



INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique


Stephen D. Cohen, Giorgos Kapetanakis and Lucas Reis

The existence of \mathbb{F}_q -primitive points on curves using freeness

Volume 360 (2022), p. 641-652

<<https://doi.org/10.5802/crmath.328>>

© Académie des sciences, Paris and the authors, 2022.
Some rights reserved.

 This article is licensed under the
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.
<http://creativecommons.org/licenses/by/4.0/>



Les Comptes Rendus. Mathématique sont membres du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org



Number theory / *Théorie des nombres*

The existence of \mathbb{F}_q -primitive points on curves using freeness

Stephen D. Cohen^{*, a}, Giorgos Kapetanakis^b and Lucas Reis^c

^a 6 Bracken Road, Portlethen, Aberdeen AB12 4TA, Scotland, UK

^b Department of Mathematics, University of Thessaly, 3rd km Old National Road Lamia-Athens, 35100 Lamia, Greece

^c Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte MG, 31270901, Brazil

E-mails: Stephen.Cohen@glasgow.ac.uk, gnkapet@gmail.com, lucasreismat@gmail.com

Abstract. Let \mathcal{C}_Q be the cyclic group of order Q , n a divisor of Q and r a divisor of Q/n . We introduce the set of (r, n) -free elements of \mathcal{C}_Q and derive a lower bound for the number of elements $\theta \in \mathbb{F}_q$ for which $f(\theta)$ is (r, n) -free and $F(\theta)$ is (R, N) -free, where $f, F \in \mathbb{F}_q[x]$. As an application, we consider the existence of \mathbb{F}_q -primitive points on curves like $y^n = f(x)$ and find, in particular, all the odd prime powers q for which the elliptic curves $y^2 = x^3 \pm x$ contain an \mathbb{F}_q -primitive point.

Keywords. finite fields, character sums, elliptic curves.

2020 Mathematics Subject Classification. 11T30, 11A07, 11T23.

Manuscript received 6th December 2021, revised and accepted 13th January 2022.

1. Introduction

For a prime power q , let \mathbb{F}_q be the finite field with q elements. It is well-known that the multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is cyclic and any generator of such a group is a *primitive* element of \mathbb{F}_q . Primitive elements are a recurrent object of study in the finite field theory, mainly because of their applications in practical situations such as the discrete logarithm problem. Vinogradov obtained a simple character sum formula for the indicator (characteristic) function of such elements [17, Theorem 6.3.90]. The latter can be subsumed into a general concept of freeness, which is strongly related to the multiplicative structure of the elements of \mathbb{F}_q^* . More precisely, for a divisor d of $q-1$, an element of \mathbb{F}_q is *d-free* if is not of the form β^s for any divisor $s > 1$ of d . Evidently, primitive elements of \mathbb{F}_q are just the $(q-1)$ -free elements of \mathbb{F}_q .

From a theoretical point of view, many authors have explored the existence and number of primitive elements of finite fields with additional properties. The main tools are Vinogradov's

* Corresponding author.

The first author is Emeritus Professor of Number Theory, University of Glasgow

formula and bounds on multiplicative character sums such as Weil's bound. A common theme is the description of finite fields containing a pair $(\alpha, F(\alpha))$ of primitive elements of \mathbb{F}_q , where $F \in \mathbb{F}_q(x)$ is a rational function. The latter is equivalent to looking at \mathbb{F}_q -rational points on the 0-genus curve $\mathcal{C} : y = F(x)$ whose coordinates are primitive. Such a point will be referred to as an \mathbb{F}_q -primitive point. Relevant articles containing relatively complete results on the existence of \mathbb{F}_q -primitive points on a curve $y = F(x)$ include [11] (for F a general linear polynomial), [10, Corollary 2 (i), (ii)] (for $F(x) = x \pm 1/x$) and [1] (for F a general quadratic polynomial). Additionally, [4] applies to rational functions $F = f_1/f_2$ where f_1 and f_2 are polynomials, with partial numerical results for $\deg f_1 + \deg f_2 \leq 7$. A natural extension would be to consider the existence of \mathbb{F}_q -primitive points on curves of the form $y^n = F(x)$, where n is an integer indivisible by the field characteristic and F is a rational function in $\mathbb{F}_q(x)$. An important example would be that of elliptic curves, $y^2 = f(x)$, where q is an odd prime power and f is a square-free cubic polynomial. (Note that in this last situation, our terminology is to be distinguished from that of a primitive point introduced in [15].)

In this paper we generalize the notion of freeness, also considering the more general setting of finite cyclic groups. Such a concept not only recovers the former description for primitive elements but also the description of elements in \mathbb{F}_q^* with any prescribed multiplicative order. In particular, we obtain a character sum formula for the indicator function of elements in \mathbb{F}_q^* with prescribed multiplicative order, recovering a result from Carlitz [3].

Next, we extend the idea of freeness to the definition of (r, n) -free elements in a finite cyclic group (introduced in Section 3). This is an appropriate one for the discussion of the existence of primitive points on curves of the form $y^n = F(x)$ and more general questions. In this context, we then study pairs of polynomial expressions with special restrictions, obtaining a criterion for the existence of such pairs (Corollary 17). As an application of the latter (and a "sieving" version, Theorem 21), we obtain both asymptotic and concrete results on the existence of \mathbb{F}_q -primitive points of the elliptic curve $\mathcal{C} : y^2 = f(x)$. These are especially effective when studying elliptic curves of the form $\mathcal{C}_a : y^2 = x^3 - ax$, $a \in \mathbb{F}_q^*$. In particular, we shall establish the following theorem.

Theorem 1. *Let q be an odd prime power. Then there exist an \mathbb{F}_q -primitive point on the elliptic curve \mathcal{C}_1 if and only if $q \notin \{3, 7, 13, 17, 25, 49, 121\}$.*

Similarly, there exists an \mathbb{F}_q -primitive point on the elliptic curve \mathcal{C}_{-1} if and only if $q \notin \{5, 9, 17, 41, 49\}$.

