Number Theory/Algebra

Cesàro asymptotics for the orders of $\text{SL}_k(\mathbb{Z}_n)$ and $\text{GL}_k(\mathbb{Z}_n)$ as $n \to \infty$

Alexey G. Gorinov $^a$, Sergey V. Shadchin $^b$

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

Received 6 May 2003; accepted 20 May 2003

Presented by Vladimir Arnold

Abstract

Given an integer $k > 0$, our main result states that the sequence of orders of the groups $\text{SL}_k(\mathbb{Z}_n)$ (respectively, of the groups $\text{GL}_k(\mathbb{Z}_n)$) 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 $\phi(n)$ is Cesàro equivalent to $n^6 \pi^2$. We present some experimental facts related to the main result.

Résumé

Formules asymptotiques au sens de Cesàro pour les ordres de $\text{SL}_k(\mathbb{Z}_n)$ et $\text{GL}_k(\mathbb{Z}_n)$ quand $n \to \infty$. Fixons un entier $k > 0$. Notre résultat principal dit que la suite des ordres des groupes $\text{SL}_k(\mathbb{Z}_n)$ (respectivement, des groupes $\text{GL}_k(\mathbb{Z}_n)$) est équivalente au sens de Cesàro quand $n \to \infty$ à la suite $C_1(k)n^{k^2-1}$ (respectivement, $C_2(k)n^{k^2}$), où les coefficients $C_1(k)$ et $C_2(k)$ ne dépendent que de $k$ ; on donne des formules explicites pour $C_1(k)$ et $C_2(k)$. Ce résultat généralise le théorème (publié pour la première fois par I. Schoenberg) disant que la fonction d'Euler $\phi(n)$ est équivalente au sens de Cesàro à $n^6 \pi^2$. On présente quelques faits expérimentaux liés au résultat principal. Pour citer cet article : A.G. Gorinov, S.V. Shadchin, C. R. Acad. Sci. Paris, Ser. I 337 (2003).

0. Introduction

The article is organized as follows: in Section 1 we introduce some notation and formulate our main result. Then, in Section 2, we prove this result. Finally, in Section 3 we discuss some interesting related facts.

1. 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 $\lim_{n \to \infty} \frac{\sum_{i=1}^{n} x_i}{\sum_{i=1}^{n} y_i} = 1$. 

E-mail addresses: gorinov@math.jussieu.fr (A.G. Gorinov), chadtchi@ihes.fr (S.V. Shadchin).

doi:10.1016/S1631-073X(03)00328-5
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 1.1.** For any fixed integer \(k > 0\) the sequence \((#(SL_k(\mathbb{Z}_n)))_{n \in \mathbb{N}}\) (resp., the sequence \((#(GL_k(\mathbb{Z}_n)))_{n \in \mathbb{N}}\)) is Cesàro equivalent as \(n \to \infty\) to \(C_1(k)n^{k^2-1}\) (resp., \(C_2(k)n^{k^2}\)), where \(C_1(1) = 1\), \(C_2(1) = \prod_p (1 - \frac{1}{p^k})\), and for any \(k > 1\) we have

\[
C_1(k) = \prod_p \left( 1 - \frac{1}{p} \left(1 - k \prod_{i=2}^{k} \left(1 - \frac{1}{p^i}\right)\right) \right), \quad C_2(k) = \prod_p \left( 1 - \frac{1}{p} \left(1 - \prod_{i=1}^{k} \left(1 - \frac{1}{p^i}\right)\right) \right).
\]

**Remark.** In particular, \((#(GL_1(\mathbb{Z}_n)))\) and \((#(SL_2(\mathbb{Z}_n)))\) are Cesàro equivalent to \(\frac{n}{\zeta(2)}\) and \(\frac{n^2}{\zeta(2)}\) respectively. We do not know if the asymptotics given by Theorem 1.1 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 \(\psi(n) = #(GL_1(\mathbb{Z}_n))\) is Cesàro equivalent to \(n \frac{\phi(n)}{n}\) was first published in [1] by Schoenberg, who attributes the result to Schur. This result was probably already known to Gauss. An explicit formula for the cumulative distribution function of the sequence \((\psi(n)/n)_{n \in \mathbb{N}}\) is given in [2] by Venkov.

