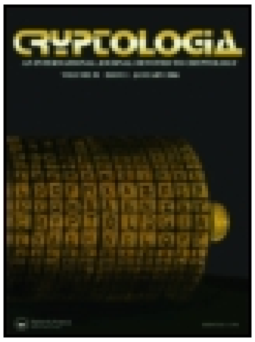

Cryptologia

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ucry20

Sidon sets and statistics of the ElGamal function

Lucas Boppré Niehues , Joachim von zur Gathen , Lucas Pandolfo Perin & Ana Zumalacárregui

To cite this article: Lucas Boppré Niehues , Joachim von zur Gathen , Lucas Pandolfo Perin & Ana Zumalacárregui (2020): Sidon sets and statistics of the ElGamal function, Cryptologia, DOI: 10.1080/01611194.2020.1790128

To link to this article: https://doi.org/10.1080/01611194.2020.1790128

Published online: 16 Jul 2020.

CRYPTOLOGIA
https://doi.org/10.1080/01611194.2020.1790128

Taylor & Francis
Taylor & Francis Group

Sidon sets and statistics of the ElGamal function

Lucas Boppré Niehues, Joachim von zur Gathen, Lucas Pandolfo Perin, and Ana Zumalacárregui

ABSTRACT

In the ElGamal signature and encryption schemes, an element x of the underlying group $G = \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$ for a prime p is also considered as an exponent, for example in g^x, where g is a generator of G. This *ElGamal map* $x \mapsto g^x$ is poorly understood, and one may wonder whether it has some randomness properties. This work presents two pieces of evidence for randomness. Firstly, experiments with small primes suggest that the map behaves like a uniformly random permutation with respect to two properties that we consider. Secondly, the theory of Sidon sets shows that the graph of this map is equidistributed in a suitable sense. It remains an open question to prove more randomness properties, for example, that the ElGamal map is pseudorandom.

KEYWORDS
Sidon set; ElGamal signature; equidistribution; cyclestructure; random permutation

1. Introduction

A basic requirement in modern cryptography are the random values needed to generate keys, nonces, and other values. But our computers and their usual models are deterministic machines that cannot, for reasons of principle, generate uniformly random values. A powerful methodology overcomes this obstacle: pseudorandomness.

Starting with only few uniformly random values—which must come from other sources, say physical generators—a pseudorandom generator (prg) produces an arbitrarily large amount of output that is indistinguishable from uniformly random values by any efficient (that is, polynomial-time) algorithm such as a cryptosystem. Thus pseudorandom values are as good as uniformly random ones for cryptographic purposes. Distinguishing here means that the algorithm can request an arbitrarily long sequence of values which are either all from the generator or all uniformly random, and then has to tell which of the two is the case. The algorithm is successful if its answer is correct with non-negligible probability, that is, there exists a polynomial f so that this probability is more than $1/f(n)$, where n is the size parameter. These asymptotic notions assume that the generator is defined for infinitely many n. The current state of mathematics and

CONTACT Joachim von zur Gathen gathen@bit.uni-bonn.de B-IT, Universität Bonn, Bonn, Germany.

computer science, say the open P vs. NP question, only allows to show the desired property by assuming that some computational problem is hard; factoring integers and computing discrete logarithms are two such candidates.

Any bias of a prg is negligible, since otherwise the bias would be efficiently detectable. Thus pseudorandomness implies (approximate) equidistribution. The converse is false. For example, linear congruential generators are usually equidistributed but not pseudorandom at all.

Alas, few prg's are known and it is hard to come up with new ones. It is easier (but still not always easy) to study the weaker property of equidistribution. The present paper does this for the ElGamal function which is suspected to be pseudorandom, but so far efforts to prove this have been unsuccessful. Theorem 3.1 shows the following property: ElGamal values (g^x, x) in a (sufficiently large) box $B = I \times J$ given by two intervals I and J are indeed close to being equidistributed, that is, there are about $\#B/p$ many of them, with an explicit error term of $50p^{1/2}\log^2 p$.

We now describe the ElGamal signature scheme (ElGamal 1985) with size parameter n. One takes an n-bit number d and a cyclic group $G = \langle g \rangle$ of order d. In ElGamal's original proposal, p is an n-bit prime number, $G = \mathbb{Z}_p^\times = \{1, \ldots, p-1\}, d = p-1$, and $\mathbb{Z}_d = \{1, \ldots, d\}$ is the *exponent group*. More commonly, one takes $\mathbb{Z}_d = \{0, \ldots, d-1\}$, but both are valid sets of representatives. We let g be a generator of G, so that $G = \{g^b : b \in \mathbb{Z}_d\}$. The object of this paper is to investigate randomness properties of the *ElGamal map* from G to G with $x \mapsto g^x$, where $x \in \mathbb{Z}_d$ on the right hand side. Since g^x determines x uniquely, this is a permutation of G. If we consider $x \in \mathbb{Z}_d$ on the left hand side, it is the discrete exponentiation map in base g. This map is trivial from a computer science point of view, but does not seem to have any mathematical structure.

