CONNECTED COMPONENTS OF THE GRAPH GENERATED BY POWER MAPS IN PRIME FINITE FIELDS

CARL POMERANCE AND IGOR E. SHPARLINSKI

For Jeffrey Outlaw Shallit on his 60th birthday

ABSTRACT. Consider the power pseudorandom-number generator in a finite field $\mathbb{F}_q$. That is, for some integer $e \geq 2$, one considers the sequence $u, u^e, u^{e^2}, \ldots$ in $\mathbb{F}_q$ for a given seed $u \in \mathbb{F}_q^\times$. This sequence is eventually periodic. One can consider the number of cycles that exist as the seed u varies over $\mathbb{F}_q^\times$. This is the same as the number of cycles in the functional graph of the map $x \mapsto x^e$ in $\mathbb{F}_q^\times$. We prove some estimates for the maximal and average number of cycles in the case of prime finite fields.

1. INTRODUCTION

1.1. **Set up.** For a prime power q, we use $\mathbb{F}_q$ to denote the finite field of q elements. For a fixed integer $e \geq 2$ we denote by $\mathcal{G}_{e,q}$ the functional graph of the map $x \mapsto x^e$ with vertices formed by the elements of $\mathbb{F}_q^\times$. We also denote by $N(e,q)$ the total number of cycles in $\mathcal{G}_{e,q}$. Alternatively, $N(e,q)$ can be defined as the number of connected components of $\mathcal{G}_{e,q}$ when it is considered as an undirected graph.

By a result of [4, Theorem 1] for prime fields (see also [15] for $e = 2$), which can easily be extended to arbitrary finite fields, we have

$$N(e,q) = \sum_{d \mid \rho} \frac{\varphi(d)}{\ell_e(d)}, \tag{1.1}$$

where ρ is the largest divisor of $q-1$ which is relatively prime to e and, for a, b relatively prime and b positive, $\ell_a(b)$ denotes the multiplicative order of a modulo b.

Here we are interested in the extreme and average values of $N(e,q)$ when e is fixed and q varies over primes.

We remark that under the Generalised Riemann Hypothesis, the orders $\ell_a(b)$ tend to be large (of magnitude b in a logarithmic scale); we refer to [13]. Hence one expects that for most primes we have $N(e,p) \leq p^{o(1)}$. On the other hand, we show that the average value of $N(e,p)$ is quite large.

1.2. **Notation.** Throughout the paper, the letters p and r always denote prime numbers while the letters a, e, k, m, and n denote positive integers.

As usual, for a positive real number x we use $\pi(x)$ to denote the number of primes $p \le x$. Furthermore, for integers a and $k \ge 1$ we define $\pi(x;k,a)$ as the number of primes $p \le x$ in the arithmetic progression $p \equiv a \pmod k$.

We also use $P(k)$ and $\varphi(k)$ to denote the largest prime divisor and the Euler function of k, respectively, with $P(1) = 1$.

We recall that the statements $U = O(V)$, $V \gg U$ and $U \ll V$ are all equivalent to the inequality $|U| \le cV$ with some positive constant c. In this note, implied constants may depend on the exponent e unless stated otherwise.

1.3. **New results.** First, we show that $N(e,p)$ is rather large for infinitely many primes p.

Theorem 1.1. *For any fixed integer $e \ge 2$, there are infinitely many primes p with*

$$N(e,p) \ge p^{5/12+o(1)}.$$

We also show the following lower bound on the average value of $N(e,p)$.

Theorem 1.2. *For any fixed integer $e \ge 2$ and all sufficiently large real numbers x, we have*

$$\frac{1}{\pi(x)} \sum_{p \le x} N(e,p) \ge x^{0.293}.$$

2. Preliminaries

2.1. **Primes in arithmetic progressions.** We need a version of a result of Alford, Granville and Pomerance [1, Theorem 2.1] .

Lemma 2.1. *For each fixed $\varepsilon > 0$ and sufficiently large x, depending on ε, there is a finite set $\{m_1, \ldots, m_t\}$ of integers, where t depends only on ε, and each $m_i > \log x$, with the following property. If $m \le x^{5/12-\varepsilon}$, and m is not divisible by any of $m_1, \ldots, m_t$, then we have uniformly over integers a with $\gcd(a,m) = 1$, that*

$$\pi(x;m,a) \gg \frac{1}{\varphi(m)} \pi(x)$$

where the implied constant depends only on ε.

