n^k} = \langle x \rangle.
\]

**Proof of Lemma 3.3** The proof is by induction on \( k \). If \( k = 0 \), there is nothing to prove. Suppose Lemma 3.3 holds for some \( k \). For any sequence \( y = (y_n)_{n \in \mathbb{N}} \) set
\[
S_n^k[y] = y_1 + 2^k y_2 + \cdots + n^k y_n.
\]
We have
\[
S_n^k[x] = n^{k+1} \left( \frac{\langle x \rangle}{k+1} + \varepsilon_n, \right)
\]
where \((\varepsilon_n)_{n \in \mathbb{N}}\) is a sequence such that \(\lim_{n \to \infty} \varepsilon_n = 0\). Note that for any sequence \(y = (y_n)_{n \in \mathbb{N}}\) we have

\[(*) \quad S^{k+1}_n[y] = nS^k_n[y] - \sum_{m=1}^{n-1} S^k_m[y].\]

Thus, we can write

\[S^{k+1}_n[x] = \frac{\langle x \rangle}{k+1} \left( n^{k+2} - \sum_{m=1}^{n-1} m^{k+1} \right) + \varepsilon_n n^{k+2} - S^{k+1}_{n-1}[\varepsilon].\]

We have

\[\lim_{n \to \infty} \frac{S^{k+1}_{n-1}[\varepsilon]}{n^{k+2}} = 0,\]

and hence

\[\lim_{n \to \infty} \frac{S^{k+1}_n[x]}{n^{k+2}} = \frac{\langle x \rangle}{k+1} \left( 1 - \frac{1}{k+2} \right) = \frac{\langle x \rangle}{k+2},\]

which implies the statement of Lemma 3.3.

\[\diamondsuit\]

4 Convergence rates and the distribution of the values of \(\tilde{\varphi}_\ell\)

Let \(\ell\) be a finite (nonempty) ordered collection of positive integers: \(\ell = (i_1, \ldots, i_l)\). In this section we briefly discuss the convergence rate of the sequences

\[\left( \frac{1}{n^{s+1}} \sum_{k=1}^{n} k^s \tilde{\varphi}_\ell(k) \right)_{n \in \mathbb{N}}\]

for different fixed \(s \in \mathbb{N}\) and the distribution of the values of the function \(\tilde{\varphi}_\ell\).

Set

\[\Phi_\ell = \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \tilde{\varphi}_\ell(k) = \prod_p f_\ell \left( \frac{1}{p} \right),\]

\[\xi_{\ell,s}(n) = \frac{1}{n^s} \left( \sum_{k=1}^{n} k^s \tilde{\varphi}_\ell(n) - \frac{n^{s+1}}{s+1} \Phi_\ell \right).\]
It follows immediately from these definitions that
\[ \sum_{k=1}^{n} k^s \tilde{\phi}_\ell(k) = \frac{n^{s+1}}{s+1} \Phi_\ell + n^s \xi_{\ell,s}(n). \]

We have carried out computer experiments for \( \ell = (1), (2) \) and \((1, 2)\) and for \( s = 0, ..., 3 \). In all these cases the sequence \( \xi_{\ell,s} = (\xi_{\ell,s}(n))_{n \in \mathbb{N}} \) seems to be bounded. This means that the first relative correction to \( \Phi_\ell \) should be of order \( O \left( \frac{1}{n} \right) \). Computer tests suggest that the sequence \( \xi_{\ell,s} \) has no limit, but has a Cesàro limit, which is equal to \( \frac{1}{2} \Phi_\ell \) for every nonnegative integer \( s \). At this moment we are able to prove only the following weaker statement.

**Theorem 4.1** If \( \langle \xi_{\ell,0} \rangle \) exists, then for all integers \( s > 0 \) the limit \( \langle \xi_{\ell,s} \rangle \) exists and is equal to \( \frac{1}{2} \Phi_\ell \).