A secret global key $a \in \mathbb{Z}_d$ and session key $k \in \mathbb{Z}_d^\times$ are chosen uniformly at random, and their public versions $A = g^a$ and $K = g^k$ in G are published. The signature of a message $m \in \mathbb{Z}_d$ is (K, b) with $b = k^{-1}(m - aK) \in \mathbb{Z}_d$.

The private key is easily broken if discrete logarithms in G can be calculated efficiently, since then the secret a and k can be calculated from the public A and K. For more details, see von zur Gathen (2015), Sections 8.2 and 9.8.

Related work by Cobeli, Vâjâitu, and Zaharescu (2002) studies distributions of the difference $x - g^x$ and of the function $x \mapsto ux + vg^x$ for fixed u and v. This includes the ElGamal function as a special case. The present work improves their result with an error term of $50p^{1/2}\log^2 p$ instead of their $O(p^{1/2}\log^3 p)$ and thus provides an explicit bound for the ElGamal distribution, which they only do for $x - g^x$. Both approaches are based on exponential sums, but Sidon sets, as used here, seem to provide a simpler tool than general bounds. This may prove useful in further work on such distribution questions.

The Decisional Diffie-Hellman (DDH) problem is to decide whether, given a triple $(x, y, z) \in G^3$, there exist $a, b \in \mathbb{Z}_d$ so that $x = g^a, y = g^b$, and $z = g^{ab}$; then (x, y, z) is a *Diffie-Hellman triple.*

If such triples are indistinguishable from uniformly random triples, for uniformly random a and b, then the ElGamal encryption scheme is indistinguishable by public key only attacks. The results of Canetti, Friedlander, Konyagin, Larsen, Lieman, and Shparlinski (Canetti et al. 2000), indicate that the most significant and least significant bits of each element in DDH triples are indeed distributed uniformly. Do the pairs (x, g^x), for uniformly random x, exhibit a similar behavior?

This paper first gives some experimental evidence in favor of this conjecture. We take some small primes, just above 1000, and consider two parameters of permutations: the number of cycles and the number of k-cycles for given k. Their averages for random permutations are well-known, and we find that the average values for the ElGamal function are reasonably close to those numbers. Secondly, we use the theory of Sidon sets to prove an equidistributional property with appropriate parameters.

Martins and Panario (2016) study similar questions, but for general polynomials that need not be permutations, and for different parameters. Konyagin et al. (2016) consider enumerative and algorithmic questions about (non-)isomorphic functional graphs, and Mans et al. (2019) provide statistics, conjectures, and results about cycle lengths of quadratic polynomials over finite prime fields. Kurlberg, Luca, and Shparlinski (2015) and Felix and Kurlberg (2017) deal with fixed points of the map $x \mapsto x^x$ modulo primes.

2. Experiments in $\mathbb{F}_p$

The table below shows the cycle structure of 12 permutations $x \mapsto g^x$ in $\mathbb{F}_p^\times$ with $p = 1009$ and the 12 smallest generators g. In the pictorial representation of Figure 1, each oval corresponds to a cycle whose length is proportional to the oval's circumference. For each g, the smaller ovals are placed arbitrarily inside or next to the largest one. By their nature, experiments only give a limited insight into such asymptotic questions. For primes of cryptographically relevant size, the required computations are infeasible.

In the following subsections, we take the cycle structures for all $\phi(1008) = 288$ generators of $\mathbb{F}_{1009}^\times$, and then of all generators for the first fifty primes larger than 1000. We calculate the averages for the number of cycles and the number of k-cycles and compare them to the known values

Generator	Cycle lengths
11	2, 2, 3, 9, 34, 69, 207, 330, 352
17	1, 184, 823
22	1, 14, 37, 49, 90, 104, 298, 415
26	1, 1, 1, 3, 3, 4, 4, 7, 24, 38, 228, 694
31	1, 2, 3, 18, 42, 211, 292, 439
33	1, 2, 14, 15, 28, 948
34	2, 19, 118, 172, 209, 488
38	12, 13, 47, 936
46	1, 2, 11, 12, 15, 20, 22, 50, 112, 151, 245, 367
51	1, 1, 2, 2, 6, 10, 17, 46, 265, 658
52	1, 2, 3, 6, 13, 15, 16, 20, 32, 135, 765
53	1, 3, 3, 4, 9, 99, 889