More generally, after our theoretical work and calculations, we are enabled to make the following conjecture.

Conjecture 2. *Let q be an odd prime power.*

Suppose $q \notin S := \{3, 5, 7, 9, 13, 17, 25, 29, 31, 41, 49, 61, 73, 81, 121, 337\}$. Then, for any $a \in \mathbb{F}_q^$, there exists an \mathbb{F}_q -primitive point on \mathcal{C}_a .*

We know that Conjecture 2 holds for prime powers q outside the interval [141121, 167763671] (see Section 4). With reference to Conjecture 2, for any $q \in S$, the precise number of curves \mathcal{C}_a (values of $a \in \mathbb{F}_q^*$) which do *not* contain an \mathbb{F}_q -primitive point is tabulated in Table 1 below (at the end of Section 4).

2. Preparation

This section provides some background material that is further used. We start fixing some notation. For positive integers a and b , we set $a_{(b)} = \frac{a}{\gcd(a,b)}$. As usual, μ and ϕ stand for the Möbius and Euler totient function, respectively. Moreover, for a positive integer A , we denote its square-free part by A^* .

2.1. Characters

Recall that, for a finite group G , a *character* of G is a group homomorphism $\eta : G \rightarrow \mathbb{C}^*$. If G is cyclic of order n with generator g , any character of G is uniquely determined by the image of g . Moreover, since $g^n = 1$, such an image must be an n -th complex root of unity. From these observations, we readily obtain the following result.

Lemma 3. *If G is a cyclic group of order n with generator g , the set of characters of G is a multiplicative group of order n , generated by the character $\eta : g^k \mapsto e^{\frac{2\pi ik}{n}}$.*

The map $g \mapsto 1 \in \mathbb{C}$ is always a character of G , commonly called the *trivial* character of G . Given a character η of G , the least positive integer k such that $\eta(h)^k = 1$ for every $h \in G$ is the *order* of η , denoted by $\text{ord}(\eta)$.

Definition 4. *If \mathbb{F}_q is a finite field, a multiplicative character of \mathbb{F}_q is a character η of the multiplicative cyclic group $G = \mathbb{F}_q^*$. We extend η to $0 \in \mathbb{F}_q$ by setting $\eta(0) = 0$.*

The following well-known theorem provides a bound on character sums over finite fields with polynomial arguments.

Theorem 5 ([16, Theorem 5.41]). *Let η be a multiplicative character of \mathbb{F}_q of order $r > 1$ and $F \in \mathbb{F}_q[x]$ be a polynomial of positive degree such that F is not of the form $ag(x)^r$ for some $g \in \mathbb{F}_q[x]$ with degree at least 1 and $a \in \mathbb{F}_q$. Suppose that z is the number of distinct roots of F in its splitting field over \mathbb{F}_q . Then the following holds:*

$$\left| \sum_{c \in \mathbb{F}_q} \eta(F(c)) \right| \leq (z - 1)\sqrt{q}.$$

2.2. On n -primitive elements

If $n \mid q - 1$, then an element of \mathbb{F}_q of order $(q - 1)/n$ is called *n -primitive* and recently these elements have started attracting attention [7–9, 14]. This is mainly due to their theoretical interest and partially because, unlike primitive elements, we have efficient algorithms that locate such elements [2, 12, 18]. A challenging aspect of their study is their characterization. According to Carlitz [3], we have the following result.

Lemma 6. *If N is a divisor of $q - 1$, the characteristic function for the set of elements in \mathbb{F}_q with multiplicative order N can be expressed as*

$$\mathcal{O}_N(\omega) = \frac{N}{q - 1} \sum_{d \mid N} \frac{\mu(d)}{d} \sum_{\text{ord}(\eta) \mid \frac{d(q-1)}{N}} \eta(\omega). \tag{1}$$

By reordering of the terms in Eq. (1), a standard number-theoretic argument based on Möbius inversion yields the following alternative formula:

$$\mathcal{O}_N(\omega) = \frac{\phi(N)}{N} \sum_{t \mid q-1} \frac{\mu(t_n)}{\phi(t_n)} \sum_{\text{ord}(\eta)=t} \eta(\omega), \quad n = \frac{q-1}{N}. \tag{2}$$

Note that the above expression of the characteristic function for n -primitive elements is in fact a generalization of Vinogradov’s expression for the characteristic function for primitive elements [17, Theorem 6.3.90]. Further, note that a similar variation of Vinogradov’s formula, that characterizes n -primitive elements is proven in [5, Lemma 2.1]. We omit the proof of the latter since a more general result is proved in Section 3; see Remark 9 and Proposition 13 for more details.

We end this section with an identity related to the sum appearing in Lemma 6 that is further used.

Lemma 7. For positive integers r, n , we have that

$$T(r, n) := \sum_{t|r} \frac{|\mu(t_{(n)})|}{\phi(t_{(n)})} \cdot \phi(t) = \gcd(r, n) \cdot W(\gcd(r, r_{(n)})),$$

where $W(a)$ denotes the number of square-free divisors of a .

Proof. Observe that $f_n(r) := \frac{|\mu(r_{(n)})|}{\phi(r_{(n)})} \cdot \phi(r)$ and $g_n(r) := \gcd(r, n) \cdot W(\gcd(r, r_{(n)}))$ are multiplicative functions on r . In particular, the same holds for $T(r, n)$ and so it suffices to prove the equality $T(r, n) = g_n(r)$ in the case where r is a prime power. Write $r = s^a$ with s prime and $a \geq 1$, and write $n = s^b \cdot n_0$, where $b \geq 0$ and $\gcd(n_0, s) = 1$. We split the proof into two cases according as $a > b$ or $a \leq b$.

