Bull. Aust. Math. Soc. **99** (2019), 388–391
doi:10.1017/S0004972718001302

ON FINDING SOLUTIONS TO EXPONENTIAL CONGRUENCES

IGOR E. SHPARLINSKI

(Received 29 August 2018; accepted 23 October 2018; first published online 27 December 2018)

Abstract

We improve some previously known deterministic algorithms for finding integer solutions x, y to the exponential equation of the form $af^x + bg^y = c$ over finite fields.

2010 *Mathematics subject classification*: primary 11D61; secondary 11T71, 11Y16, 68Q25.

Keywords and phrases: exponential equation, algorithm, finite field.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements and let $\mathbb{F}_q^*$ denote the multiplicative group of nonzero elements of $\mathbb{F}_q$. For $a, b, c, f, g \in \mathbb{F}_q^*$ we consider the exponential equation

$$af^x + bg^y = c \tag{1.1}$$

in nonnegative integers x and y.

Various classical and quantum algorithms for solving Equation (1.1) have been given by van Dam and Shparlinski [7]. Some of the motivation behind [7] comes from a certain cryptographic construction of Lenstra and de Weger [3] and also connections with the theory of cyclotomic classes (see [1, 6]). Sasaki [4] extended some of the results and ideas of [7] to the case of exponential equations in $n \geq 2$ variables, that is,

$$\sum_{i=1}^{n} a_i f_i^{x_i} = c.$$

The approach of [7], also used in [4], is based on number-theoretic results on the distribution of solutions to exponential equations in finite fields. Here we supplement the ideas of [7] by another very simple argument which allows us to improve some of the results from [7].

During the preparation of this work, the author was supported in part by the Australian Research Council Grant DP170100786.

In particular, by [7, Theorem 1], for any $a, b, c, f, g \in \mathbb{F}_q^*$, one can either find a solution to Equation (1.1) or decide that it has no solution, in deterministic time

$$T_{\det} \le q^{9/8+o(1)} \tag{1.2}$$

as $q \to \infty$.

Furthermore, it is shown in [7, Theorem 2] that for any $a, b, f, g \in \mathbb{F}_q^*$, for all but $o(q)$ elements $c \in \mathbb{F}_q^*$, one can either find a solution to Equation (1.1) or decide that it has no solution, in deterministic time

$$T_{\det} \le q^{1+o(1)} \tag{1.3}$$

as $q \to \infty$.

Here we improve both (1.2) and (1.3) quite significantly. As in [7], our approach is based on results about the distribution of solutions to Equation (1.1) in small boxes (see, for example, Lemmas 3.1 and 3.2). In turn, the proofs of these results are based on estimates of character and exponential sums (see [7]). Thus any progress in this direction immediately leads to further improvements.

2. Results

We start with a result which applies to all equations.

Theorem 2.1. *Let $a, b, c, f, g \in \mathbb{F}_q^*$ and let f and g be of multiplicative orders s and t, respectively. One can either find a solution $(x, y) \in \mathbb{Z}^2$ to Equation (1.1), or decide that it does not have a solution, in deterministic time*

$$T_{\det} \le \min\{(st)^{1/2}, q^{3/4}\}(\log q)^{O(1)}.$$

In particular, we see that, for any s and t, the algorithm of Theorem 2.1 runs in time $T_{\det} \le q^{3/4+o(1)}$ as $q \to \infty$, improving (1.2) for any s and t.

We next consider the case where the right hand side of the Equation (1.1) varies.

Theorem 2.2. *Let $a, b, f, g \in \mathbb{F}_q^*$ and let f and g be of multiplicative orders s and t, respectively. For all but $o(q)$ elements $c \in \mathbb{F}_q^*$, one can either find a solution $(x, y) \in \mathbb{Z}^2$ to Equation (1.1), or decide that it does not have a solution, in deterministic time*

$$T_{\det} \le \min\{(st)^{1/2}, qs^{-1/2}, qt^{-1/2}\}(\log q)^{O(1)}.$$

In particular, we see that for any s and t, the algorithm of Theorem 2.2 runs in time $T_{\det} \le q^{2/3+o(1)}$ as $q \to \infty$, improving (1.3) for any s and t.

It is very likely that the same argument can also be used to improve the results of [4].

https://doi.org/10.1017/S0004972718001302 Published online by Cambridge University Press

3. Distribution of solutions to Equation (1.1)

We recall the following result given by [7, Corollary 1].

LEMMA 3.1. *Let $a, b, c, f, g \in \mathbb{F}_q^*$ and let f and g be of multiplicative orders s and t, respectively. There exists an absolute constant $C > 0$ such that if*

$$Cq^{3/2}s^{-1}\log q \le r \le t,$$

for some integer r, then Equation (1.1) has a solution in integers x and y with $x \in \{0, \dots, s-1\}$ and $y \in \{0, \dots, r-1\}$.