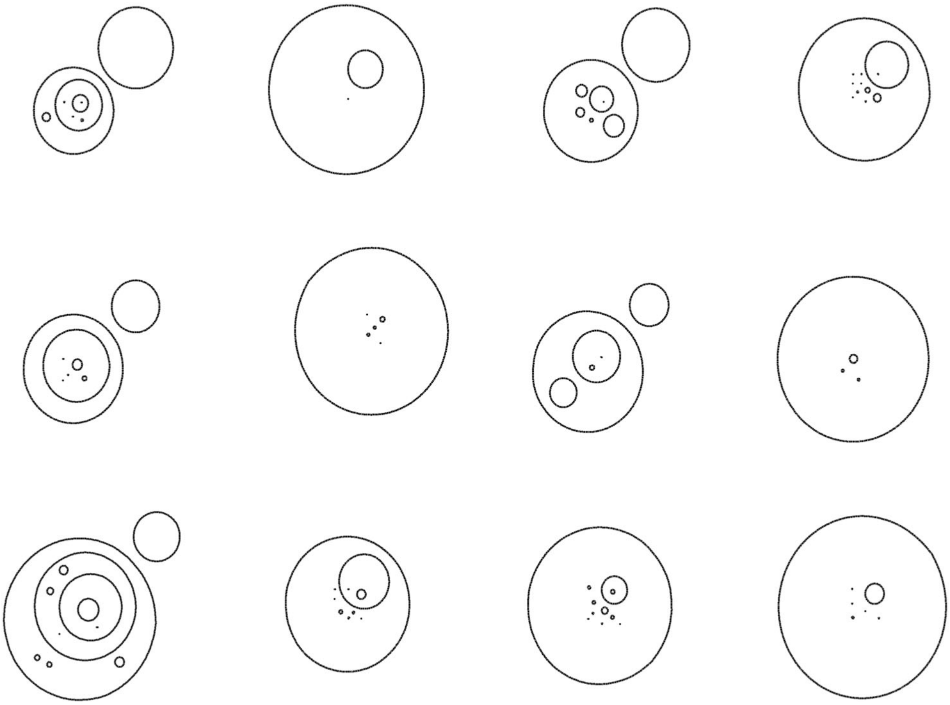

Figure 1. Graphical presentation of 12 permutations $x \mapsto g^x$ in $\mathbb{F}_{1009}$.

for random permutations. By their nature, such experiments can only give a limited insight into an asymptotic question.

2.1. Number of cycles in permutations

We study in detail the number of cycles in the permutations. The number of permutations in S_n with c cycles equals the Stirling number $s(n, c)$ of the first kind, and thus is the coefficient of x^c in the falling factorial $x_n = x \cdot (x-1) \cdots (x-n+1)$ (Wilf 1990, Section 3.5). Figure 2 shows the

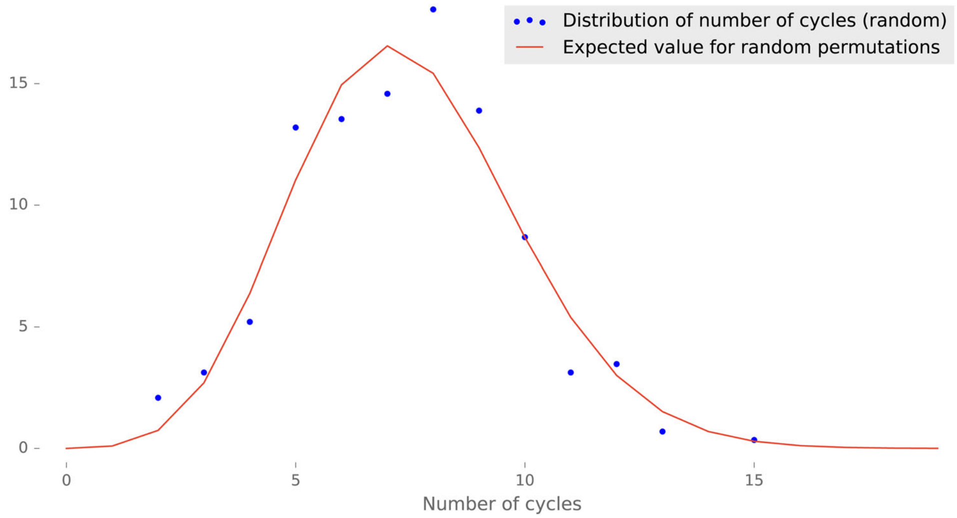

Figure 2. Distribution in percent of number of cycles for 288 uniformly random permutations in S_{1009}.

