NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 56 (2025), 1–13
https://doi.org/10.53733/579

ON THE WARING PROBLEM WITH DICKSON POLYNOMIALS MODULO A PRIME

Igor E. Shparlinski and José Felipe Voloch

(Received 25 October 2024)

Abstract. We improve recent results of D. Gomez and A. Winterhof (2010) and of A. Ostafe and I. E. Shparlinski (2011) on the Waring problem with Dickson polynomials in the case of prime finite fields. Our approach is based on recent bounds of Kloosterman and Gauss sums due to A. Ostafe, I. E. Shparlinski and J. F. Voloch (2021).

1. Introduction

1.1. Previous results. Let $\mathbb{F}_q$ be the finite field of q elements. For $a \in \mathbb{F}_q$ we define the sequence of Dickson polynomials $D_e(X,a)$, $e = 0,1,\ldots$, recursively by the relation

$$D_e(X,a) = XD_{e-1}(X,a) - aD_{e-2}(X,a), \qquad e = 2,3,\ldots,$$

where $D_0(X,a) = 2$ and $D_1(X,a) = X$, see [**9**] for background on Dickson polynomials.

Gomez and Winterhof [**7**] have considered an analogue of the Waring problem for Dickson polynomials over $\mathbb{F}_q$, that is, the question of the existence and estimation of a positive integer s such that the equation

$$D_e(u_1,a) + \ldots + D_e(u_s,a) = c, \qquad u_1,\ldots,u_s \in \mathbb{F}_q, \tag{1.1}$$

is solvable for any $c \in \mathbb{F}_q$, see also [**1**].

In particular, we denote by $g_a(e,q)$ the smallest possible value of s in (1.1) and put $g_a(e,q) = \infty$ if such s does not exist.

Since for $a = 0$ we have $D_e(X,a) = X^e$, this case corresponds to the classical Waring problem in finite fields where recently quite substantial progress has been achieved, see [**2, 3, 4, 19**]; a survey of earlier results can also be found in [**18**]. So, we can restrict ourselves to the case of $a \in \mathbb{F}_q^*$.

Using the identity

$$D_e(v + av^{-1}, a) = v^e + a^e v^{-e}, \tag{1.2}$$

which holds for any nonzero v in the algebraic closure of $\mathbb{F}_q$, see [**7**, Equation (1.1)], and Weil-type bounds of additive character sums with rational functions, Gomez and Winterhof [**7**, Theorem 4.1] proved that for $s \geqslant 3$ the inequality $g_a(e,q) \leqslant s$ holds

---

2020 *Mathematics Subject Classification* 11P05, 11T06, 11T23.
Key words and phrases: Dickson polynomials, Waring problem, Kloosterman sums, Gauss sums.
The authors are grateful to Domingo Gomez, Kaimin Cheng and Arne Winterhof for very helpful comments and suggestions. During the preparation of this work I.E.S. was partially supported by ARC Grants DP230100530 and DP230100534, J.F.V. by the Ministry for Business, Innovation and Employment and by the Marsden Fund, administered by the Royal Society of New Zealand.

- for any $a \in \mathbb{F}_q^*$ and $\gcd(e, q-1) \leqslant 2^{-3} q^{1/2-1/(2s-2)}$;
- for $a = 1$ and $\gcd(e, q+1) \leqslant 2^{-1} q^{1/2-1/(2s-2)}$.

Note that if $\min\{\gcd(e, q-1), \gcd(e, q+1)\} \leqslant 2^{-3} q^{1/4}$ the above result gives a very strong bound $g_a(e, q) \leqslant 3$. Hence, throughout this paper we can assume that

$$\min\{\gcd(e, q-1), \gcd(e, q+1)\} > 2^{-3} q^{1/4}. \tag{1.3}$$

A different approach from [**12**], based on additive combinatorics, in particular on results of Glibichuk [**5**] and Glibichuk and Rudnev [**6**] has allowed to substantially extend the range of e. In particular, by [**12**, Theorem 2], we have $g_a(e, q) \leqslant 16$ if

- for any $a \in \mathbb{F}_q^*$ and
$$\gcd(e, q-1) \leqslant 2^{-3/2}(q-2)^{1/2};$$
- for any $a \in \mathbb{F}_q^*$ which is a square and
$$\gcd(e, q+1) \leqslant 2^{-3/2}(q-2)^{1/2}.$$

Furthermore, for any $\varepsilon > 0$, by [**12**, Theorem 2], we have an upper bound on $g_1(e, q)$ in terms of only ε provided that

$$\min\{\gcd(e, q-1), \gcd(e, q+1)\} \leqslant q^{1-\varepsilon}.$$

We also note that a multivariate version of the above question has been studied in [**14**].

1.2. Main results. Here we use some results and ideas from [**13**] to improve the above bounds in the case of prime $q = p$ and in intermediate ranges of $\gcd(e, p-1)$ and $\gcd(e, p+1)$.

Since we are mostly interested in large values of e, we assume that e is not very small to simplify some technical details.

Theorem 1.1. *Let p be prime. There is an absolute constant $C > 0$ such that for any fixed even integer $s \geqslant 4$, uniformly over $a \in \mathbb{F}_p^*$ the inequality $g_a(e, p) \leqslant s$ holds provided that*

$$\gcd(e, p-1) \leqslant C p^{(4s-7)/(7s+8)},$$

and, if a is a quadratic residue modulo p, also provided that

$$\gcd(e, p+1) \leqslant C \max\left\{p^{(11s-82)/(21s-42)}, p^{(6s-57)/(11s-22)}\right\}.$$

Theorem 1.1 is based on new bounds on Kloosterman and Gauss sums over a thin subgroup, see Lemmas 2.1 and 2.3, and is most interesting in the case when $\min\{\gcd(e, p-1), \gcd(e, p+1)\}$ is large, for example, of order $p^{1/2}$ or slightly larger.