(i) If $a > b$, then

$$\begin{aligned} T(r, n) &= \sum_{i=0}^b \frac{|\mu(1)|}{\phi(1)} \phi(s^i) + \sum_{i=b+1}^a \frac{|\mu(s^{i-b})|}{\phi(s^{i-b})} \phi(s^i) \\ &= s^b + \frac{\phi(s^{b+1})}{\phi(s)} = 2s^b. \end{aligned}$$

Moreover, since $\gcd(r, n) = s^b$ and $\gcd(r, r_{(n)}) = s^{a-b}$ then $g_n(r) = 2s^b = T(r, n)$.

(ii) If $a \leq b$, we have that

$$T(r, n) = \sum_{i=0}^a \frac{|\mu(1)|}{\phi(1)} \cdot \phi(s^i) = s^a = r.$$

Moreover, in this case, $\gcd(r, n) = r$ and $r_{(n)} = 1$, implying $g_n(r) = r$. □

3. Introducing (r, n) -free elements

Motivated by the characterization of n -primitive elements in Eq. (2), we will generalize the well-known notion of r -free elements, considering also the more general setting of cyclic groups.

Definition 8. Let \mathcal{C}_Q be a multiplicative cyclic group of order Q . For a divisor n of Q and a divisor r of Q/n , an element $h \in \mathcal{C}_Q$ is (r, n) -free if the following hold:

- (i) $\text{ord}(h)|\frac{Q}{n}$, i.e., h is in the subgroup $\mathcal{C}_{Q/n}$;
- (ii) h is r -free in $\mathcal{C}_{Q/n}$, i.e., if $h = g^s$ with $g \in \mathcal{C}_{Q/n}$ and $s|r$, then $s = 1$.

In the following remark we present some straightforward facts on (r, n) -free elements.

Remark 9. For a divisor n of Q and a divisor r of Q/n , the following hold:

- (i) $(r, 1)$ -free elements in \mathcal{C}_Q are just the usual r -free elements;
- (ii) the $(Q/n, n)$ -free elements in \mathcal{C}_Q are exactly the elements of order Q/n .

The following is a generalization of [13, Proposition 5.2] and its proof is a mere adaptation of the original proof in our setting. We add it here, with the intention of making the relation between (r, n) -freeness and the multiplicative order of an element clear.

Lemma 10. Let n be a divisor of Q and r a divisor of Q/n . Then an element $h \in \mathcal{C}_Q$ is (r, n) -free if and only if $h = g^n$ for some $g \in \mathcal{C}_Q$ but h is not of the form g_0^{np} with $g_0 \in \mathcal{C}_Q$, for every prime divisor p of r . In particular, $h \in \mathcal{C}_Q$ is (r, n) -free if and only if $\gcd\left(rn, \frac{Q}{\text{ord}(h)}\right) = n$.

Proof. Since the set $\{g^n \mid g \in \mathcal{C}_Q\}$ describes the elements in \mathcal{C}_Q whose order divides Q/n , the first statement follows directly by the definition of (r, n) -free elements. For the second statement, pick h an arbitrary element of \mathcal{C}_Q . One can easily verify that there exists a generator g of \mathcal{C}_Q and a

divisor t of Q such that $h = g^t$. In this case, we have that h is (r, n) -free if and only if $t = n \cdot s$, where s divides Q/n and $\gcd(s, r) = 1$. We observe that the order of h equals $\frac{Q}{t} = \frac{Q}{ns}$ and so

$$\gcd\left(rn, \frac{Q}{\text{ord}(h)}\right) = n \cdot \gcd(r, s),$$

from where the result follows. □

The following is an obvious consequence of Lemma 10.

Lemma 11. *Let n be a divisor of Q and r a divisor of Q/n . An element of \mathcal{C}_Q is (r, n) -free if and only if it is (r^*, n) -free.*

It follows from Lemma 11 that, wherever it is convenient, we may assume that r is square-free.

Our next aim (see Proposition 13) is to prove that

$$\mathbb{1}_{r,n}(h) := \frac{\phi(r)}{rn} \sum_{t|rn} \frac{\mu(t(n))}{\phi(t(n))} \sum_{\text{ord}(\eta)=t} \eta(h), \quad h \in \mathcal{C}_Q,$$

is a character-sum expression of the characteristic function for (r, n) -free elements of \mathcal{C}_Q . Note that this expression of the characteristic function is in fact a generalization of Vinogradov’s expression of the characteristic function for r -free elements. In order to proceed with the proof, we will need the following lemma.

Lemma 12. *Let $t \mid Q$ and $h \in \mathcal{C}_Q$. Then*

$$S_0 := \frac{1}{t} \sum_{\text{ord}(\eta)|t} \eta(h) = 1,$$

if $h = g^t$ for some $g \in \mathcal{C}_Q$. Otherwise, $S_0 = 0$.

Proof. Immediate from the orthogonality relations; see Section 5.1 of [16]. □

Proposition 13. *Let n be a divisor of Q and r a divisor of Q/n . If $h \in \mathcal{C}_Q$, then*

$$\mathbb{1}_{r,n}(h) = \begin{cases} 1, & \text{if } h \text{ is } (r, n)\text{-free,} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let p_1, \dots, p_κ be the distinct prime divisors of r . From Lemma 10, we obtain that $h \in \mathcal{C}_Q$ is (r, n) -free if and only if $h = g^n$ for some $g \in \mathcal{C}_Q$, but h is not of the form $g_0^{np_i}$ with $g_0 \in \mathcal{C}_Q$, for every $1 \leq i \leq \kappa$. Further, if I_k stands for the characteristic function of the set $\{g^k : g \in \mathcal{C}_Q\}$, we have that $I_{np_i} I_n = I_{np_i}$. If $I_{r,n}$ is the characteristic function for (r, n) -free elements of \mathcal{C}_Q , it follows that, for every $h \in \mathcal{C}_Q$