For almost all $c \in \mathbb{F}_q^*$ we have a stronger result given by [7, Corollary 2].

LEMMA 3.2. *Let $a, b, f, g \in \mathbb{F}_q^*$ and let f and g be of multiplicative orders s and t, respectively. There exists an absolute constant $C > 0$ such that, for all but $o(q)$ elements $c \in \mathbb{F}_q^*$, if*

$$Cq^2s^{-2}\log q \le r \le t,$$

for some integer r, then Equation (1.1) has a solution in integers x and y with $x \in \{0, \dots, s-1\}$ and $y \in \{0, \dots, r-1\}$.

4. Proof of Theorem 2.1

Set

$$r = \min\{t, \lceil Cq^{3/2}s^{-1}\log q\rceil\}.$$

Clearly, by Lemma 3.1, if there is a solution to Equation (1.1) then there is also a solution

$$(x, y) \in [0, s-1] \times [0, r-1].$$

We now employ the classical 'baby-steps, giant-steps' strategy of Shanks [5] (see also [2, Section 5.3]).

We first consider the case when $s \le r$. Choose an integer parameter $L \le r$, compute the list $\mathcal{L}$ of elements bg^u, $0 \le u \le L$, and then sort this list in any prescribed order. This part takes time $L(\log q)^{O(1)}$.

Next, for each $v = 1, \dots, \lceil r/L\rceil$ and $x = 0, \dots, s-1$, compute $g^{-Lv}(c - af^x)$ and search for a match in the list $\mathcal{L}$ (since $\mathcal{L}$ is sorted this can be done in polynomial time for every v and x). Every match gives us a solution to Equation (1.1). Conversely, if there is a solution, we can always find one in this way. Hence the total time is $(L + sr/L)(\log q)^{O(1)}$. This time optimises for

$$L = \lceil (rs)^{1/2}\rceil, \tag{4.1}$$

which is an admissible choice since $L \le r$ for $s \le r$. Thus in this case the algorithm runs in time

$$(rs)^{1/2}(\log q)^{O(1)} = \min\{(st)^{1/2}, q^{3/4}\}(\log q)^{O(1)}$$

and we have the desired result.

Now we consider the case when $s > r$. We now choose an integer parameter $L \le s$ and compute the list $\mathcal{L}$ of elements af^u, $0 \le u \le L$, and sort this list in any prescribed order. Then, for each $v = 1, \ldots, \lceil s/L \rceil$ and $y = 0, \ldots, r-1$, we compute $f^{-Lv}(c - bg^y)$ and search for a match in the list $\mathcal{L}$. Exactly as before, we see that the total time is $(L + sr/L)(\log q)^{O(1)}$. We use L as in (4.1) again to conclude the proof.

5. Proof of Theorem 2.2

Set

$$r = \min\{t, \lceil Cq^2 s^{-2} \log q \rceil\},$$

but otherwise proceed as in the proof of Theorem 2.1. By Lemma 3.2, if there is a solution to Equation (1.1) then there is also a solution

$$(x, y) \in [0, s-1] \times [0, r-1].$$

With the choice of L as in (4.1), we obtain an algorithm of complexity

$$\begin{aligned}(L + sr/L)(\log q)^{O(1)} &= (sr)^{1/2}(\log q)^{O(1)} \\ &= \min\{(st)^{1/2}, qs^{-1/2}\}(\log q)^{O(1)}.\end{aligned}$$

By interchanging the roles of s and t we also obtain an algorithm of complexity $\min\{(st)^{1/2}, qt^{-1/2}\}(\log q)^{O(1)}$, which concludes the proof.

Acknowledgement

The author is grateful to Rich Schroeppel for suggesting the idea which led to this work.

References

[1] B. Berndt, R. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, 21 (John Wiley & Sons, New York, 1998).

[2] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective* (Springer, Berlin, 2005).

[3] A. K. Lenstra and B. de Weger, *On the Possibility of Constructing Meaningful Hash Collisions for Public Keys*, Lecture Notes in Computer Science, 3574 (Springer, Berlin, 2005), 267–279.

[4] Y. Sasaki, 'On zeros of exponential polynomials and quantum algorithms', *Quantum Inf. Processing* **9** (2010), 419–427.

[5] D. Shanks, *Class Number, A Theory of Factorization and Genera*, Proceedings of Symposia in Pure Mathematics, 20 (American Mathematical Society, Providence, RI, 1971), 415–440.

[6] T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, 2 (Markham Publishing Company, Chicago, IL, 1967).

[7] W. van Dam and I. E. Shparlinski, *Classical and Quantum Algorithms for Exponential Congruences*, Lecture Notes in Computer Science, 5106 (Springer, Berlin, 2008), 1–10.

IGOR E. SHPARLINSKI, Department of Pure Mathematics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au