Next, we show that using the classical Weil bound, see (2.1) below, we can still improve previous estimates in certain ranges of $\gcd(e, p-1)$ (below $p^{1/2}$).

Theorem 1.2. *Let p be prime. There is an absolute constant $C > 0$ such that for any fixed even integer $s \geqslant 4$, the inequality $g_a(e, p) \leqslant s$ holds provided that*

$$\gcd(e, p-1) \leqslant C p^{1/2-1/(3s-8)}.$$

We note that the bound of Theorem 1.1 with respect to $\gcd(e, p-1)$ is significantly stronger than with respect to $\gcd(e, p+1)$. Furthermore, while our proof of Theorem 1.2, can easily be adjusted to work with $\gcd(e, p+1)$, it merely recovers the previous result of Gomez and Winterhof [**7**, Theorem 4.1] in this case. This is because we do not have a good version of Lemma 2.6 below, see Question 2.7.

However, for a related equation our approach works and leads to Lemma 2.9 which in turn allows us to get new results for the classical Waring problem with monomials in the norm-one subgroup of $\mathbb{F}_{p^2}$, that is in

$$\mathcal{N}_{p^2} = \{z \in \mathbb{F}_{p^2} : \ \mathrm{Nm}(z) = 1\}, \tag{1.4}$$

where $\mathrm{Nm}(z) = z^{p+1}$ is the $\mathbb{F}_{p^2}/\mathbb{F}_p$ norm of z.

Let $G(k, p)$ denote the smallest possible value of s such that the equation

$$u_1^k + \ldots + u_s^k = c, \qquad u_1, \ldots, u_s \in \mathcal{N}_{p^2},$$

is solvable for any $c \in \mathbb{F}_{p^2}$.

Since we are mostly interested in large values of k when traditional methods do not work, we assume that $\gcd(k, p+1) \geqslant p^{1/6}$ in order to simplify the calculations,.

Theorem 1.3. *Let p be prime. There is an absolute constant $C > 0$ such that for any fixed even integer $s \geqslant 4$, the inequality $G(k, p) \leqslant s$ holds provided that*

$$p^{1/6} \leqslant \gcd(k, p+1) \leqslant C \min\left\{p^{(6s-186)/(11s-116)}, p^{(5s-56)/(10s-56)}\right\}.$$

2. Preliminaries

2.1. Notation. We use $\#\mathcal{A}$ to denote the cardinality of a finite set $\mathcal{A}$.

For a prime p and $u \in \mathbb{Z}$, we let

$$\mathbf{e}_p(u) = \exp(2\pi i u/p).$$

Finally, we recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are equivalent to $|U| \leqslant c|V|$ for some positive constant c which, throughout this work, is absolute.

2.2. Value sets of Dickson polynomials. We note that throughout the paper we use the following trivial observation

$$\{v^e + a^e v^{-e} : \ v \in \mathbb{F}_p^*\} \subseteq \{D_e(u, a) : \ u \in \mathbb{F}_p^*\},$$

see (1.2).

Next, let $\mathrm{Tr}(z) = z + z^p$ be the trace of $z \in \mathbb{F}_{p^2}$ in $\mathbb{F}_p$, respectively.

We also recall the definition of the norm-one subgroup $\mathcal{N}_{p^2}$ of $\mathbb{F}_{p^2}^*$, given by (1.4). Then we note a slightly less obvious inclusion

$$\{b^e \,\mathrm{Tr}\,(v^e) : \ v \in \mathcal{N}_{p^2}\} \subseteq \{D_e(u, a) : \ u \in \mathbb{F}_p\}$$

provided that $a = b^2$, $b \in \mathbb{F}_p^*$, is a quadratic residue modulo p. Indeed, we first note that for $v \in \mathcal{N}_{p^2}$

$$bv + a(bv)^{-1} = b\left(v + v^{-1}\right) = b\,\mathrm{Tr}(v) \in \mathbb{F}_p.$$

Thus

$$\{D_e\left(bv + a(bv)^{-1}, a\right) : \ v \in \mathcal{N}_{p^2}\} \subseteq \{D_e(u, a) : \ u \in \mathbb{F}_p\}.$$

On the other hand, from (1.2) we have

$$D_e\left(bv + a(bv)^{-1}, a\right) = (bv)^e + a^e(bv)^{-e} = b^e \,\mathrm{Tr}\,(v^e).$$

2.3. Bounds of some exponential sums. Given a multiplicative subgroup $\mathcal{H} \subseteq \mathbb{F}_p^*$ and $\alpha, \beta \in \mathbb{F}_p$ we consider Kloosterman sums over $\mathcal{H}$

$$\mathcal{K}_p(\mathcal{H}; \alpha, \beta) = \sum_{u \in \mathcal{H}} \mathbf{e}_p\left(\alpha u + \beta u^{-1}\right).$$

The classical Weil bound for exponential sums with rational functions, see, for example [**11**, Theorem 2], implies

$$\mathcal{K}_p(\mathcal{H}; \alpha, \beta) \ll p^{1/2} \tag{2.1}$$

provided $(\alpha, \beta) \neq (0, 0)$.

The following bound is given by [**13**, Corollary 2.9].