2.2. **Shifted primes with prescribed smoothness.** We also need the following result, which follows from the work of Baker and Harman [2, Theorem 1], which improves the estimate in [7]. We recall our convention that r always denotes a prime number

Lemma 2.2. *There is an absolute positive constant κ with the following property. Let $u > 10$,*

$$v = \frac{\log u}{\log_2 u}, \quad w = v^{1/0.2961},$$

and let

$$\mathcal{Q} = \{r \in [w/(\log w)^\kappa, w] \ : \ r - 1 \mid M_v\},$$

where M_v is the least common multiple of the integers in $[1, v]$. Then for u sufficiently large, we have

$$\#\mathcal{Q} \geq w/(\log w)^\kappa.$$

3. Proofs of main results

3.1. **Proof of Theorem 1.1.** We fix some integer $e \geq 2$ and a real $\varepsilon > 0$. For a sufficiently large number K we define x by the equation

$$e^K = x^{5/12-\varepsilon}.$$

Now let $m_1, \ldots, m_t$ be as in Lemma 2.1.

Clearly if $\gcd(m_i, e) > 1$ then $m_i \nmid e^k - 1$. For each i with m_i coprime to e, we obviously have

$$\ell_e(m_i) \gg \log m_i \gg \log\log x, \qquad i = 1, \ldots, m. \tag{3.1}$$

Hence for any integer $h \geq 1$ we have at least

$$h - \sum_{i=1}^{t} \left(\frac{h}{\ell_e(m_i)} + 1 \right) = h + O(h/\log\log x + 1)$$

integers k in the interval $[K - h, K]$, which are not divisible by any of the multiplicative orders $\ell_e(m_i)$ for which $\gcd(m_i, e) > 1$. Thus $e^k - 1$ is not divisible by any of the integers m_i, $i = 1, \ldots, t$. In particular, we can always find $k \in [K - h_0, K]$, where h_0 depends only on ε, for which $m_i \nmid e^k - 1$, $i = 1, \ldots, t$. We fix such an integer k and denote $m = e^k - 1$. Thus by Lemma 2.1 there exists a prime

$$p \ll x = e^{12K/(5-12\varepsilon)} \ll m^{12/(5-12\varepsilon)} \tag{3.2}$$

with

$$p \equiv 1 \pmod{m}.$$

Since $\gcd(m,e) = 1$, we have $m \mid \rho$, where ρ is the part of $p-1$ coprime to e. Thus, using $\ell_e(m) = k$, we obtain

$$N(e,p) = \sum_{d \mid \rho} \frac{\varphi(d)}{\ell_e(d)} \ge \frac{\varphi(m)}{k} \gg \frac{\varphi(m)}{\log m}.$$

Using the minimal order of the Euler function, see [9, Theorem 328], we thus have

$$N(e,p) \gg \frac{m}{\log m \log\log m},$$

which together with (3.2) and taking into account that $\varepsilon > 0$ is arbitrary, concludes the proof.

3.2. **Proof of Theorem 1.2.** We follow the construction from the proof of [14, Theorem 1] which in turn is based on some ideas of Erdős [5] .

We fix some sufficiently small $\varepsilon > 0$ and let x be large. For

$$u = x^{5/12-\varepsilon}$$

we consider the set $\mathcal{Q}$ and parameters v and w as in Lemma 2.2. Furthermore, let $m_1, \ldots, m_t$ be as in Lemma 2.1. Note that (3.1) guarantees that for each $i = 1, \ldots, t$ with $\gcd(m_i, e) = 1$ we have $\ell_e(m_i) > 1$ and thus we can choose a prime divisor r_i of $\ell_e(m_i)$ (we do not claim nor require these primes to be distinct). We now remove at most t such primes from the set $\mathcal{Q}$ and denote the remaining set by $\mathcal{Q}^*$. Thus $\#\mathcal{Q}^* = \#\mathcal{Q} + O(1)$. Note too that $\mathcal{Q}^*$ contains no prime dividing e.

Put

$$\nu = \left\lfloor \frac{\log u}{\log w} \right\rfloor$$

and consider the set $\mathcal{S}$ of all products of ν distinct primes from $\mathcal{Q}^*$. Clearly

$$u \ge w^\nu \ge m \ge (w/(\log w)^\kappa)^\nu = u^{1+o(1)} \tag{3.3}$$

for every $m \in \mathcal{S}$.

Furrthermore, using Lemma 2.2, an easy calculation shows that

$$\#\mathcal{S} = \binom{\#\mathcal{Q}^*}{\nu} = u^{0.7039+o(1)}. \tag{3.4}$$

For every $m \in \mathcal{S}$ we have

$$\ell_e(m) \mid M_v$$

and so by the prime number theorem, we obtain that

$$\ell_e(m) \le \exp((1+o(1))v) = u^{o(1)} = x^{o(1)}. \tag{3.5}$$

Recalling the definition of $\mathcal{Q}^*$ we see that for any $m \in \mathcal{S}$ we have $m_i \nmid m$, $i = 1, \dots, t$. By the choice of u and the upper bound in (3.3) we see that by Lemma 2.1 we have