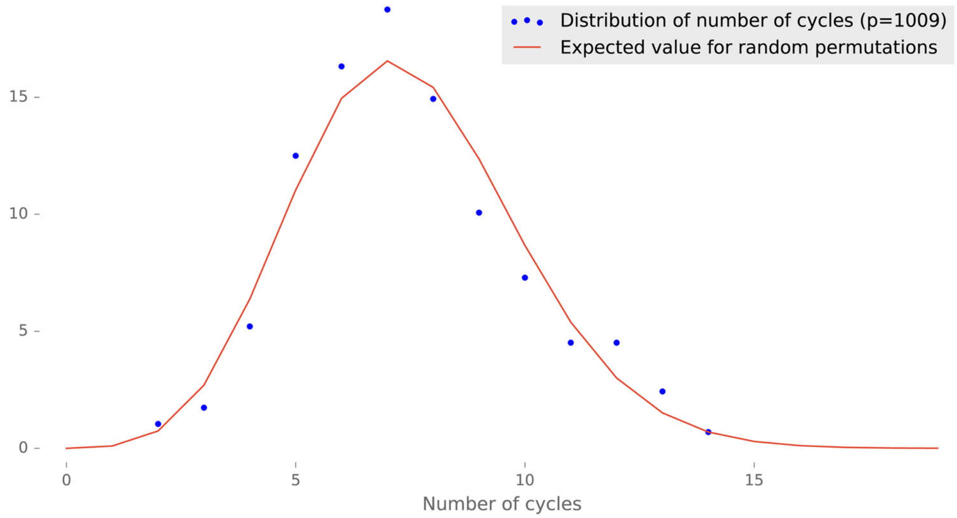

Figure 3. Distribution of number of cycles in ElGamal functions on $\mathbb{F}_{1009}$.

distribution of the number of cycles for uniformly random permutations of n elements, that is, the fraction $s(n, c)/n!$ (in percent) for $n = 1009$ and $1 \leq c \leq 20,$ as a continuous line. In the same figure, experimental statistics for 288 permutations chosen uniformly at random are presented as dots. This was done in order to calibrate our expectations. Theory and experiments match quite well.

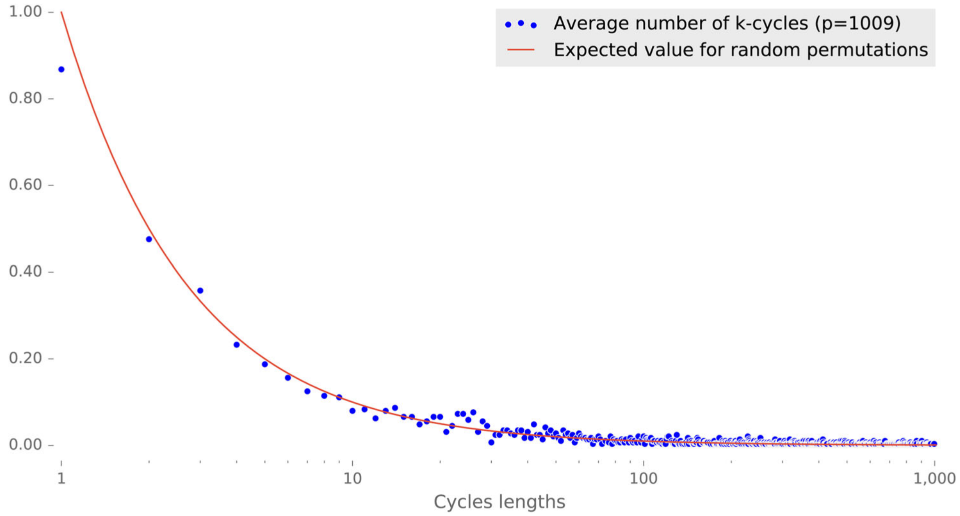

Figure 4. Average number of k-cycles in ElGamal functions on $\mathbb{F}_{1009}$.

Figure 3 shows the same continuous line, but now the dots represent the counts for the 288 generators of $\mathbb{F}_{1009}$. The result looks quite similar to Figure 2.

2.2. Number of k-cycles in permutations

For uniformly random permutations of a finite set, the number of cycles of length k is on average $1/k$ (Flajolet and Sedgewick 2009, Example III.9). In Figure 4, we give the average number of cycles of length k for all 288 generators of the multiplicative group $\mathbb{F}_{1009}^{\times}$ in dots. The experimental results are reasonably close to the theoretical values.

For the specific case $k = 1$, the average number of fixed points in random permutations is 1. The results in Figure 4 are very close, by a small error margin. Therefore, to better illustrate this property, Figure 5 shows the average number of fixed points for all generators in the multiplicative group for all prime numbers from 2 to 2111. As expected, the average of fixed points is closely distributed to the theoretical value. We also note that by increasing p, the average of fixed points in the experiments gets closer to the expected theoretical value.