Lemma 2.1. *Let p be prime and let $\mathcal{H}$ be a multiplicative subgroup of $\mathbb{F}_p^*$ of order τ. Then uniformly over $(\alpha, \beta) \in \mathbb{F}_p^2$, $(\alpha, \beta) \neq (0, 0)$, we have*

$$\mathcal{K}_p(\mathcal{H}; \alpha, \beta) \ll \min\{p^{1/2}, \tau^{23/36} p^{1/6}, \tau^{20/27} p^{1/9}\}.$$

We also need a similar result for Gaussian sums

$$\mathcal{G}_p(\mathcal{H}; \alpha) = \sum_{u \in \mathcal{H}} \mathbf{e}_p\left(\mathrm{Tr}\,(\alpha u)\right),$$

over $\mathbb{F}_{p^2}$.

We recall the definition of $\mathcal{N}_{p^2}$ in (1.4). We need the following analogue of (2.1), following easily from the bound

$$\sum_{u \in \mathcal{N}_{p^2}} \chi(u)\, \mathbf{e}_p\left(\mathrm{Tr}\,(\alpha u)\right) \ll p^{1/2}$$

with an arbitrary multiplicative character χ of $\mathbb{F}_{p^2}^*$, which in turn is a very special case of a result of Li [**8**, Theorem 2].

Lemma 2.2. *Let p be prime and let $\mathcal{H}$ be a multiplicative subgroup of $\mathcal{N}_{p^2}$ of order τ. Then uniformly over $\alpha \in \mathbb{F}_{p^2}^*$, we have*

$$\mathcal{G}_{p^2}(\mathcal{H}; \alpha) \ll p^{1/2}.$$

Furthermore, by [**13**, Corollary 2.9], we have the following.

Lemma 2.3. *Let p be prime and let $\mathcal{H}$ be a multiplicative subgroup of $\mathcal{N}_{p^2}$ of order τ. Then uniformly over $\alpha \in \mathbb{F}_{p^2}^*$, we have*

$$\mathcal{G}_{p^2}(\mathcal{H}; \alpha) \ll \min\left\{\tau^{13/20} p^{1/6}, \tau^{34/45} p^{1/9}, p^{1/2}\right\}.$$

Proof. It has been shown in [**13**, Corollary 2.10].

$$\mathcal{G}_{p^2}(\mathcal{H}; \alpha) \ll \min\left\{\tau^{1/4} p^{1/2}, \tau^{13/20} p^{1/6}, \tau^{34/45} p^{1/9}\right\}.$$

However, it is easy to see that the first bound is always dominated by the bound of Lemma 2.2. □

We note that it is crucial for our improvement that the bounds of Lemmas 2.1 and 2.3 are nontrivial for $\tau < p^{1/2}$.

2.4. Bounds on the number of solutions to some equations. We first recall the following result, combining [**17**, Theorem (i)] with the Weil bound [**10**, Equation (5.7)] which gives an upper bound on the number of points on curves over $\mathbb{F}_p$.

Lemma 2.4. *Let p be prime and let $F(X,Y) \in \mathbb{F}_p[X,Y]$ be an absolutely irreducible polynomial of degree d. Then*

$$\#\{(x,y) \in \mathbb{F}_p^2 : \ F(x,y) = 0\} \leqslant 4d^{4/3}p^{2/3} + 3p.$$

We also need the following characterisation of possible factorisations of certain bivariate polynomials over the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$.

Lemma 2.5. *Let p be prime and let $F_e = X^{2e}Y^e + X^eY^{2e} + X^e + Y^e + AX^eY^e \in \bar{\mathbb{F}}_p[X,Y]$ with $p \nmid e$ and assume that $A \neq 0, \pm 4$. Then, for some $r \mid 8$, F_e has r absolutely irreducible factors of degree $3e/r$.*

Proof. First we prove the following claim: if F_1 is irreducible and $K = \bar{\mathbb{F}}_p(x,y)$ is the function field of the curve defined by $F_1 = 0$, then the number of irreducible factors of F_e is the same as the index of the Galois group Γ of $K(x^{1/e}, y^{1/e})/K$ in the group $\mu_e \times \mu_e$ (where $x^{1/e}, y^{1/e}$ are e-th roots of x, y in some extension of K and μ_e is the group of e-th roots of unity).

Indeed, if G is the irreducible factor of F_e with $G(x^{1/e}, y^{1/e}) = 0$, the Galois group Γ preserves G, in the sense that $G(\zeta X, \eta Y) = G(X,Y)$ for any $(\zeta, \eta) \in \Gamma$. On the other hand, $F_e(\zeta X, \eta Y) = F_e(X,Y)$, for any $(\zeta,\eta) \in \mu_e \times \mu_e$ so if we let

$$H(X,Y) = \prod_{(\zeta,\eta)\in\Omega_e} G(\zeta X, \eta Y),$$

with (ζ, η) running through the set Ω_e of coset representatives of Γ in $\mu_e \times \mu_e$, we have $H \mid F_e$ and $H(\zeta X, \eta Y) = H(X,Y)$, $(\zeta,\eta) \in \mu_e \times \mu_e$. It follows that $H = H_1(X^e, Y^e)$ and $H_1 \mid F_1$. Since F_1 is irreducible by assumption, we get $H_1 = F_1$, $H = F_e$ and the claim follows.

It is now enough to show that the extension of K obtained by adjoining e-th roots of x and y has degree e^2/r over K for some r as in the statement of the lemma. The proof now follows a similar strategy to the proof of [**13**, Lemma 4.3].

One can check directly, for example, with a computer algebra package, that F_1 is absolutely irreducible if $A \neq 0$ and that $F_1 = 0$ defines a smooth projective curve if, in addition, $A \neq \pm 4$.