2. **Proof of Theorem 1.1**

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 \(\tilde{\psi}_k\)\(^1\) the map \(\mathbb{N} \to \mathbb{R}\) given by the formula \(\tilde{\psi}_k(p_1^{i_1} \cdots p_m^{i_m}) = (1 - 1/p_1^{i_1}) \cdots (1 - 1/p_m^{i_m})\) (here \(p_1, \ldots, p_m\) are pairwise distinct primes).

**Lemma 2.1.** We have \( #(SL_1(\mathbb{Z}_n)) = n \tilde{\psi}_1(n)\), and for any integer \(k > 1\) we have \( #(SL_k(\mathbb{Z}_n)) = n^{k^2 - 1} \tilde{\psi}_2(n) \cdots \tilde{\psi}_k(n)\), \( #(GL_k(\mathbb{Z}_n)) = n^{k^2} \tilde{\psi}_1(n) \cdots \tilde{\psi}_k(n)\).

The proof is an exercise in linear algebra. \(\square\)

Now let us calculate the limits of the averages of the sequences \((\tilde{\psi}_1(n) \cdots \tilde{\psi}_k(n))_{n \in \mathbb{N}}\) and \((\tilde{\psi}_2(n) \cdots \tilde{\psi}_k(n))_{n \in \mathbb{N}}\). 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 \(\tilde{\psi}_\ell(n) = \tilde{\psi}_{i_1}(n) \cdots \tilde{\psi}_{i_l}(n)\). For any sequence \(x = (x_n)_{n \in \mathbb{N}}\) denote by \(\langle x \rangle\) the Cesàro limit of \(x\), i.e., the limit

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{m=1}^{n} x_m.
\]

**Theorem 2.2.** For any \(\ell = (i_1, \ldots, i_l)\) the limit \(\langle \tilde{\psi}_\ell \rangle\) exists and is equal to \(\prod_p f_\ell\left(\frac{1}{p}\right)\), where \(f_\ell(t) = 1 - t(1 - \prod_{j=1}^{l} (1 - t^{1/i_j}))\).

**Sketch of a proof of Theorem 2.2.** 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 2.2 is to give a probabilistic interpretation to some complicated expressions (such as \(\frac{1}{n} \sum_{m=1}^{n} \tilde{\psi}_\ell(m)\)). This idea goes back to Euler.

\(^1\) This notation can be explained as follows: the function \(\tilde{\psi}_k\) generalizes the function \(n \mapsto \psi(n)/n = \tilde{\psi}_1(n)\).
Let us note that for any positive integer \( q \) the “probability” that a “random” positive integer is a not a multiple of \( q \) is \( 1 - 1/q \). 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 \( \hat{q}_k(m) \) 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 \( \hat{q}_k(m) \) 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 \( \frac{1}{n} \sum_{m=1}^{n} \hat{q}_k(m) \) is the “probability” that a “random” element of the set \( \{(x_0, x_1, \ldots, x_l) \mid x_0, \ldots, x_l \in \mathbb{N}, x_0 \leq n \} \) 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 \( \langle \hat{q}_k \rangle \) is the “probability” of the limit event, which can be described as the intersection for all prime \( p \) of the following events: “\( x_0 \) 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 \( f_\ell(\frac{1}{p}) = 1 - \frac{1}{p} \left(1 - \prod_{j=1}^{l} (1 - \frac{1}{p^{i_j}})\right) \). This gives the desired expression for \( \langle \hat{q}_k \rangle \).

This idea is formalized as follows. Let \( I \) be a positive integer, and let \( A \) and \( B \) be subsets of \( \mathbb{N} \) such that there exists \( \lim_{n \to \infty} \frac{|A \cap B(n)|}{|B(n)|} \), where \( B(n) = (x_1, \ldots, x_k) \in \mathbb{N}^k \mid x_i \leq n \). This limit will be called the density of \( A \) in \( B \) and will be denoted by \( p_B(A) \). For any \( B \subset \mathbb{N} \) the correspondence \( B \supset A \mapsto p_B(A) \) defines a measure on \( B \).