**Proof of Theorem 4.1** Set
\[ \eta_{\ell,s}(n) = \frac{1}{n^s} \sum_{k=1}^{n} k^s (\tilde{\phi}_\ell(k) - \Phi_\ell). \]
Note that \( \xi_{\ell,0} = \eta_{\ell,0} \), hence \( \langle \eta_{\ell,0} \rangle \) exists. Using formula \((\ast)\) we get
\[ \eta_{\ell,s+1}(n) = \eta_{\ell,s}(n) - \frac{1}{n^{s+1}} \sum_{k=1}^{n} k^s \eta_{\ell,s}(k). \]
Hence we obtain using Lemma 3.3 that \( \langle \eta_{\ell,s+1} \rangle = \frac{s}{s+1} \langle \eta_{\ell,s} \rangle \) for any integer \( s \geq 0 \). Thus, \( \langle \eta_{\ell,s} \rangle = 0 \) for any integer \( s > 0 \).

For any integer \( s \geq 1 \) we have
\[ \sum_{k=1}^{n} k^s = \frac{n^{s+1}}{s+1} + \frac{1}{2} n^s + O \left( n^{s-1} \right). \]
Hence we get the following relation:
\[ \xi_{\ell,s}(n) = \eta_{\ell,s}(n) + \frac{1}{2} \Phi_\ell + O \left( \frac{1}{n} \right), \]
which implies that \( \langle \xi_{\ell,s} \rangle = \frac{1}{2} \Phi_\ell \). The theorem is proven. \( \diamond \)
Let us now consider the distribution of the values of the function \( \tilde{\varphi}_\ell \). Using the argument from [1, §5], one can prove that for any \( t \in [0, 1] \) the limit
\[
\lim_{n \to \infty} \frac{1}{n} \# \{ k \in \mathbb{N} | k \leq n, \tilde{\varphi}_\ell(k) \leq t \}
\]
exists, and that the function \( F_\ell \) defined by the formula
\[
F_\ell(t) = \lim_{n \to \infty} \frac{1}{n} \# \{ k \in \mathbb{N} | k \leq n, \tilde{\varphi}_\ell(k) \leq t \}
\]
is continuous (I. Schoenberg considers only the case \( \ell = (1) \), but his argument can be easily extended to the case of an arbitrary \( \ell \)). The function \( F_\ell \) is the analogue of the cumulative distribution function in probability theory. Given a nonnegative integer \( s \), the \( s \)-th moment of \( F_\ell \) is defined as follows:
\[
\mu_{\ell,s} = \int_0^1 t^s dF_\ell(t).
\]
It is easy to prove (see [1 Satz I]) that \( \mu_{\ell,s} = \langle (\tilde{\varphi}_\ell)^s \rangle \). Due to Theorem 3.2 we have \( \mu_{\ell,s} = \Phi_\ell^s \) where \( \ell^s \) is the following collection of positive integers: \( \ell^s = (i_1, i_1, \ldots, i_1 \ (s \text{ times}), i_2, i_2, \ldots, i_2 \ (s \text{ times}), \ldots) \).

The Fourier series for \( F_\ell(t) \) is equal to \( \sum_{n \in \mathbb{Z}} u_n e^{2\pi int} \), where
\[
u_0 = 1 - \Phi_\ell = \frac{1}{2} - \sum_{k \neq 0} \frac{\langle e^{-2\pi i k \tilde{\varphi}_\ell} \rangle}{2\pi ik}
\]
(the sum of the series in the latter formula is to be taken in Cesàro sense), and the Fourier coefficients \( u_n \) for \( n \neq 0 \) can be calculated using either the formula
\[
u_n = -\sum_{m=1}^{\infty} \frac{(-2\pi in)^{m-1}}{m!} \Phi_{\ell^m},
\]
or the formula
\[
u_n = \frac{1}{2\pi in} (\langle e^{-2\pi in \tilde{\varphi}_\ell} \rangle - 1).
\]
Since \( F_\ell \) is continuous, its Fourier series converges in Cesàro sense to \( F_\ell \) uniformly on every compact subset of the open interval \((0, 1)\).
References

[1] I. Schoenberg, Über die asymptotische Verteilung reeller Zahlen mod 1, Math. Z. 28 (1928), 171-199.

[2] B. A. Venkov, On a certain monotonic function, Uchenye Zapiski Leningrad State Univ., Math. Ser. 111, fasc. 16 (1949), 3-19 (in Russian).