We repeatedly use the elementary fact that $Z^e - c$, $c \in K$ has a factor of degree d in $K[Z]$ if and only if a is a d-th power in K and $d \mid e$. Indeed, if the factor is $\prod_{i\in I}(Z - \zeta^i c^{1/e})$, then the constant term is (up to a factor in $\bar{\mathbb{F}}_p$) equal to $c^{d/e}$ and the result follows.

Note that $[K : \bar{\mathbb{F}}_p(xy, x/y)] = 2$. The divisor of the function xy on $F_1 = 0$ is $2P - 2Q$ where $P = (0,0)$ and Q is the point at infinity on the line $X + Y = 0$. So the polynomial $Z^e - xy$ is irreducible over K for e odd, by [**15**, Proposition 3.7.3]. To treat the case of general e, it is then enough to treat the case $e = 2$. But xy cannot be a square in K as this would give a function of divisor $P - Q$ which is impossible since $F_1 = 0$ defines a smooth projective curve of degree three, hence genus one so K cannot have a function of degree one.

Let z be a root of $Z^e - xy$ and consider the field $K(z)$. The function x/y has divisor $4R - 4S$ on the curve $F_1 = 0$ where R, S are the points at infinity on the y-axis and x-axis respectively. It follows that the function x/y is not an eighth-power or an odd power in $K(z)$ because R, S are unramified in $K(z)/K$. So the extension of $K(z)$ obtained by adjoining a root of $W^e = x/y$ has degree $e, e/2$ or $e/4$ over $K(z)$ and the result follows. □

We use Lemmas 2.4 and 2.5 to estimate the number of solutions of the following equation.

Lemma 2.6. *Let p be prime and let $\mathcal{H}$ be a multiplicative subgroup of $\mathbb{F}_p^*$ of order τ. Then the number of solutions R_τ to the equation*

$$u + u^{-1} + v + v^{-1} = x + x^{-1} + y + y^{-1}, \qquad u, v, x, y \in \mathcal{H},$$

satisfies

$$R_\tau \ll \tau^{8/3} + \tau^4/p.$$

Proof. There are obviously at most 4τ choices of $(u, v) \in \mathcal{H}^2$ for which $u + u^{-1} + v + v^{-1} \in \{0, -4\}$, and there are also at most $O(\tau^2)$ pairs $(x, y) \in \mathcal{H}^2$ which satisfy the above equation and thus we have $O(\tau^2)$ such solutions. We now fix $(u, v) \in \mathcal{H}^2$ such that for $A = -\left(u + u^{-1} + v + v^{-1}\right)$ we have $A \neq 0, 4$. Clearly

$$\#\{(x, y) \in \mathcal{H}^2 : \ x + x^{-1} + y + y^{-1} - A = 0\} \leqslant e^{-2} \#\{(x, y) \in \mathbb{F}_p^2 : \ F_e(x, y) = 0\},$$

where $e = (p-1)/\tau$ and $F_e(X, Y)$ is as in Lemma 2.5. Applying Lemma 2.4 to each of at most 8 irreducible factors of F_e each of degree at most $3e$, we obtain

$$R_\tau \ll \tau^2 + e^{-2}\left(e^{4/3}p^{2/3} + p\right)\tau^2,$$

and the result follows. □

To improve our main results for $\gcd(e, p+1)$ we need to obtain good estimates on the number of solutions to the following trace-equation.

Remark 2.7. Given a subgroup $\mathcal{H} \subseteq \mathcal{N}_{p^2}$, it is an interesting question to obtain a version of Lemma 2.6 for the equation

$$\mathrm{Tr}(u + v) = \mathrm{Tr}(x + y), \qquad u, v, x, y \in \mathcal{H}.$$

While the question posed in Remark 2.7 is still open, we are able to estimate the so-called *additive energy* of a subgroup of $\mathcal{N}_{p^2}$. We start with an analogue of [**13**, Lemma 4.5], which we believe is of independent interest.

Lemma 2.8. *Let p be prime and let $t = k(p-1)$, where k is a positive integer with* $\gcd(k, p) = 1$. *Then for $a \in \mathbb{F}_{p^2}$ with $a \neq 0$, for the polynomial*

$$F(X, Y) = X^t + Y^t + a \in \mathbb{F}_{p^2}[X, Y]$$

we have

$$\#\{(x, y) \in \mathbb{F}_{p^2}^2 : \ F(x, y) = 0\} \ll t^{6/5}p^{8/5} + p^3.$$

Proof. The proof follows a strategy which is similar to that used in the proof of [**13**, Lemma 4.5].

Clearly we can assume that

$$k < 2^{-5/4}p \tag{2.2}$$

as otherwise the result is trivial.

We know that the equation $F(X,Y) = 0$ defines a smooth, hence absolutely irreducible curve, of degree s that we call E. Let $\alpha \in \mathbb{F}_{p^2}$ satisfy $\alpha^t = -a$. The point $P_0 = (0,\alpha)$ defines a point on E and the line $Y = \alpha$ meets E at P_0 with multiplicity s, since $F(X,\alpha) = X^t$. We denote by x, y the functions on E satisfying $F(x,y) = 0$.

We want to bound the number R of solutions of $F = 0$ in $\mathbb{F}_{p^2}$. We follow the proof of Lemma 2.4 given in [**17**, Theorem (i)]. It proceeds by considering, for some integer m, the embedding of E in $\mathbb{P}^n$, with $n = (m+2)(m+1)/2 - 1$, given by the monomials in X, Y of degree at most m.