$$\pi(x; m, 1) \gg \frac{1}{\varphi(m)}\pi(x) = x^{1+o(1)}u^{-1}$$

for every $m \in \mathcal{S}$. Thus, using (3.4) we obtain

$$\sum_{m\in\mathcal{S}} \pi(x; m, 1) \geq x^{1+o(1)}u^{-0.2961}. \tag{3.6}$$

Now, let $\mathcal{P}$ be the union of all primes $p \leq x$ with $m \mid p-1$ for some $m \in \mathcal{S}$. Since, by the classical bound on the divisor function, each prime $p \in \mathcal{P}$ can come from at most $x^{o(1)}$ integers $m \in \mathcal{S}$, we obtain from (3.6) that

$$\#\mathcal{P} \geq x^{1+o(1)}u^{-0.2961}. \tag{3.7}$$

For every p with $m \mid p-1$ for some $m \in \mathcal{S}$, using (3.5) and then (3.3), we have

$$N(e, p) \geq \frac{\varphi(m)}{\ell_e(m)} = m^{1+o(1)} = u^{1+o(1)}.$$

Therefore, using (3.7),

$$\sum_{p\leq x} N(e, p) \geq \sum_{p\in\mathcal{P}} N(e, p) \geq u^{1+o(1)}\#\mathcal{P} \geq x^{1+o(1)}u^{0.7039}.$$

Recalling the choice of u and taking ε to be sufficiently small, we conclude the proof.

4. Further improvements

Hypothetically the exponents in Theorems 1.1 and 1.2 may be replaced with any fixed number smaller than 1. This is true for Theorem 1.1 on the assumption that we have exponent $1 + \varepsilon$ in Linnik's theorem; that is, for each integer $k > k_0(\varepsilon)$ and residue class $a \pmod k$ coprime to k, the least prime in this residue class is smaller than $k^{1+\varepsilon}$. The proof that $N(e, p) > p^{1-\varepsilon}$ for infinitely many primes p then follows the same lines as our proof of Theorem 1.1.

To prove a $1 - \varepsilon$ analogue of Theorem 1.2 we need in addition to the strong Linnik constant as above, the conjecture that in Lemma 2.2 we may replace the number 0.2961 with ε. This conjecture of Erdős is known to follow from the Elliott–Halberstam conjecture. The proof that the average of $N(e, p)$ for $p \leq x$ exceeds $x^{1-\varepsilon}$ is then the same as our proof of Theorem 1.2.

The above improvements are probably out of reach. However, there is a possible way to achieve more modest improvements of Theorems 1.1 and 1.2, which is based on a combination of a recent result of Chang [3] with a result of Harman [11]. For this approach, one first has to verify that that the exponent $3/4$ in [11, Equation (1.2)] can be replaced by any constant $c < 1$, see also the remark after [10, Theorem 1.2]. Then this result can be combined with the bound of Chang [3, Theorem 10] on the zero-free region of L-functions of characters with smooth moduli, where the modulus m is chosen to satisfy two properties

- $m = e^k - 1$ where k is an integer with a small value of $\varphi(k)$, that is, with $\varphi(k) = o(k)$;
- m is not divisible by a Siegel modulus, which can be achieved via the same argument as that used in the proof of Theorem 1.2.

Combining these ideas with our approach one is likely to be able replace $5/12$ with 0.472 and 0.293 with 0.332 in Theorems 1.1 and 1.2 respectively. We also note that using the moduli of the form $m = e^k - 1$ with $\varphi(k) = o(k)$ as in the above, together with the version of the Linnik theorem given by Chang [3, Corollary 11] one can obtain an alternative proof of Theorem 1.1. However this produces a much sparser sequence of primes than in the current proof of Theorem 1.1.

5. Further results and directions

In [12, Theorem 2] lower bounds are given for the order of e modulo the part of $p-1$ coprime to e that translate to upper bounds for $N(e,p)$. Indeed, we have for any function $\varepsilon(p) \downarrow 0$ that $N(e,p) < p^{1/2-\varepsilon(p)}$ for almost all primes p and on the generalized Riemann Hypothesis, $N(e,p) < p^{\varepsilon(p)}$ for almost all p. (These normal-order results are in stark contrast to the above extremal and average-order results.)

One can also consider the average cycle length. For a positive integer n, let $\ell_e^*(n)$ denote the order of e modulo the prime-to-e part of n. The average cycle length is then

$$C(e,p) = \frac{1}{p-1} \sum_{d \mid p-1} \varphi(d) \ell_e^*(d).$$

Note that $\ell_e^*(p-1) = \ell_e(\rho)$, so we have

$$\frac{\varphi(p-1)}{p-1} \ell_e(\rho) \le C(e,p) \le \ell_e(\rho).$$

One then sees that results on $\ell_e(\rho)$ immediately translate to results on $C(e,p)$. So, it follows from [12, Theorem 2] that for any $\varepsilon(p) \downarrow 0$, we

have that for almost all primes p, $C(e,p) > p^{1/2+\varepsilon(p)}$. Further, the average of $C(e,p)$ for $p \le x$ exceeds $x^{0.592}$ for all sufficiently large values of x. And on the Generalised Riemann Hypothesis, the average exceeds $x^{1-\epsilon}$. An upper bound for the minimal order of $C(e,p)$ follows from the proof of Theorem 1.1. In particular, we have $C(e,p) < p^{0.472+o(1)}$ for infinitely many primes p.