3. Sidon sets

A subset A of an abelian group G (written additively) is a *Sidon set* if for every $y \in G \setminus \{0\}$ there exists at most one pair $(a, b) \in A^2$ such that $y =$

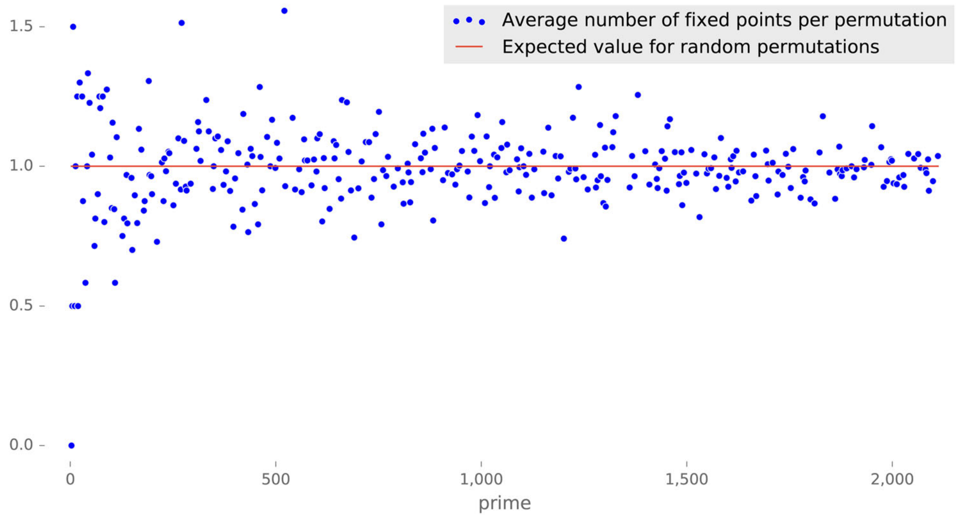

Figure 5. Average number of fixed points for all generators of $\mathbb{F}_p$ with $2 \le p \le 2111$.

$a - b$. Clearly, for any set A there are exactly $\#A$ pairs $(a, b) \in A^2$ for which $0 = a - b$, where $\#A$ is the cardinality of A.

Let p be a prime, $g \in \mathbb{Z}_p^\times$ a generator of the multiplicative group $\mathbb{Z}_p^\times$, and identify $\mathbb{Z}_{p-1} = \{0, 1, ..., p-2\}$ and $\mathbb{Z}_p = \{0, 1, ..., p-1\}$. We consider the additive group $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_p$ (using the additive structure of both factors), and the subset

$$S = \{(g^x, x) : x \in \mathbb{Z}_{p-1}\}. \tag{3.1}$$

Thus S is the graph of the discrete logarithm function modulo p, since $S = \{(y, \log_g y) : y \in \mathbb{Z}_p \setminus \{0\}\}$, and, after swapping the coordinates, the graph of the ElGamal function.

The following result is well known; see Cilleruelo (2012), Example 2. We include a proof for the sake of completeness.

Lemma 3.1. *The set S in (3.1) is a Sidon set in $\mathbb{Z}_p \times \mathbb{Z}_{p-1}$.*

Proof. For some $(u, v) \neq (0, 0)$ in $\mathbb{Z}_p \times \mathbb{Z}_{p-1}$ and $c_1, c_2 \in \mathbb{Z}_{p-1}$, suppose that $(g^{c_1}, c_1) - (g^{c_2}, c_2) = (u, v)$. Then

$$\begin{aligned} c_1 - c_2 &\equiv v \bmod p - 1, \\ g^{c_1} - g^{c_2} &\equiv u \bmod p. \end{aligned} \tag{3.2}$$

In particular $v \not\equiv 0 \bmod p - 1$, since otherwise $u \equiv g^{c_1} - g^{c_1} \equiv 0 \bmod p$ which contradicts the assumption. From (3.2) we know that $g^{c_1 - v} \equiv g^{c_2} \bmod p$, and hence $g^{c_1}(1 - g^{-v}) \equiv u \bmod p$. Furthermore, $(1 - g^{-v}) \not\equiv 0 \bmod p$, and we conclude that $g^{c_1} \equiv (1 - g^{-v})^{-1} u \bmod p$ and thus the pair (c_1, c_2) is uniquely determined by (u, v). □