We recall some definitions and some results from [**16**]. We consider the given embedding of E in $\mathbb{P}^n$. For a point $P \in E$, the order sequence of E at P is the sequence $0 = j_0 < j_1 < \cdots < j_n$ of all possible intersection multiplicities at P of E with a hyperplane in $\mathbb{P}^n$. The embedding is *classical* if the order sequence at a generic point of E is $0, 1, \ldots, n$ and non-classical, otherwise. The point P is an osculation point if the order sequence at P is not $0, 1, \ldots, n$ and a Weierstrass point if the order sequence at P is not the same as the order sequence at a generic point of E. These two notions coincide if the embedding is classical. This embedding is $\mathbb{F}_q$-*Frobenius classical* if, for a generic point of E, the numbers $0, 1, \ldots, n-1$ are the possible intersection multiplicities at P of E with a hyperplane in $\mathbb{P}^n$ that also passes through the image of P under the $\mathbb{F}_q$-Frobenius map.

If this embedding is Frobenius classical, then by [**16**, Theorem 2.13]

$$R \leqslant (n-1)t(t-3)/2 + mt(p^2+n)/n. \tag{2.3}$$

If

$$m < p/2 \qquad \text{and} \qquad p \nmid \prod_{i=1}^{m} \prod_{j=-m}^{m-i} (ti + j) \tag{2.4}$$

then we claim that the above embedding is classical. Indeed, the order sequence of the embedding at the point P_0 defined above consists of the integers $ti + j$, $i, j \geqslant 0$, $i + j \leqslant m$ as follows by considering the order of vanishing at P_0 of the functions $x^j(y-\alpha)^i$, $i, j \geqslant 0$, $i + j \leqslant m$. The claim now follows from [**16**, Corollary 1.7].

If the embedding is Frobenius classical, we get the inequality (2.3) as mentioned above. If the embedding is classical but Frobenius nonclassical then, by [**16**, Corollary 2.16], every rational point of E is a Weierstrass point for the embedding. Hence, as the embedding is classical, we get

$$R \leqslant n(n+1)t(t-3)/2 + mt(n+1) \tag{2.5}$$

since the right-hand side is the number of Weierstrass points of the embedding counted with multiplicity, see [**16**, Page 6]. Indeed, we note that in the present case, the degree of the embedding (denoted by d in [**16**]) is mt and the order sequence (denoted by ε_i in [**16**]) is just $\varepsilon_i = i$ since the embedding is classical. Thus $\varepsilon_1 + \cdots + \varepsilon_n = n(n+1)/2$.

We now choose

$$m = \min\left\{\left\lfloor (p/k)^{1/5}\right\rfloor, k-1\right\}. \tag{2.6}$$

If $|i|, |j| \leqslant m$, then for the choice of m as in (2.6) we have

$$0 < |-ki + j| \leqslant 2km \leqslant 2k^{4/5}p^{1/5} < p \tag{2.7}$$

provided that (2.2) holds.

Note also that $ti + j \equiv -ki + j \pmod p$, as $t = k(p-1)$. Hence,

$$\prod_{i=1}^{m}\prod_{j=-m}^{m-i}(ti+j) \equiv \prod_{i=1}^{m}\prod_{j=-m}^{m-i}(-ki+j) \pmod p.$$

Thus from the definition of m in (2.6) and the inequalities (2.7) we see that the conditions (2.4) are satisfied. We note that (2.3) and (2.5) can be simplified and combined as

$$R \ll \max\{m^2t^2 + tp^2/m, m^4t^2\} \ll tp^2/m + m^4t^2.$$

Since $m \ll (p/k)^{1/5} \ll (p^2/t)^{1/5}$, we have $m^4t^2 \ll tp^2/m$ and thus we obtain

$$R \ll tp^2/m \ll kp^3/m.$$

Recalling the choice of m in (2.6), we obtain the desired result. □

We note that for $k \gg p^{1/6}$ the bound of Lemma 2.8 is $O\left(t^{6/5}p^{8/5}\right)$.

Using Lemma 2.8 instead of Lemma 2.4 (and noticing that $\tau = (p^2-1)/t$), we derive the following analogue of Lemma 2.6.

Lemma 2.9. *Let p be prime and let $\mathcal{H}$ be a multiplicative subgroup of $\mathcal{N}_{p^2}$ of order τ. Then the number of solutions T_τ to the equation*

$$u + v = x + y, \qquad u, v, x, y \in \mathcal{H},$$

satisfies

$$T_\tau \ll \tau^{14/5} + \tau^4/p.$$

3. Proof of Theorem 1.1

3.1. Small $\gcd(e, p-1)$**.** Let

$$\tau = \frac{p-1}{\gcd(e, p-1)},$$

and let $\mathcal{H}$ be the subgroup of $\mathbb{F}_p$ of order τ. By our assumption (1.3) on e, we have

$$\tau \ll p^{3/4}. \tag{3.1}$$

We write $s = 2r$ and denote by $\mathcal{F}_r$ the set of $f \in \mathbb{F}_p$ which cannot be represented as

$$f = \sum_{i=1}^{r}\left(u_i + au_i^{-1}\right), \qquad u_i \in \mathcal{H},\ i = 1, \ldots, s.$$

In particular, for the number $N_r(\mathcal{F}_r)$ of the solutions to the equation

$$f = \sum_{i=1}^{r}\left(u_i + au_i^{-1}\right), \qquad f \in \mathcal{F}_r,\ u_i \in \mathcal{H},\ i = 1, \ldots, s,$$

we have $N_r(\mathcal{F}_r) = 0$. We see from (1.2) that each element of the complementing set $\mathcal{R}_r = \mathbb{F}_p \setminus \mathcal{F}_r$ can be represented by a sum of s values of $D_e(x,a)$, $x \in \mathbb{F}_p$.

