Journal of Number Theory 133 (2013) 3578–3588

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On a uniformly distributed phenomenon in matrix groups

Su Hu [a], Yan Li [b,*]

[a] Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. West, Montréal, Québec, H3A 2K6, Canada
[b] Department of Applied Mathematics, China Agriculture University, Beijing 100083, China

ARTICLE INFO

Article history:
Received 25 February 2013
Revised 15 April 2013
Accepted 15 April 2013
Available online 5 July 2013
Communicated by Dinesh S. Thakur

MSC:
11C20
11T23

Keywords:
Matrices
Finite fields
Uniform distribution
Character sum

ABSTRACT

We show that a classical uniformly distributed phenomenon for an element and its inverse in $(\mathbb{Z}/n\mathbb{Z})^*$ also exists in $\mathrm{GL}_n(\mathbb{F}_p)$. A $\mathrm{GL}_n(\mathbb{F}_p)$ analogy of the uniform distribution on modular hyperbolas has also been considered.

1. Introduction

The distance between an element $x \in (\mathbb{Z}/n\mathbb{Z})^*$ and its inverse x^{-1} (mod n) has been studied by many authors [1,4,11,18,20–22]. Shparlinski [16] gave a survey of a variety of recent results about the distribution and some geometric properties of points (x, y) on modular hyperbolas $xy \equiv a$ (mod n).

Denote by $\{x\}$ the fractional part of a real number x. Let

$$f_n : (\mathbb{Z}/n\mathbb{Z})^* \to [0, 1] \times [0, 1],$$
$$x \mapsto \left(\left\{\frac{x}{n}\right\}, \left\{\frac{x^{-1}}{n}\right\}\right).$$

* Corresponding author.
E-mail addresses: hus04@mails.tsinghua.edu.cn, hu@math.mcgill.ca (S. Hu), liyan_00@mails.tsinghua.edu.cn (Y. Li).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.04.020

By using the Erdös–Turán–Koksma inequality and the Weil–Estermann inequality for Kloosterman sum, Beck and Khan [1] gave an elegant proof for the following classical result.

Theorem 1.1. *Let $R \subset [0,1]^2$ be a measurable set having the following property that for every $\epsilon > 0$, there exist two finite collections of non-overlapping rectangles $R_1, \ldots, R_k$ and $R^1, \ldots, R^l$ such that $\bigcup_{i=1}^k R_i \subseteq R \subseteq \bigcup_{j=1}^l R^j$, $\operatorname{area}(R/\bigcup_{i=1}^k R_i) < \epsilon$ and $\operatorname{area}(\bigcup_{j=1}^l R^j/R) < \epsilon$. Then*

$$\lim_{n\to\infty} \frac{\text{cardinality}(\text{Image}(f_n) \cap R)}{\varphi(n)} = \operatorname{area}(R).$$

Remark 1.2. Notice that our statement of the above theorem is slightly different from the statement in Beck and Khan [1]. The statement in [1] is as follows:

"Let $R \subseteq [0,1]^2$ be a measurable set having the following property that for every $\epsilon > 0$, there exists a finite collection of non-overlapping rectangles $\{R_1, R_2, \ldots, R_k\}$ such that $\bigcup_{i=1}^k R_i \subseteq R$ and $\operatorname{area}(R/\bigcup_{i=1}^k R_i) < \epsilon$. Then

$$\lim_{n\to\infty} \frac{\text{cardinality}(\text{Image}(f_n) \cap R)}{\varphi(n)} = \operatorname{area}(R).\text{''}$$

(See Theorem 2 of [1].)

The original assumption should be strengthened. Otherwise there is a counterexample as follows:

Let $R_1 = [0,1/2)^2$ and $R_2 = \{(x,y) \in [0,1]^2 \mid x, y \in \mathbb{Q}\}$. Denote by $R = R_1 \cup R_2$. Since $\operatorname{area}(R_2) = 0$, we have $\operatorname{area}(R) = \operatorname{area}(R_1) = 1/4$. So R satisfies the conditions in the statement of Theorem 2 in [1]. Since the image of f_n are rational points in $[0,1]^2$ and R contains all the rational points in $[0,1]^2$, we have $\text{Image}(f_n) \cap R = \varphi(n)$ for any positive integer n, thus

$$\lim_{n\to\infty} \frac{\text{cardinality}(\text{Image}(f_n) \cap R)}{\varphi(n)} = 1.$$

But $\operatorname{area}(R) = \operatorname{area}(R_1) = 1/4$, so

$$\lim_{n\to\infty} \frac{\text{cardinality}(\text{Image}(f_n) \cap R)}{\varphi(n)} \neq \operatorname{area}(R).$$

Notice that, the new conditions in Theorem 1.1 are quite natural. Numerous types of regions satisfy the conditions of Theorem 1.1 such as polygons, disks, annuli lying in the unit square.

Beck and Khan [1, p. 150] remarked that: "In all likelihood this theorem dates back to the late 20's and early 30's and was known to mathematicians such as Davenport, Estermann, Kloosterman, Salie."

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ be the finite field with p elements, $M_n(\mathbb{F}_p)$ be the set of all $n \times n$ matrices over $\mathbb{F}_p$, $\mathrm{GL}_n(\mathbb{F}_p)$, $\mathrm{SL}_n(\mathbb{F}_p)$ and $\mathcal{Z}_n(\mathbb{F}_p)$ be the group of invertible matrices, the group of matrices of determinant 1 and the set of singular matrices, respectively, where all matrices are from $M_n(\mathbb{F}_p)$.

In this paper, by using bounds of Ferguson, Hoffman, Ostafe, Luca and Shparlinski [3] for the matrix analogue of classical Kloosterman sums (see Lemma 2.1 below), we show that the above mentioned uniformly distributed phenomenon also exists in $\mathrm{GL}_n(\mathbb{F}_p)$.

For $A = (\overline{a_{ij}}) \in \mathrm{GL}_n(\mathbb{F}_p)$, $A^{-1} = (\overline{b_{ij}})$ denotes the inverse of A.

Let

$$g_p : \mathrm{GL}_n(\mathbb{F}_p) \to \underbrace{[0,1] \times [0,1] \times \cdots \times [0,1]}_{2n^2}, \tag{1.1}$$