Lemma 3.2. *Let φ be a nontrivial character of $G = \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ and let S be the set in (3.1). Then*

$$\left|\sum_{a\in S}\varphi(a)\right| < (3(p-1))^{1/2}.$$

Proof. Any nontrivial character φ of G satisfies $\sum_{x\in G}\varphi(x) = 0$. Thus, for the set $S-S = \{x \in G : \ x = a-b \text{ for some } a, b \in S\}$ we have

$$\sum_{x\in S-S}\varphi(x) = -\sum_{x\notin S-S}\varphi(x). \tag{3.3}$$

Since $|z| = (z \cdot \bar{z})^{1/2}$ for a complex number z and $\overline{\varphi(x)} = \varphi(-x)$ for every $x \in G$, where $\bar{z}$ denotes the complex conjugate of z, it follows that

$$\begin{aligned}\left|\sum_{a\in S}\varphi(a)\right|^2 &= \Big(\sum_{a\in S}\varphi(a)\Big)\Big(\sum_{b\in S}\varphi(-b)\Big) = \sum_{a,\,b\in S}\varphi(a-b)\\ &= \sum_{y\in G}\varphi(y)\cdot \#\{(a,b)\in S^2 : \ y = a-b\}.\end{aligned} \tag{3.4}$$

Since S is a Sidon set by Lemma 3.1, we know that

$$\#\{(a,b)\in S^2 : \ y = a-b\} = \begin{cases} \#S & \text{if } y = 0,\\ 1 & \text{if } y \in S-S \setminus \{0\},\\ 0 & \text{otherwise.}\end{cases}$$

Thus

$$\begin{aligned}\left|\sum_{a\in S}\varphi(a)\right|^2 &= \#S-1 + \sum_{y\in S-S}\varphi(y)\\ &= \#S-1-\sum_{y\notin S-S}\varphi(y)\\ &\le \#S-1 + |\sum_{y\notin S-S}\varphi(y)|.\end{aligned} \tag{3.5}$$

Luckily, we have a complete description of the set $S - S$, since every pair $(a,b) \in S^2$ is uniquely determined by the difference $a - b$ unless $a-b = 0$, for which we have exactly $\#S = p-1$ options; hence

$$\#(S-S) = (\#S)^2-\#S + 1 = (p-1)^2-(p-1) + 1 = \#G-2\#S + 1 \tag{3.6}$$

since $\#G = p(p-1)$. Clearly we have from (3.6) that

$$\left|\sum_{y\notin S-S}\varphi(y)\right| \leq \#G-\#(S-S) = 2\#S-1. \tag{3.7}$$

Combining (3.4), (3.5), and (3.7) we have

$$\left|\sum_{a\in S}\varphi(a)\right|^2 \leq 3\#S-2,$$

which concludes the proof. □

The following classical result is only included here for the sake of completeness. log is always the natural logarithm in this paper.

Lemma 3.3. *Let n and N be positive integers with $1 \leq N<n$. Then, for any integer h*

$$\sum_{0\leq a<n}\left|\sum_{h\leq x<N+h}\exp\left(2\pi iax/n\right)\right|<5n\log n.$$

Proof. By factoring out $\exp\left(2\pi iah/n\right)$, of absolute value 1, in the inner sum, we may assume without loss of generality that $h=0$.

The contribution of $a=0$ to the inner sum is precisely $N<n$. For $1 \leq a<n$, the inner sum is a geometric sum with ratio $q = \exp\left(2\pi ia/n\right) \neq 1$, so that

$$\left|\sum_{0\leq x<N}\exp\left(2\pi iax/n\right)\right| = \left|\frac{q^N-1}{q-1}\right| \leq \frac{2}{|q-1|}.$$

We have

$$\begin{aligned}|q-1| &= |\exp\left(2\pi ia/n\right)-1| = |\exp\left(\pi ia/n\right)-\exp\left(-\pi ia/n\right)|\\ &= 2|\sin\left(\pi a/n\right)|.\end{aligned}$$

Then

$$|\sin\left(\pi a/n\right)| = |\sin\left(\pi(a-n)/n\right)| \geq \frac{2\min\{a,n-a\}}{n}$$

because $\sin(\alpha) \geq 2\alpha/\pi$ for $0 \leq \alpha \leq \pi/2$. Therefore

$$\begin{aligned}\sum_{0\leq a<n}\left|\sum_{0\leq x<N}\exp\left(2\pi iax/n\right)\right| &\leq N+\sum_{0<a<n}\frac{n}{\min\{a,n-a\}}\\ &\leq N+2n\sum_{1\leq a\leq n/2}\frac{1}{a}.\end{aligned}$$