On the other hand, by the orthogonality of exponential functions, we have

$$\begin{aligned} N_r(\mathcal{F}_r) &= \sum_{u_1,\ldots,u_r \in \mathcal{H}} \sum_{f \in \mathcal{F}_r} \frac{1}{p} \sum_{\alpha \in \mathbb{F}_p} \mathbf{e}_p\left(\alpha\left(\sum_{i=1}^{r}(u_i + au_i^{-1}) - f\right)\right) \\ &= \frac{1}{p}\sum_{\alpha \in \mathbb{F}_p}\left(\sum_{u\in\mathcal{H}} \mathbf{e}_p\left(\alpha\left(u + au^{-1}\right)\right)\right)^r \sum_{f\in\mathcal{F}_r} \mathbf{e}_p\left(-\alpha f\right) \\ &= \frac{1}{p}(\#\mathcal{H})^r \#\mathcal{F}_r + O\left(p^{-1}\Delta\right), \end{aligned}$$

where

$$\Delta = \sum_{\alpha\in\mathbb{F}_p^*}\left|\sum_{u\in\mathcal{H}} \mathbf{e}_p\left(\alpha\left(u+au^{-1}\right)\right)\right|^r \left|\sum_{f\in\mathcal{F}_r}\mathbf{e}_p\left(\alpha f\right)\right|.$$

Thus, recalling that $N_r(\mathcal{F}_r) = 0$, we obtain

$$\tau^r \#\mathcal{F}_r \ll \Delta \tag{3.2}$$

Next, using the second bound of Lemma 2.1, we write

$$\Delta \ll \left(\tau^{20/27}p^{1/9}\right)^{r-2}\Gamma, \tag{3.3}$$

where (after extending the summation to all $\alpha \in \mathbb{F}_p$) we can take

$$\Gamma = \sum_{\alpha\in\mathbb{F}_p}\left|\sum_{u\in\mathcal{H}} \mathbf{e}_p\left(\alpha\left(u+au^{-1}\right)\right)\right|^2 \left|\sum_{f\in\mathcal{F}_r}\mathbf{e}_p\left(\alpha f\right)\right|.$$

By the Cauchy inequality

$$\Gamma^2 \leqslant \sum_{\alpha\in\mathbb{F}_p}\left|\sum_{u\in\mathcal{H}} \mathbf{e}_p\left(\alpha\left(u+au^{-1}\right)\right)\right|^4 \sum_{\alpha\in\mathbb{F}_p}\left|\sum_{f\in\mathcal{F}_r}\mathbf{e}_p\left(\alpha f\right)\right|^2.$$

Using the orthogonality of exponential functions again and also Lemma 2.6, and recalling (3.1), we infer

$$\Gamma^2 \ll \left(p\tau^{8/3} + \tau^4\right)p\#\mathcal{F}_r \ll p^2\tau^{8/3}\#\mathcal{F}_r.$$

We now see from (3.2) and (3.3) that

$$\tau^r\#\mathcal{F}_r \ll \left(\tau^{20/27}p^{1/9}\right)^{r-2} p\tau^{4/3}\left(\#\mathcal{F}_r\right)^{1/2}, \tag{3.4}$$

or

$$\begin{aligned} \#\mathcal{F}_r &\ll \tau^{40r/27-80/27+8/3-2r}p^{2(r-2)/9+2} = \tau^{-14r/27-8/27}p^{2r/9+14/9} \\ &\ll \gcd(e,p-1)^{14r/27+8/27}p^{-8r/27+34/27}. \end{aligned}$$

Therefore, there is an absolute constant $C > 0$ such that for

$$\gcd(e,p-1) \leqslant Cp^{(8r-7)/(14r+8)}$$

we have $\#\mathcal{F}_r < p/2$.

Thus, for any $f \in \mathbb{F}_p$ we see that the set $f - \mathcal{R}_r = \{f - u : \ u \in \mathcal{R}_r\}$ of cardinality $\#\mathcal{R}_r > p/2$ has a nontrivial intersection with $\mathcal{R}_r$. Hence $f \in \mathcal{R}_{2r}$.

Remark 3.1. Certainly the first bound of Lemma 2.1 can also be used in our argument. However the bound it implies is always weaker than a combination of the current bound and the bound of Theorem 1.2.

3.2. Small $\gcd(e, p+1)$**.** We now let

$$\tau = \frac{p+1}{\gcd(e, p+1)},$$

and let $\mathcal{H}$ be the subgroup of $\mathcal{N}_{p^2}$ of order τ.

This time we write $s = 2r$ and denote by $\mathcal{F}_r$ the set of $f \in \mathbb{F}_p$ which cannot be represented as

$$f = \sum_{i=1}^{r} u_i + u_i^{-1} = \sum_{i=1}^{r} \mathrm{Tr}(u_i), \qquad u_i \in \mathcal{H},\ i = 1, \ldots, s.$$

In particular, for the number $N_r(\mathcal{F}_r)$ of the solutions to the equation

$$f = \sum_{i=1}^{r} \mathrm{Tr}(u_i), \qquad f \in \mathcal{F}_r,\ u_i \in \mathcal{H},\ i = 1, \ldots, s,$$

we have $N_r(\mathcal{F}_r) = 0$. We see from (1.2) that each element the complementing set $\mathcal{R}_r = \mathbb{F}_p \setminus \mathcal{F}_r$ can be represented by a sum of s values of $D_e(x, a)$, $x \in \mathbb{F}_p$