$$\begin{aligned} I_{r,n}(h) &= I_n(h) \prod_{i=1}^{\kappa} (1 - I_{np_i}(h)) = \sum_{m|r} \mu(m) I_{nm}(h) \\ &= \frac{1}{n} \sum_{m|r} \frac{\mu(m)}{m} \sum_{\text{ord}(\eta)|mn} \eta(h) = \frac{1}{n} \sum_{m|r} \sum_{t|mn} \frac{\mu(m)}{m} \mathfrak{X}_t(h), \end{aligned} \tag{3}$$

where $\mathfrak{X}_t := \sum_{\text{ord}(\eta)=t} \eta(h)$ and in the second-to-last equality we use Lemma 12. In order to obtain a more convenient expression of the above, let $n = p_1^{n_1} \dots p_k^{n_k}$ and $r = p_1^{r_1} \dots p_k^{r_k}$ be the prime factorization of n and r , where p_1, \dots, p_k are distinct primes and $n_i, r_i \geq 0$. Further, observe, that for any arithmetic functions f and g , we have that

$$\begin{aligned} \sum_{m|r} \sum_{t|mn} f(m)g(t) &= \sum_{\substack{1 \leq i \leq k \\ 0 \leq m_i \leq r_i}} \sum_{\substack{1 \leq i \leq k \\ 0 \leq t_i \leq n_i + m_i}} f(p_1^{m_1} \dots p_k^{m_k}) g(p_1^{t_1} \dots p_k^{t_k}) \\ &= \sum_{\substack{1 \leq i \leq k \\ 0 \leq t_i \leq n_i + r_i}} \sum_{\substack{1 \leq i \leq k \\ \max(0, t_i - n_i) \leq m_i \leq r_i}} f(p_1^{m_1} \dots p_k^{m_k}) g(p_1^{t_1} \dots p_k^{t_k}) = \sum_{t|rn} \sum_{\substack{m|t \\ t/n}} f(t(n)m)g(t). \end{aligned}$$

We use the latter in Eq. (3) and obtain

$$I_{r,n}(h) = \frac{1}{n} \sum_{t|rn} \mathfrak{X}_t \sum_{m|(r/t_{(n)})} \frac{\mu(t_{(n)}m)}{t_{(n)}m}.$$

Note that the presence of the Möbius function of the inner sum of the above, implies that only the square-free divisors m of $r/t_{(n)}$ that are relatively prime with $t_{(n)}$ contribute to sum, i.e., we may rewrite the above as

$$I_{r,n}(h) = \frac{1}{n} \sum_{t|rn} \mathfrak{X}_t \sum_{m|r_{t,n}} \frac{\mu(t_{(n)}m)}{t_{(n)}m},$$

where $r_{t,n}$ is the product of the prime factors of $r/t_{(n)}$ that do not divide $t_{(n)}$. In particular, notice that $r_{t,n}t_{(n)}$ has exactly the same prime factors with r . Now, since $\mu(x)/x$ is multiplicative, we may rewrite the latter displayed equation as follows:

$$I_{r,n}(h) = \frac{1}{n} \sum_{t|rn} \mathfrak{X}_t \frac{\mu(t_{(n)})}{t_{(n)}} \sum_{m|r_{t,n}} \frac{\mu(m)}{m} = \frac{1}{n} \sum_{t|rn} \mathfrak{X}_t \frac{\mu(t_{(n)})}{t_{(n)}} \frac{\phi(r_{t,n})}{r_{t,n}},$$

where we used the well-known identity $\sum_{d|a} \frac{\mu(d)}{d} = \frac{\phi(a)}{a}$. Then we rewrite the above as follows

$$I_{r,n}(h) = \frac{1}{n} \sum_{t|rn} \mathfrak{X}_t \frac{\mu(t_{(n)})}{\phi(t_{(n)})} \frac{\phi(r_{t,n}t_{(n)})}{r_{t,n}t_{(n)}} = \frac{1}{n} \sum_{t|rn} \mathfrak{X}_t \frac{\mu(t_{(n)})}{\phi(t_{(n)})} \frac{\phi(r)}{r}.$$

The result follows after replacing \mathfrak{X}_t and accordingly rearranging the order in the above expression. \square

Remark 14. If $\mathcal{C}_Q = \mathbb{F}_q^*$, recall that we extended the multiplicative characters η of \mathbb{F}_q^* to $0 \in \mathbb{F}_q$ with $\eta(0) = 0$. Within this extension the equality $\mathbb{1}_{r,n}(0) = 0$ holds, as expected.

4. On (r, n) -freeness through polynomial values

For polynomials $f, F \in \mathbb{F}_q[x]$, we study the number of pairs $(f(y), F(y))$ such that $f(y)$ is (r, n) -free and $F(y)$ is (R, N) -free with $y \in \mathbb{F}_q$. It is only interesting to explore the case where $q-1$ has proper divisors, so we may assume that $q \geq 5$. Of course, this number of pairs can be zero if f and F have certain multiplicative dependence with respect to the numbers rn and RN . The following example gives an instance of the latter.

Example 15. Let q be an odd prime power, $n = N = 1$ and $r = R = 2$. Suppose that $f, F \in \mathbb{F}_q[x]$ are non constant polynomials such that $f \cdot F$ is of the form λg^2 with λ a nonsquare of \mathbb{F}_q . In particular, there is no $y \in \mathbb{F}_q$ such that $f(y)$ and $F(y)$ are $(2, 1)$ -free since this would imply that $f(y) \cdot F(y)$ is a nonzero square in \mathbb{F}_q .

We can avoid pathological situations like the one in Example 15 by imposing the following mild condition: $f, F \in \mathbb{F}_q[x]$ are non constant square-free polynomials such that f/F is not a constant. The next theorem shows that this condition asymptotically guarantees the existence of polynomial values $(f(y), F(y))$ with prescribed freeness.