This together with the harmonic inequality

$$\sum_{1\le a\le n/2}\frac{1}{a}<1+\log(n),$$

which holds for any integer $n\ge 2,$ implies the claim. □

Theorem 3.1. *Let $S=\{(g^x,x):x\in\mathbb{Z}_{p-1}\}$. For any box $B=[h+1..h+N]\times[k+1..k+M]\subseteq\mathbb{Z}_p\times\mathbb{Z}_{p-1}$ we have*

$$\left|\#(S\cap B)-\frac{\#B}{p}\right|\le 50p^{1/2}\log^2 p.$$

Proof. By the orthogonality of characters and separating the contribution of the trivial character $\varphi_0=1,$ we have

$$\begin{aligned}\#(S\cap B)&=\frac{1}{p(p-1)}\sum_{\varphi}\sum_{a\in S}\sum_{b\in B}\varphi(a-b)\\ &=\frac{\#B}{p}+\frac{1}{p(p-1)}\sum_{\varphi\ne\varphi_0}\sum_{a\in S}\sum_{b\in B}\varphi(a-b).\end{aligned}$$

Thus

$$\begin{aligned}\left|\#(S\cap B)-\frac{\#B}{p}\right|&=\frac{1}{p(p-1)}\left|\sum_{\varphi\ne\varphi_0}\sum_{a\in S}\sum_{b\in B}\varphi(a-b)\right|\\ &\le\frac{1}{p(p-1)}\sum_{\varphi\ne\varphi_0}\left|\sum_{a\in S}\varphi(a)\right|\left|\sum_{b\in B}\varphi(b)\right| \qquad (3.8)\\ &\le\frac{1}{p(p-1)}\left(\max_{\varphi\ne\varphi_0}\left|\sum_{a\in S}\varphi(a)\right|\right)\sum_{\varphi\ne\varphi_0}\left|\sum_{b\in B}\varphi(b)\right|.\end{aligned}$$

The characters of G act as follows:

$$\varphi((x,y))=\exp\left(2\pi i\left(\frac{sx}{p}+\frac{ty}{p-1}\right)\right),\qquad\text{for some }(s,t)\in G.$$

Hence we have

$$\begin{aligned}\sum_{\varphi\ne\varphi_0}\left|\sum_{b\in B}\varphi(b)\right|\le&\left(\sum_{0\le s<p}\left|\sum_{h<x\le h+N}\exp(2\pi isx/p)\right|\right)\\ &\times\left(\sum_{0\le t<p-1}\left|\sum_{k<y\le k+M}\exp(2\pi ity/(p-1))\right|\right),\end{aligned}$$

which implies, by Lemma 3.3, that

$$\sum_{\varphi \neq \varphi_0} \left| \sum_{b \in B} \varphi(b) \right| < 25p(p-1) \log^2 p. \tag{3.9}$$

By Lemma 3.2,

$$\max_{\varphi \neq \varphi_0} \left| \sum_{a \in S} \varphi(a) \right| < \sqrt{3(p-1)},$$

which combined with (3.9) in (3.8) concludes the proof. □

One can show, with a bit more of work, see Cilleruelo and Zumalacárregui (2017), that in fact

$$\left| \#(S \cap B) - \frac{\#B}{p} \right| \in O(p^{1/2} \log_+^2 (\#B \cdot p^{-3/2})),$$

where $\log_+(x) = \max\{\log(x), 1\}$ for $x \in \mathbb{R}^+$. The implied asymptotics are for growing p. In particular, for $\#B$ asymtotically larger than $p^{3/2} \log p$, then $\#(S \cap B) \sim \#B/p$. In Cilleruelo and Zumalacárregui (2017) such a result was obtained for a much larger family of dense Sidon sets.

As mentioned in the Introduction, Cobeli, Vâjâitu, and Zaharescu (2002) study a similar question. Besides using a box as in Theorem 3.1, they allow the further constraint that $ux + vg^x < t$ for a parameter t; our result corresponds to the special case $t = p$. They exhibit an explicit and easily calculated function that approximates the distribution considered with an error of $O(p^{1/2} \log^3 p)$. Theorem 3.1 improves this in two directions: the error term is only $p^{1/2} \log^2 p$ and the estimate is explicit with the constant 50—which can presumably be improved. For the distribution of $x - g^x$ (Cobeli, Vâjâitu, and Zaharescu 2002), provide an explicit estimate with error proportional to $p^{1/2} \log^3 p$.

4. Ideas for future work

We have shown, both experimentally and theoretically, some randomness properties of the ElGamal function over $G = \mathbb{Z}_p^\times$ for a prime p. In particular, our upper bound of $50p^{1/2} \log^2 p$ on the distance of this function from equidistribution is new. Many questions along these lines remain open:

- stronger results, perhaps even pseudorandomness,
- other groups for G, for example, elliptic curves,
- similar questions about the Schnorr function, where G is a "small" subgroup of a "large" group $\mathbb{Z}_p$.

Acknowledgements

Part of this work was done by the first three authors at LabSEC of the Universidade Federal de Santa Catarina, Brazil. We thank Daniel Panario for providing background material, Ricardo Custódio for making our collaboration possible, and an anonymous referee for useful suggestions.