Using the same argument as above (and replacing “probabilities” with “densities” and “events” with “sets”), we can represent \( \frac{1}{n} \sum_{m=1}^{n} \hat{q}_k(m) \) as the density of a certain subset of the set \( \{(x_0, x_1, \ldots, x_l) \mid x_0, \ldots, x_l \in \mathbb{N}, x_0 \leq n \} \). 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 \( \frac{1}{n} \sum_{m=1}^{n} \hat{q}_k(m) \). Define the sequence \( (a_k)_{k \in \mathbb{N}} \) by the formula \( \sum_{k=1}^{\infty} a_k k^t = 1 - \prod_{j=1}^{l} (1 - t^{i_j}) \). We have \( \frac{1}{n} \sum_{m=1}^{n} \hat{q}_k(m) = 1 + \sum_{r=2}^{\infty} \frac{1}{r} (-1)^{pr(r)} a(r) b_{r,n} \), where for any \( r = p_1^{a_1} \cdots p_s^{a_s} \) we define \( pr(r) = a_1 \cdots a_s \), \( b_{r,n} = [\prod_{j=1}^{l} (1 - \frac{1}{p_j^{i_j}})] \) (in particular, \( a(r) = 0 \), if \( \max\{a_1, \ldots, a_s\} > i_1 + \cdots + i_l \)). Now let us note that this expression has the form \( \sum_{k=1}^{\infty} b'_i n^r \), where \( c_k \) is the \( k \)-th term of the absolutely convergent series obtained by multiplying out the product \( \prod_{j=1}^{l} (1 - \frac{1}{p_j^{i_j}}) \), and every \( b'_{i,n} \) has the form \( \frac{\prod_{p|n} (1 - \frac{1}{p^{i_p}})}{\prod_{p|n} (1 - \frac{1}{p^{i_p}})} \). We have \( 0 \leq b'_{i,n} \leq 1 \) for any \( k, n \), and the limit \( \lim_{n \to \infty} b'_{i,n} \) is equal to 1 for any \( k \). This implies Theorem 2.2.

Theorem 1.1 can be obtained from Theorem 2.2, from Lemma 2.1 and from the following lemma.

**Lemma 2.3.** 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 \( \lim_{n \to \infty} \frac{x_1 + x_2 + \cdots + x_n}{1 + 2^k + \cdots + n^k} = \langle x \rangle \).

**Proof of Lemma 2.3.** The proof is by induction on \( k \). If \( k = 0 \), there is nothing to prove. Lemma 2.3 holds for some \( k \). For any sequence \( y = (y_n)_{n \in \mathbb{N}} \) set \( S^k_n[y] = y_1 + 2^k y_2 + \cdots + n^k y_n \). We have \( S^k_n[x] = n^{k+1} \langle \frac{x}{k+1} + \varepsilon_n \rangle \), 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 \( S^{k+1}_n[y] = S^k_n[y] - \sum_{m=1}^{n-1} e_m^k[y] \).

Thus, we can write \( S^{k+1}_n[x] = \langle \frac{x}{k+1} (n^{k+2} - \sum_{m=1}^{n-1} m^{k+1}) + \varepsilon_n n^{k+2} - S^{k+1}_n[x] \rangle \). We have \( \lim_{n \to \infty} \frac{S^{k+1}_n[x]}{n^{k+2}} = 0 \), and hence \( \lim_{n \to \infty} \frac{S^{k+1}_n[x]}{n^{k+2}} = \langle \frac{x}{k+1} (1 - \frac{1}{k+2}) \rangle = \langle \frac{x}{k+2} \rangle \), which implies the statement of Lemma 2.3.
3. Convergence rates and the distribution of the values of \( \tilde{\varphi}_t \)

Let \( t \) 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 \( \frac{1}{\pi^*} \sum_{k=1}^n k^s \tilde{\varphi}_t(k) \) for different fixed \( s \in \mathbb{N} \) and the distribution of the values of the function \( \tilde{\varphi}_t \).

Set \( \Phi_t = \lim_{n \to \infty} \frac{1}{\pi^*} \sum_{k=1}^n \tilde{\varphi}_t(k) = \prod_p f_t(\frac{1}{p}) \), \( \xi_{t,s}(n) = \frac{1}{\pi^*} \sum_{k=1}^n k^s \tilde{\varphi}_t(n) - \frac{n^{s+1}}{s+1} \Phi_t \). It follows immediately from these definitions that \( \sum_{k=1}^n k^s \tilde{\varphi}_t(k) = \frac{\xi_{t,s}(n)}{\pi^*} + n^s \xi_{t,s}(n) \).