Theorem 16. Fix $q \geq 5$ a prime power, let n, N be divisors of $q-1$ and let r and R be divisors of $\frac{q-1}{n}$ and $\frac{q-1}{N}$, respectively. Let $f, F \in \mathbb{F}_q[x]$ be non constant square-free polynomials such that the ratio f/F is not a constant and let $D+1 \geq 2$ be the number of distinct roots of $f \cdot F$ over its splitting field. Then the number $N_{f,F} = N_{f,F}(r, n, R, N)$ of elements $\theta \in \mathbb{F}_q$ such that $f(\theta)$ is (r, n) -free and $F(\theta)$ is (R, N) -free satisfies

$$N_{f,F} = \frac{\phi(r)\phi(R)}{rnRN} (q + H(r, n, R, N)),$$

with $|H(r, n, R, N)| \leq DnNW(r)W(R)q^{1/2}$.

Proof. By definition, we have that $N_{f,F} = \sum_{w \in \mathbb{F}_q} \mathbb{1}_{r,n}(f(w)) \cdot \mathbb{1}_{R,N}(F(w))$. From Proposition 13, for $\delta = \frac{\phi(r)\phi(R)}{rnRN}$ we have that

$$\begin{aligned} \frac{N_{f,F}}{\delta} &= \sum_{w \in \mathbb{F}_q} \left(\sum_{t|rn} \frac{\mu(t(n))}{\phi(t(n))} \sum_{\text{ord}(\eta)=t} \eta(f(w)) \right) \cdot \left(\sum_{T|RN} \frac{\mu(T(N))}{\phi(T(N))} \sum_{\text{ord}(\chi)=T} \chi(F(w)) \right) \\ &= \sum_{t|rn, T|RN} \frac{\mu(t(n)) \cdot \mu(T(N))}{\phi(t(n)) \cdot \phi(T(N))} \sum_{\substack{\text{ord}(\eta)=t \\ \text{ord}(\chi)=T}} G_{f,F}(\eta, \chi), \end{aligned}$$

where $G_{f,F}(\eta, \chi) = \sum_{w \in \mathbb{F}_q} \eta(f(w)) \cdot \chi(F(w))$. Fix $t|rn$ and $T|RN$ and let η, χ be multiplicative characters of \mathbb{F}_q with orders t and T , respectively. Then

$$\eta(w) \cdot \chi(f(w)) = \tilde{\eta}(f(w)^{cL/t} \cdot F(w)^{CL/T}),$$

for some multiplicative character $\tilde{\eta}$ of \mathbb{F}_q order $L = \text{lcm}(t, T)$ and some integers $1 \leq c \leq t$ and $1 \leq C \leq T$ with $\text{gcd}(c, t) = \text{gcd}(C, T) = 1$. Since f, F are square-free and the ratio f/F is not a constant, we easily verify that the polynomial $\mathcal{F}(x) = f(x)^{cL/t} \cdot F(x)^{CL/T}$ is of the form $\kappa \cdot g(x)^L$ if and only if $t = T = 1$. Therefore, from Theorem 5, we have that $|G_{f,F}(\eta, \chi)| \leq Dq^{1/2}$ whenever $(t, T) \neq (1, 1)$. For $t = T = 1$, we observe that η and χ are just the trivial multiplicative character over \mathbb{F}_q and so $G_{f,F}(\eta, \chi) = q - \epsilon$, where ϵ is the number of roots of $f \cdot F$ over \mathbb{F}_q . Since $\epsilon \leq D + 1$, applying estimates we obtain that

$$\left| \frac{N_{f,F}}{\delta} - q \right| \leq D + 1 + Dq^{1/2} \cdot M,$$

where

$$M = \sum_{\substack{t|rn, T|RN \\ (t,T) \neq (1,1)}} \frac{|\mu(t(n)) \cdot \mu(T(N))|}{\phi(t(n)) \cdot \phi(T(N))} \sum_{\substack{\text{ord}(\eta)=t \\ \text{ord}(\chi)=T}} 1 = T(rn, n) \cdot T(RN, N) - 1,$$

and $T(a, b)$ is as in Lemma 7. According to Lemma 7, we have the equality $T(ab, b) = b \cdot W(a)$ and so

$$\left| \frac{N_{f,F}}{\delta} - q \right| \leq D + 1 + Dq^{1/2}(nNW(r)W(R) - 1) < DnNW(r)W(R)q^{1/2},$$

where in the last inequality we used the fact that $D + 1 - Dq^{1/2} < 0$ if $D \geq 1$ and $q \geq 5$. The proof is complete. □

We immediately obtain the following corollary:

Corollary 17. *Let q, r, R, n, N, f, F and D be as in Theorem 16. If*

$$q^{1/2} > DnNW(r)W(R),$$

then $N_{f,F}(r, n, R, N) > 0$.

Remark 18. Following the proof of Theorem 16, one may check that the condition we impose on f, F can be replaced by a less restrictive one. In fact it suffices to assume that, for every $t | rn$ and $T | RN$ with $(t, T) \neq (1, 1)$, and integers $1 \leq c \leq t$ and $1 \leq C \leq T$ with $\text{gcd}(t, c) = \text{gcd}(T, C) = 1$, the polynomial $f^{cT} F^{Ct}$ is not the form $\kappa \cdot g^{tT}$ with $g \in \mathbb{F}_q[x]$ and $\kappa \in \mathbb{F}_q$. We observe that if both f and F have one simple linear factor (distinct from each other), then the latter always holds and such polynomials are not necessarily square-free.

4.1. *The prime sieve*

The aim of the section is to relax further the condition of Theorem 16. For this reason, we will employ the Cohen–Huczynska sieving technique, [6].

We describe the prime sieve in the context of the general cyclic group \mathcal{C}_Q as introduced in Definition 8.