The collaboration with Ana Zumalacárregui was begun at a meeting at the CIRM, Luminy, France, whose support we gratefully acknowledge.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The second author was supported by the B-IT Foundation and the Land Nordrhein-Westfalen. The last author was supported by Australian Research Council Grants DP140100118.

About the authors

Lucas Boppré Niehues studied Computer Science at Universidade Federal de Santa Catarina in Brazil, where he researched modern authentication schemes and optimizations to finite field arithmetic. He is currently working on hardware security modules and key management systems at Deutsche Bank, Germany. His research interests are related to usable security and privacy, post-quantum cryptography, and open-source projects. Address: Frankfurt am Main, Germany. Email: lucasboppre@gmail.com.

Joachim von zur Gathen is an Emeritus Professor at the University of Bonn in Germany. After undergraduate studies at ETH Zürich and a PhD from Universität Zürich, he held positions at the universities of Toronto, Canada, and Paderborn, Germany. Besides visiting professorships in Australia, Brazil, Chile, Germany, Singapore, South Africa, Spain, Switzerland, Uruguay, USA, he has travelled widely, in fact, to all countries in the world. His research interests, past and present, include computational complexity, computer algebra, finite field computations, and cryptography, modern and classical. Address: B-IT, Universität Bonn, Bonn, Germany. Email: gathen@bit.uni-bonn.de.

Lucas Pandolfo Perin is a PhD student at Universidade Federal de Santa Catarina in Brazil, under the supervision of Ricardo Felipe Custódio and co-supervision of Daniel Panario. Previously, he acquired a bachelor's degree in Computer Science and defended his master's dissertation in the same institution. During his PhD, he received a scholarship from CAPES to conduct research at Carleton University as a visiting researcher, hosted by Daniel Panario. His research interests are mostly related to cryptography, such as post-quantum schemes, implementations and applications. Address: LabSEC - Universidade Federal de Santa Catarina, Florianópolis, Brazil. Email: lucas.perin@posgrad.ufsc.br

Ana Zumalacárregui was a PostDoc at the Mathematics Department of the University of New South Wales, Australia, when this work was done. She has since left academia. Address: University of New South Wales, Sydney, Australia. Email: ana.zumalacarregui@gmail.com

References

Canetti, R., J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. Shparlinski. 2000. On the statistical properties of Diffie-Hellman distributions. *Israel Journal of Mathematics* 120 (1):23–46. doi: 10.1007/s11856-000-1270-1.

Cilleruelo, J. 2012. Combinatorial problems in finite fields and Sidon sets. *Combinatorica* 32 (5):497–511. doi: 10.1007/s00493-012-2819-4.

Cilleruelo, J., and A. Zumalacárregui. 2017. Saving the logarithmic factor in the error term estimates of some congruence problems. *Mathematische Zeitschrift* 286 (1–2):545–58. doi: 10.1007/s00209-016-1771-1.

Cobeli, C., M. Vâjâitu, and A. Zaharescu. 2002. On the set $ax + bg^x$ (mod$p$). *Portugaliae Mathematica (N.S.)* 59 (2):195–203.

ElGamal, T. 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* 31 (4):469–72. doi: 10.1109/TIT.1985.1057074.

Felix, A. T., and P. Kurlberg. 2017. On the fixed points of the map $x \mapsto x^x$ modulo a prime, II. *Finite Fields and their Applications*, 48:141–159.

Flajolet, P., and B. Sedgewick. 2009. *Analytic combinatorics*. Cambridge, UK: Cambridge University Press.

Konyagin, S. V., F. Luca, B. Mans, L. Mathieson, M. Sha, and I. E. Shparlinski. 2016. Functional graphs of polynomials over finite fields. *Journal of Combinatorial Theory, Series B* 116:87–122. doi: 10.1016/j.jctb.2015.07.003.

Kurlberg, P., F. Luca, and I. E. Shparlinski. 2015. On the fixed points of the map $x \mapsto x^x$ modulo a prime. *Mathematical Research Letters* 22 (1):141–68. doi: 10.4310/MRL.2015.v22.n1.a8.

Mans, B., M. Sha, I. E. Shparlinski, and D. Sutantyo. 2019. On functional graphs of quadratic polynomials. *Experimental Mathematics*. 28:292–300.

Martins, R. S. V., and D. Panario. 2016. On the heuristic of approximating polynomials over finite fields by random mappings. *International Journal of Number Theory* 12 (07):1987–2016. Erratum pages 2041–2042. doi: 10.1142/S1793042116920020.

von zur Gathen, J. 2015. *CryptoSchool*. Springer.

Wilf, H. 1990. *Generating functionology*. New York: Academic Press.