On the other hand, by the orthogonality of exponential functions, we have

$$\begin{aligned} N_r(\mathcal{F}_r) &= \sum_{u_1,\ldots,u_r \in \mathcal{H}} \sum_{f \in \mathcal{F}_r} \frac{1}{p} \sum_{\alpha \in \mathbb{F}_p} \left(\sum_{u \in \mathcal{H}} \mathbf{e}_p\left(\alpha \,\mathrm{Tr}(u)\right) \right)^r \sum_{f \in \mathcal{F}_r} \mathbf{e}_p\left(-\alpha f\right) \\ &= \frac{1}{p} \sum_{\alpha \in \mathbb{F}_p} \mathbf{e}_p\left(\alpha \left(\sum_{i=1}^{r} \mathrm{Tr}(u_i) - f \right) \right) \\ &= \frac{1}{p} (\#\mathcal{H})^r \#\mathcal{F}_r + O(p^{-1}\Delta), \end{aligned}$$

where

$$\Delta = \sum_{\alpha \in \mathbb{F}_p^*} \left| \sum_{u \in \mathcal{H}} \mathbf{e}_p\left(\alpha \,\mathrm{Tr}(u)\right) \right|^r \left| \sum_{f \in \mathcal{F}_r} \mathbf{e}_p\left(\alpha f\right) \right|.$$

Thus, recalling that $N_r(\mathcal{F}_r) = 0$, we obtain a full analogue of (3.2).

Next, using the first bound of Lemma 2.3, we write

$$\Delta \ll \left(\tau^{13/20} p^{1/6} \right)^{r-1} \Gamma, \qquad (3.5)$$

where (after extending the summation to all $\alpha \in \mathbb{F}_p$) we can take

$$\Gamma = \sum_{\alpha \in \mathbb{F}_p} \left| \sum_{u \in \mathcal{H}} \mathbf{e}_p\left(\alpha \,\mathrm{Tr}(u)\right) \right| \left| \sum_{f \in \mathcal{F}_r} \mathbf{e}_p\left(\alpha f\right) \right|.$$

We remark that in Section 3.1, Lemma 2.1 is used $r-2$ times, while now the bounds of Lemma 2.3 is used $r-1$ times. This is because we are lacking an appropriate analogue of Lemma 2.6 in this case.

Next by the Cauchy inequality

$$\Gamma^2 \leqslant \sum_{\alpha\in\mathbb{F}_p} \left| \sum_{u\in\mathcal{H}} \mathbf{e}_p\left(\alpha\,\mathrm{Tr}(u)\right) \right|^2 \sum_{\alpha\in\mathbb{F}_p} \left| \sum_{f\in\mathcal{F}_r} \mathbf{e}_p\left(\alpha f\right) \right|^2 .$$

We observe that for elements $u.v \in \mathcal{N}_{p^2}$, the equation $\mathrm{Tr}(u) = \mathrm{Tr}(v)$ implies that u and v have the same characteristic polynomial. Thus, either $u = v$ or $u = v^p = v^{-1}$ and by the orthogonality of exponential functions again, we derive

$$\Gamma^2 \ll p^2\#\mathcal{H}\#\mathcal{F}_r \ll p^2\tau\#\mathcal{F}_r.$$

We now see from (3.2) and (3.5) that

$$\tau^r\#\mathcal{F}_r \ll \left(\tau^{13/20}p^{1/6}\right)^{r-1} p\tau\left(\#\mathcal{F}_r\right)^{1/2}, \qquad (3.6)$$

or

$$\begin{aligned}\#\mathcal{F}_r &\ll \tau^{13r/10-13/10+2-2r}p^{(r-1)/3+2} = \tau^{-7(r-1)/10}p^{r/3+5/3}\\ &\ll \gcd(e,p+1)^{7(r-1)/10}p^{-(11r-41)/30}.\end{aligned}$$

Therefore, there is an absolute constant $C > 0$ such that for

$$\gcd(e,p+1) \leqslant Cp^{(11r-41)/(21r-21)}$$

we have $\#\mathcal{F}_r < p/2$ and we conclude the proof as before.

Similarly, using the second bound of Lemma 2.3, instead of (3.6) we derive that

$$\tau^r\#\mathcal{F}_r \ll \left(\tau^{34/45}p^{1/9}\right)^{r-1} p\tau\left(\#\mathcal{F}_r\right)^{1/2}.$$

Then after simple calculations we obtain that $\mathcal{R}_{2r} = \mathbb{F}_p$ provided

$$\gcd(e,p+1) \leqslant Cp^{(12r-57)/(22r-22)}.$$

4. Proof of Theorem 1.2

We proceed as in the proof of Theorem 1.1. Indeed, an application of the bound (2.1), instead of (3.4) leads us to the inequality

$$\tau^r\#\mathcal{F}_r \ll \left(p^{1/2}\right)^{r-2} p\tau^{4/3}\left(\#\mathcal{F}_r\right)^{1/2}.$$

This implies that $\mathcal{R}_{2r} = \mathbb{F}_p$ provided

$$\gcd(e,p-1) \leqslant Cp^{(3r-5)/(6r-8)}$$

and we obtain the desired result with $s = 2r$.