Proposition 19 (Sieving inequality). *Let n, N be fixed divisors of Q and r, R divisors of $Q/n, Q/N$, respectively. Set*

$$N(r, R) := \#\{(x, y) \in \mathcal{C}_Q^2 : x \text{ is } (r, n)\text{-free and } y \text{ is } (R, N)\text{-free}\}.$$

For choices p_1, \dots, p_u of distinct prime divisors of r and l_1, \dots, l_v of distinct prime divisors of R , write $r^* = k_r p_1 \dots p_u$ and $R^* = k_R l_1 \dots l_v$, where k_r and k_R are also square-free. Then

$$N(r, R) \geq \sum_{i=1}^u N(k_r p_i, k_R) + \sum_{i=1}^v N(k_r, k_R l_i) - (u + v - 1)N(k_r, k_R). \tag{4}$$

Further, set $\delta = 1 - \sum_{i=1}^u 1/p_i - \sum_{i=1}^v 1/l_i$. Then (4) can be expressed in the form

$$N(r, R) \geq \delta N(k_r, k_R) + \sum_{i=1}^u \left(N(k_r p_i, k_R) - \left(1 - \frac{1}{p_i}\right) N(k_r, k_R) \right) + \sum_{i=1}^v \left(N(k_r, k_R l_i) - \left(1 - \frac{1}{l_i}\right) N(k_r, k_R) \right). \tag{5}$$

Proof. Each of the N -terms on the right side of (4) can only score (count one) for pairs $(x, y) \in \mathcal{C}_Q^2$ for which x is (k_r, n) -free and y is (k_R, N) -free. In addition, to be scored, for instance, by $N(k_r p_i, k_R)$, (x, y) has to be (p_i, n) -free. We conclude that the aggregate score counted on the right side by members of the set in the definition of $N(r, R)$ is $u + v - (u + v - 1) = 1$. On the other hand, if, for instance (x, y) is (k_r, n) -free but not (p_i, n) -free and y is (k_R, N) -free, it will not score in $N(k_r p_i)$ and so its aggregate score will be non-positive. \square

We apply the sieving inequality with $\mathcal{C}_Q = \mathbb{F}_q^*$ to produce a sieving version of Theorem 16. From Lemma 11 we could assume r, R are square-free (though some of their prime factors may also be divisors of n, N , respectively).

Theorem 20. *Assume the notation and conditions of Theorem 16. Further, let p_1, \dots, p_u be distinct primes dividing r and l_1, \dots, l_v be distinct primes dividing R . Write $r^* = k_r P_r$, where, for each $i = 1, \dots, u$, $p_i | P_r$ but $p_i \nmid k_r$ and similarly $R^* = k_R P_R$. Set $\delta = 1 - \sum_{i=1}^u 1/p_i - \sum_{i=1}^v 1/l_i$ and suppose that $\delta > 0$. Then*

$$N_{f,F} \geq \delta \cdot \frac{\phi(k_r)\phi(k_R)}{k_r n k_R N} \left(q - DnNW(k_r)W(k_R) \left(\frac{u + v - 1}{\delta} + 2 \right) q^{1/2} \right). \tag{6}$$

Proof. Assume that r, R are square-free. Given n, F, n, N , let $N(r, R)$ stand for $N_{f,F}(r, n, R, N)$. Further, set $\theta = \frac{\phi(k_r)\phi(k_R)}{k_r n k_R N}$. From Theorem 16,

$$N(k_r, k_R) \geq \theta(q - DnNW(k_r)W(k_R)q^{1/2}). \tag{7}$$

Next, we bound the differences shown in (5). Towards this, for $1 \leq i \leq u$, set $\Delta_{p_i} = N(k_r p_i, k_R) - \left(1 - \frac{1}{p_i}\right)N(k_r, k_R)$. Then, with G standing for $G_{f,F}$ in the proof of Theorem 16, we have that

$$\Delta_{p_i} = \theta \left(1 - \frac{1}{p_i} \right) \left(\sum_{\substack{t|k_r n \\ T|k_R N}} \frac{\mu((tp_i)_{(n)})\mu(T_{(N)})}{\phi((tp_i)_{(n)})\phi(T_{(N)})} \sum_{\substack{\text{ord}(\eta)=tp_i \\ \text{ord}(\chi)=T}} G(\eta, \chi) \right).$$

Since each character η is nontrivial, we have the bound

$$\begin{aligned} |\Delta_{p_i}| &\leq \theta \left(1 - \frac{1}{p_i}\right) DnN(W(k_r p_i) - W(k_r))W(k_R)q^{1/2} \\ &= \theta \left(1 - \frac{1}{p_i}\right) DnNW(k_r)W(k_R)q^{1/2}. \end{aligned} \tag{8}$$

Similarly, if $\Delta_{l_i} = N(k_r, k_R l_i) - \left(1 - \frac{1}{l_i}\right)N(k_r, k_R)$ for each $1 \leq i \leq v$, we have

$$|\Delta_{l_i}| \leq \theta \left(1 - \frac{1}{l_i}\right) DnNW(k_r)W(k_R)q^{1/2}. \tag{9}$$

Inserting the bounds (7), (8) and (9) in (5), we obtain (6). □

The next theorem is an immediate consequence of Theorem 20 when $r = (q - 1)/n$ and $R = (q - 1)/N$.

Theorem 21. *Let f, F, n, N be as in Theorem 16. Write $((q - 1)/n)^* = k_n p_1 \dots p_u$, where p_1, \dots, p_u are distinct primes and similarly $((q - 1)/N)^* = k_N l_1 \dots l_v$. Set $\delta = 1 - \sum_{i=1}^u 1/p_i - \sum_{i=1}^v 1/l_i$ and assume $\delta > 0$. Then, using the same notation as in Theorem 16, there exists some $(x, X) \in \mathbb{F}_q^2$, such that $f(x)$ is n -primitive and $F(X)$ is N -primitive, provided that*

$$q^{1/2} > DnNW(k_n)W(k_N) \left(\frac{u + v - 1}{\delta} + 2\right).$$

We will refer to the primes $p_1, \dots, p_u, l_1, \dots, l_v$ appearing above as the *sieving primes*.