**Theorem 3.1.** If \( \langle \xi_{t,0} \rangle \) exists, then for all integers \( s > 0 \) the limit \( \langle \xi_{t,s} \rangle \) exists and is equal to \( \frac{1}{2} \Phi_t \).

**Proof of Theorem 3.1.** Set \( \eta_{t,s}(n) = \frac{1}{\pi^*} \sum_{k=1}^n k^s (\tilde{\varphi}_t(k) - \Phi_t) \). Note that \( \xi_{t,0} = \eta_{t,0} \), hence \( \langle \eta_{t,0} \rangle \) exists. Using formula (\( \ast \)) we get \( \eta_{t,s+1}(n) = \eta_{t,s}(n) - \frac{n^{s+1}}{s+1} \Phi_t \). Hence we obtain using Lemma 2.3 that \( \langle \eta_{t,s} \rangle = \frac{\xi_{t,s}(n)}{\pi^*} \) for any integer \( s \geq 0 \). Thus, \( \langle \eta_{t,s} \rangle = 0 \) for any integer \( s > 0 \).

For any integer \( s \geq 1 \) we have \( \sum_{k=1}^n k^s = \frac{n^{s+1}}{s+1} + \frac{1}{2} n^s + O(n^{s-1}) \). Hence we get the following relation: \( \xi_{t,s}(n) = \eta_{t,s}(n) + \frac{1}{2} \Phi_t + O(n) \), which implies that \( \langle \xi_{t,s} \rangle = \frac{1}{2} \Phi_t \). The theorem is proven. \( \square \)

Let us now consider the distribution of the values of the function \( \tilde{\varphi}_t \). Using the argument from [1, §5], one can prove that for any \( t \in [0, 1] \) the limit \( \lim_{n \to \infty} \frac{1}{\pi^*} \sum_{k=1}^n k^s \tilde{\varphi}_t(k) \) exists, and that the function \( F_t \) defined by the formula \( F_t(t) = \lim_{n \to \infty} \frac{1}{\pi^*} \sum_{k=1}^n k \tilde{\varphi}_t(k) \) 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 \( F_t \) is the analogue of the cumulative distribution function in probability theory. Given a nonnegative integer \( s \), the \( s \)-th moment of \( F_t \) is defined as follows: \( \mu_{t,s} = \int_0^t t^s dF_t(t) \). It is easy to prove (see [1, Satz I]) that \( \mu_{t,s} = \langle (\tilde{\varphi}_t)^s \rangle \). Due to Theorem 2.2, we have \( \mu_{t,s} = \Phi_t \) where \( \ell^s \) is the following collection of positive integers: \( \ell^s = (i_1, i_1, \ldots, i_1) \) \( (s \) times\), \( i_2, i_2, \ldots, i_l \) \( (s \) times\), \( \ldots \).

The Fourier series for \( F_t(t) \) is equal to \( \sum_{n \in \mathbb{Z}} u_n e^{2\pi i n t} \), where \( u_0 = 1 - \Phi_t = \frac{1}{\pi^*} - \sum_{k \neq 0} \frac{(e^{-2\pi i \tilde{\varphi}_t})}{2\pi i k} \) (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 \( u_n = -\sum_{m=1}^{\infty} \frac{(e^{-2\pi i \tilde{\varphi}_t})^{m-1}}{2\pi i m} \Phi_{t^m} \), or the formula \( u_n = \frac{1}{\pi^*} (e^{-2\pi i \tilde{\varphi}_t} - 1) \). Since \( F_t \) is continuous, its Fourier series converges in Cesàro sense to \( F_t \) uniformly on every compact subset of the open interval \((0, 1)\).

**Note added in proof.** Recently we proved that for any \( t = (i_1, \ldots, i_l) \) such that all \( i_j > 1 \), the limit \( \langle \xi_{t,0} \rangle \) exists and \( \langle \xi_{t,0} \rangle = \frac{1}{2} \Phi_t - \frac{1}{\pi^*} \sum_{(i_1, \ldots, i_l)} \xi_{t,i_1} \cdots \xi_{t,i_l} \). After the article has been accepted for publication, we learn from P. Moree an alternative proof of Theorem 1.1 based on a lemma in [3, p. 108] (the proof of that lemma given in [1] is due to Erdős).

**Acknowledgements**

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

**References**