It would be interesting to generalize the results of this paper to arbitrary finite fields, or perhaps to consider quantities such as

$$N(e,p^k), \quad k = 1, 2, \dots .$$

For example, we can show that for any fixed choice of e and p, for infinitely many k we have

$$N(e,p^k) > \exp(k^{c/\log\log k}), \tag{5.1}$$

where c is a positive constant. Indeed, from [6, Theorem 1] there are infinitely many positive integers m with $\lambda(m) \le (\log m)^{O(\log\log\log m)}$, where $\lambda(m)$ is the maximum order of an element in $(\mathbb{Z}/m\mathbb{Z})^\times$. Further, with an easy argument, one can insure that m is coprime to ep. Let $k = \ell_p(m) \le \lambda(m)$. We have

$$N(e,p^k) \ge \varphi(\rho)/\ell_e(\rho) \ge \varphi(\rho)/\lambda(\rho) \ge m/\lambda(m),$$

using [8, Lemma 2]. Hence $N(e,p^k) \ge m^{1+o(1)}$. The small size of $\lambda(m)$ in comparison to m implies that m is large in comparison to $\lambda(m)$. In particular, we have $m \ge \exp(\lambda(m)^{c/\log\log\lambda(m)})$ for some $c > 0$. The bound (5.1) follows using $\lambda(m) \ge k$.

It also may be of interest to study the number of cycles of the power generator in the ring $\mathbb{Z}/n\mathbb{Z}$, where a seed is coprime to n. It is likely that the methods of this paper and of [12] should be helpful.

Acknowledgements

The authors are very grateful to Glyn Harman for some clarifications concerning the possible relaxation of the conditions of [11, Theorem 1.2]. They are also grateful to the referee for a careful reading.

The first-named author was supported in part by NSF grant number DMS-1440140 at the Mathematical Sciences Research Institute. He thanks MSRI for their hospitality.

The second-named author thanks the Max Planck Institute for Mathematics, Bonn, for the generous support and hospitality. He was also supported by ARC Grant DP140100118.

References

[1] W. R. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers,' *Ann. of Math.*, **140** (1994), 703–722.

[2] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.*, **83** (1998), 331–361.

[3] M.-C. Chang, 'Short character sums for composite moduli', *J. d'Analyse Math.*, **2** (2014), 1–33.

[4] W.-S. Chou and I. E. Shparlinski, 'On the cycle structure of repeated exponentiation modulo a prime', *J. Number Theory*, **107** (2004), 345–356.

[5] P. Erdős, 'On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's φ-function', *Quart. J. Math. (Oxford Ser.)*, **6** (1935), 205–213.

[6] P. Erdős, C. Pomerance, and E. Schmutz, 'Carmichael's lambda function', *Acta Arith.*, **58** (1991), 363–385.

[7] J. B. Friedlander, 'On shifted primes without large prime factors', *Number Theory and Applications*, R. A. Mollin, ed., Kluwer NATO ASI, 1989, pp. 393–401.

[8] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, 'Period of the power generator and small values of the Carmichael function', *Math. Comp.*, **70** (2001), 1591–1605. 'Corrigendum', *op. cit.*, **71** (2002), 1803–1806.

[9] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[10] G. Harman, 'On the number of Carmichael numbers up to x', *Bull. London Math. Soc.*, **37** (2005), 641–650.

[11] G. Harman, 'Watt's mean value theorem and Carmichael numbers', *Int. J. Number Theory*, **4** (2008), no. 2, 241–248.

[12] P. Kurlberg and C. Pomerance, 'On the period of the linear congruential and power generators', *Acta Arith.*, **119** (2005), 149–169.

[13] S. Li and C. Pomerance, 'On generalizing Artin's conjecture on primitive roots to composite moduli', *J. Reine Angew. Math.*, **556** (2003), 205–224.

[14] C. Pomerance and I. E. Shparlinski, 'Rank statistics for a family of elliptic curves over a function field', *Pure and Applied Math. Quart.*, **6** (2010), 21–40.

[15] T. Vasiga and J. O. Shallit, 'On the iteration of certain quadratic maps over GF(p)', *Discr. Math.*, **277** (2004), 219–240.

Mathematics Department, Dartmouth College, Hanover, NH 03755, USA

E-mail address: carl.pomerance@dartmouth.edu

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au