5. Special points on elliptic curves

In this section, we apply our methods to study special points on elliptic curves. More specifically, given an elliptic curve $\mathcal{C} : y^2 = f(x)$ defined over \mathbb{F}_q , with $f \in \mathbb{F}_q[x]$ being a square-free cubic, we study the existence of \mathbb{F}_q -primitive points on \mathcal{C} .

Equivalently, we require a primitive x , such that $f(x)$ is 2-primitive, i.e., our goal is to prove that

$$N_f := N_{x, f(x)}(q - 1, 1, (q - 1)/2, 2)$$

is positive. Notice that $x, f(x)$ are square-free polynomials and the ratio $x/f(x)$ is not a constant. Thus Corollary 17 yields that a sufficient condition for $N_f > 0$ is

$$q^{1/2} \geq 3 \cdot 1 \cdot 2 \cdot W(q - 1)W((q - 1)/2) = 6W(q - 1)W\left(\frac{q - 1}{2}\right). \tag{10}$$

Our next aim is to explore the numerical aspects of (10). Naturally, an estimate of the number $W(a)$ is necessary.

Lemma 22. *Let t, a be positive integers and let p_1, \dots, p_j be the distinct prime divisors of t such that $p_i \leq 2^a$. Then $W(t) \leq c_{t,a} t^{1/a}$, where*

$$c_{t,a} = \frac{2^j}{(p_1 \dots p_j)^{1/a}}.$$

In particular, for $d_t := c_{t,6}$ we have the bound $d_t < 37.47$.

Proof. The statement is an immediate generalization of Lemma 3.3 of [6] and can be proved using multiplicativity. The bound for d_t can be easily computed. □

Here we have singled out the value $a = 6$ for convenience in what follows. Now, we move on to numerical computations. We note that for this purpose we relied on the SAGEMATH mathematics software system.

Notice if $(q - 1)/2$ is even, then $W((q - 1)/2) = W(q - 1)$, whilst if $(q - 1)/2$ is odd, then $W((q - 1)/2) = W(q - 1)/2$. It follows that a combination of (10) and Lemma 22 yields two conditions, depending on the parity of $(q - 1)/2$. Namely,

$$q^{1/6} \geq \frac{6 \cdot 37.47^2}{2^{1/3}} \quad \text{and} \quad q^{1/6} \geq 3 \cdot 37.47^2,$$

if $q \equiv 1 \pmod{4}$ and $q \equiv 3 \pmod{4}$ respectively. We check the stronger of the two conditions, i.e., the former, and verify that it is satisfied for $q \geq 8.94 \cdot 10^{22}$.

Then, we observe that if $q - 1$ is divided by 18 or more prime numbers, then $q > 8.94 \cdot 10^{22}$, which implies that the case $W(q - 1) \geq 2^{18}$ is settled.

Our next step will settle the cases $2^{13} \leq W(q - 1) \leq 2^{17}$. Let $t_{\min} \leq t_{\max}$ be two positive integers. Further, let p_i stand for the i -th prime number, that is, for example, $p_1 = 2$ and $p_3 = 5$. Now, assume that for some odd prime power q , we have that $2^{t_{\min}} \leq W(q - 1) \leq 2^{t_{\max}}$. It follows that $q - 1$ is divided by at least t_{\min} and by at most t_{\max} prime numbers, which implies that $q > p_1 \dots p_{t_{\min}}$. Moreover, we may choose as sieving primes the largest $n < t_{\min}$ prime divisors of $q - 1$ and, more precisely, take each of them twice, in such a way that $1 - \sum_{i=1}^n \frac{2}{p_i} > 0$. This way we ensure that the number δ (see Theorem 20) satisfies $\delta > 1 - \sum_{i=1}^n \frac{2}{p_i} > 0$. It then follows from Theorem 20 that $N_f > 0$ if

$$\sqrt{p_1 \dots p_{t_{\min}}} > 6 \cdot 4^{t_{\max} - n} \left(\frac{2n - 1}{1 - \sum_{i=1}^n \frac{2}{p_i}} + 2 \right).$$

We computationally verify that the above holds for the pairs $(t_{\max}, t_{\min}) = (17, 15)$ and $(14, 13)$, that is, the case $W(q - 1) \geq 2^{13}$ is settled, thus, the case $q > 6 \cdot 4^{12} = 100663296$ is settled.

We proceed to reduce the number of possible exceptions as much as possible. First, we try the condition of Corollary 17 within the range $3 < q \leq 100663296$ with each quantity explicitly computed, instead of using generic estimates. It turns out that within this range there are 5798811 odd prime powers, with 797566 of them failing to satisfy this condition and $q = 100663291$ being the largest among them.

Finally, we attempt to use the prime sieve (see Theorem 20) on these persistent prime powers, again with all the quantities explicitly computed. Our computations reveal that there exists a suitable set of sieving primes for almost 97% of these numbers. More precisely, this method was unsuccessful for 24826 out of the 797566 prime numbers checked, with $q = 82192111$ being the largest among them. To sum up, we have proved the following.

Theorem 23. *Let $q > 82192111$ be an odd prime power. Further, let $f(x) \in \mathbb{F}_q[x]$ be a square-free polynomial of degree 3, then the elliptic curve $\mathcal{C} : y^2 = f(x)$ contains \mathbb{F}_q -primitive points.*

We believe that identifying the genuine exceptions to the above theorem is an interesting research question.