5. Proof of Theorem 1.3

Clearly, without loss of generality we can assume that $k \mid p+1$. The set of powers x^k, $x \in \mathcal{N}_{p^2}$ forms a subgroup $\mathcal{H}$ of $\mathcal{N}_{p^2}$ of order

$$\tau = (p+1)/k.$$

Note that since $k \geqslant p^{1/6}$ we get $\tau \ll p^{5/6}$. In this case the bound of Lemma 2.9 takes the form

$$T_\tau \ll \tau^{14/5}.$$

Similarly to the proof of Theorem 1.1, we write $s = 2r$ and denote by $\mathcal{G}_r$ the set of $f \in \mathbb{F}_{p^2}$ which cannot be represented as

$$f = \sum_{i=1}^{r} u_i, \qquad u_i \in \mathcal{H},\ i = 1, \ldots, s.$$

The previous argument used with Lemmas 2.3 and 2.9 gives the following analogues of (3.4)

$$\tau^r \#\mathcal{G}_r \ll \begin{cases} \left(\tau^{34/45} p^{1/9}\right)^{r-2} p^2 \tau^{14/5} \left(\#\mathcal{G}_r\right)^{1/2}, \\ \left(p^{1/2}\right)^{r-2} p^2 \tau^{14/5} \left(\#\mathcal{G}_r\right)^{1/2}. \end{cases}$$

We note that here we do not use the first bound of Lemma 2.3 as it does not seems to give anything better than a combination of the other two.

These inequalities imply that for an appropriate absolute constant C if one of the conditions

$$k \leqslant C \begin{cases} p^{(6r-93)/(11r-58)}, \\ p^{(5r-28)/(10r-28)}, \end{cases}$$

is satisfied, then $\#\mathcal{G}_r < p^2/2$ and the previous argument concludes the proof with $s = 2r$.

References

[1] W.-S. Chou, G. L. Mullen and B. Wassermann, *On the number of solutions of equations of Dickson polynomials over finite fields*, Taiwanese J. Math. **12** (2008), 917–931. Doi: 10.11650/twjm/1500404986.

[2] J. A. Cipra, *Waring's number in a finite field*, Integers **9** (2009), A34, 435–440. Doi: 10.1515/INTEG.2009.036.

[3] J. A. Cipra, T. Cochrane and C. Pinner, *Heilbronn's conjecture on Waring's number (mod p)*, J. Number Theory **125** (2007), 289–297. Doi: 10.1016/j.jnt.2006.12.001.

[4] A. A. Glibichuk, *Sums of powers of subsets of an arbitrary finite field*, Izv. Ross. Akad. Nauk Ser. Mat. **75** (2011), 35–68. Doi: 10.1070/IM2011v075n02ABEH002534.

[5] A. A. Glibichuk, *Sums of powers of subsets of an arbitrary finite field*, Izv. Ross. Akad. Nauk Ser. Mat. **75** (2011), 35–68. Doi: 10.1070/IM2011v075n02ABEH002534.

[6] A. Glibichuk and M. Rudnev, *On additive properties of product sets in an arbitrary finite field*, J. Anal. Math. **108** (2009), 159–170. Doi: 10.1007/s11854-009-0021-4.

[7] D. Gomez and A. Winterhof, *Waring's problem in finite fields with Dickson polynomials*, Finite fields: theory and applications, Contemp. Math. 518, 185–192, Amer. Math. Soc., Providence, RI, 2010. Doi: 10.1090/conm/518/10205.

[8] W.-C. W. Li, *Character sums over norm groups*, Finite Fields Appl. **12** (2006), 1–15. Doi: 10.1016/j.ffa.2004.06.006.

[9] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics 65, Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[10] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics 9, American Mathematical Society, Providence, RI, 1996. Doi: 10.1090/gsm/009.

[11] C. J. Moreno and O. Moreno, *Exponential sums and Goppa codes. I*, Proc. Amer. Math. Soc. **111** (1991), 523–531. Doi: 10.2307/2048345.

[12] A. Ostafe and I. E. Shparlinski, *On the Waring problem with Dickson polynomials in finite fields*, Proc. Amer. Math. Soc. **139** (2011), 3815–3820. Doi: 10.1090/S0002-9939-2011-10843-8.

[13] A. Ostafe, I. E. Shparlinski and J. F. Voloch, *Equations and character sums with matrix powers, Kloosterman sums over small subgroups, and quantum ergodicity*, Int. Math. Res. Not. IMRN (2023), 14196–14238. Doi: 10.1093/imrn/rnac226.

[14] A. Ostafe, D. Thomson and A. Winterhof, *On the Waring problem with multivariate Dickson polynomials*, Theory and applications of finite fields, Contemp. Math. 579, 153–161, Amer. Math. Soc., Providence, RI, 2012. Doi: 10.1090/conm/579/11527.

[15] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics 254, Springer-Verlag, Berlin, 2009.

[16] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), 1–19. Doi: 10.1112/plms/s3-52.1.1.

[17] J. F. Voloch, *On the number of values taken by a polynomial over a finite field*, Acta Arith. **52** (1989), 197–201. Doi: 10.4064/aa-52-2-197-201.

[18] A. Winterhof, *On Waring's problem in finite fields*, Acta Arith. **87** (1998), 171–177. Doi: 10.4064/aa-87-2-171-177.

[19] A. Winterhof and C. van de Woestijne, *Exact solutions to Waring's problem for finite fields*, Acta Arith. **141** (2010), 171–190. Doi: 10.4064/aa141-2-3.

Igor Shparlinski
School of Mathematics and Statistics,
University of New South Wales,
Sydney, NSW 2052
Australia
igor.shparlinski@unsw.edu.au

José Felipe Voloch
School of Mathematics and Statistics,
University of Canterbury,
Private Bag 4800,
Christchurch 8140,
New Zealand
felipe.voloch@canterbury.ac.nz