Problem 24. *Identify all the odd prime powers $3 \leq q \leq 82192111$ and the corresponding square-free cubic polynomials $f \in \mathbb{F}_q[x]$ such that the elliptic curve $\mathcal{C} : y^2 = f(x)$ does not contain \mathbb{F}_q -primitive points.*

5.1. *The elliptic curve $\mathcal{C} : y^2 = x^3 - ax$*

Finally, we study the special case of the elliptic curve $\mathcal{C} : y^2 = f_a(x)$, where $f_a(x) = x^3 - ax$, $a \in \mathbb{F}_q^*$. Notice that since $f_a(0) = 0$, the polynomial $x \cdot f_a(x)$ has 3 distinct roots, so, in this special case, the condition of (10) may be replaced by the significantly weaker condition

$$q^{1/2} \geq 2 \cdot 1 \cdot 2 \cdot W(q-1)W((q-1)/2) = 4W(q-1)W\left(\frac{q-1}{2}\right).$$

We repeat the same steps that lead us to Theorem 23. Having a weaker condition, we obtain that if $q > 16763671$, then the elliptic curve $\mathcal{C} : y^2 = f_a(x)$ over \mathbb{F}_q , always has some \mathbb{F}_q -primitive point, while in the range $3 \leq q \leq 16763671$ there are exactly 11041 odd prime powers that may not possess this property. Additionally, observe that, so far, the same can be said for any square-free cubic $g \in \mathbb{F}_q[x]$ with $g(0) = 0$.

We return to our special case and attempt an exhaustive search. In particular, we attempt to identify explicitly a point on the curve $\mathcal{C} : y^2 = f_a(x)$, for all the 11041 persistent prime powers q and for all $a \in \mathbb{F}_q^*$. Due to hardware restrictions and the vast number of elliptic curves that have to be checked, this computation was not completed. In particular, we checked the first 4624 prime powers, which leaves us with 6417 prime powers, all within the range $141121 \leq q \leq 16763671$ unchecked. These partial results suggest that all of these elliptic curves have some \mathbb{F}_q -primitive point, with the only exceptions being $q = 3, 5, 7, 9, 13, 17, 25, 29, 31, 41, 49, 61, 73, 81, 121$ and 337, while the number of curves over the corresponding finite fields with no such points is given in Table 1.

Table 1. Number of curves $\mathcal{C} : y^2 = x^3 - ax$, $a \in \mathbb{F}_q^*$, over \mathbb{F}_q , without \mathbb{F}_q -primitive points, when $q \notin [141121, 16763671]$.

q	3	5	7	9	13	17	25	29	31	41	49	61	73	81	121	337
# curves	1	2	3	5	5	6	12	1	1	8	8	10	12	10	16	2

These findings enable us to state Conjecture 2. We believe that attacking Conjecture 2 in its full generality would be nontrivial but not hopeless: it would require a combination of advanced theoretical techniques with exhaustive computational methods.

Finally, we repeat the same procedure for two special curves within the aforementioned family of curves, namely the curves $\mathcal{C} : y^2 = x^3 - x$ and $\mathcal{C} : y^2 = x^3 + x$. In particular, after spending just a few seconds of computer time, we explicitly check all the possibly exceptional curves and, as a result, we obtain Theorem 1.

References

- [1] A. R. Booker, S. D. Cohen, N. Sutherland, T. Trudgian, “Primitive values of quadratic polynomials in a finite field”, *Math. Comput.* **88** (2019), no. 318, p. 1903-1912.
- [2] F. E. Brochero Martínez, L. Reis, “Elements of high order in Artin–Schreier extensions of finite fields \mathbb{F}_q ”, *Finite Fields Appl.* **41** (2016), p. 24-33.
- [3] L. Carlitz, “Primitive roots in a finite field”, *Trans. Am. Math. Soc.* **73** (1952), p. 373-382.
- [4] C. Carvalho, J. P. Guardieiro, V. G. L. Neumann, G. Tizziotti, “On special pairs of primitive elements over a finite field”, *Finite Fields Appl.* **73** (2021), article no. 101839 (10 pages).
- [5] S. D. Cohen, “The orders of related elements of a finite field”, *Ramanujan J.* **7** (2003), no. 1-3, p. 169-183.
- [6] S. D. Cohen, S. Huczynska, “The primitive normal basis theorem — without a computer”, *J. Lond. Math. Soc.* **67** (2003), no. 1, p. 41-56.
- [7] S. D. Cohen, G. Kapetanakis, “The trace of 2-primitive elements of finite fields”, *Acta Arith.* **192** (2020), no. 4, p. 397-419.

- [8] ———, “The translate and line properties for 2-primitive elements in quadratic extensions”, *Int. J. Number Theory* **16** (2020), no. 9, p. 2027-2040.
- [9] ———, “Finite field extensions with the line or translate property for r -primitive elements”, *J. Aust. Math. Soc.* **111** (2021), no. 3, p. 311-319.
- [10] S. D. Cohen, T. Oliveira e Silva, N. Sutherland, T. Trudgian, “Linear combinations of primitive elements of a finite field”, *Finite Fields Appl.* **51** (2018), p. 388-406.
- [11] S. D. Cohen, T. Oliveira e Silva, T. Trudgian, “A proof of the conjecture of Cohen and Mullen on sums of primitive roots”, *Math. Comput.* **84** (2015), no. 296, p. 2979-2986.
- [12] S. Gao, “Elements of provable high orders in finite fields”, *Proc. Am. Math. Soc.* **127** (1999), no. 6, p. 1615-1623.
- [13] S. Huczynska, G. L. Mullen, D. Panario, D. Thomson, “Existence and properties of k -normal elements over finite fields”, *Finite Fields Appl.* **24** (2013), p. 170-183.
- [14] G. Kapetanakis, L. Reis, “Variations of the primitive normal basis theorem”, *Des. Codes Cryptography* **87** (2018), no. 7, p. 1459-1480.
- [15] S. Lang, H. Trotter, “Primitive points on elliptic curves”, *Bull. Am. Math. Soc.* **83** (1977), p. 289-292.
- [16] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, 1996.
- [17] G. L. Mullen, D. Panario (eds.), *Handbook of Finite Fields*, Discrete Mathematics and its Applications, CRC Press, 2013.
- [18] R. Popovych, “Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ ”, *Finite Fields Appl.* **19** (2013), p. 96-92.