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

Giorgos Kapetanakis
Joint work with Stephen D. Cohen and Lucas Reis

University of the Aegean Graduate Program Workshop
Karlovasi (Samos) – November 2021

University of Thessaly

Motivation

Primitive elements

Let $\mathbf{F}_q$ be the finite field with q elements. The multiplicative group $\mathbf{F}_q^*$ is cyclic and a generator of this group is called primitive.

Primitive elements are widely studied, mainly because of their applications in practical situations such as the discrete logarithm problem.

Vinogradov obtained a character sum formula for the characteristic function of such elements. The latter can be subsumed into a general concept of freeness, which is related to the multiplicative structure of the elements of $\mathbf{F}_q^*$.

Freeness

For $d \mid q-1$, some $x \in \mathbf{F}_q$ is d-free if $x \neq \beta^s$ for every $1 < s \mid d$.

- Primitivity $\equiv$ $(q-1)$-freeness.
- $\alpha \in \mathbf{F}_q$ is d-free $\iff$ $\gcd\left(d, \frac{q-1}{\mathrm{ord}(\alpha)}\right) = 1$.
- Vinogradov's formula can be adjusted to express the characteristic function for d-free elements for every $d \mid q-1$.

Previous works

Many authors have explored the existence of primitive elements with additional properties. The main tools are Vinogradov's formula and bounds on multiplicative character sums such as Weil's bound.

A common theme is studying pairs $(\alpha, F(\alpha))$ of primitive elements, where $F \in \mathbf{F}_q(x)$. This is equivalent to looking at $\mathbf{F}_q$-rational points on the curve $\mathcal{C} : y = F(x)$ whose coordinates are primitive, i.e., $\mathbf{F}_q$-primitive points.

- Cohen, Oliveira e Silva, Trudgian, 2015: F general linear polynomial.
- Cohen, Oliveira e Silva, Sutherland, Trudgian, 2018, $F(x) = x \pm 1/x$.
- Booker, Cohen, Sutherland, Trudgian 2019, F general quadratic polynomial.
- Carvalho, Guardieiro, Neumann, Tizziotti 2021, $F = f_1/f_2$.

Our contribution

We consider the existence of $\mathbf{F}_q$-primitive points on curves of the form $y^n = F(x)$. An important example is that of elliptic curves, $y^2 = f(x)$, where q is odd and f is a square-free cubic polynomial.

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 $\mathbf{F}_q^*$ with any prescribed multiplicative order.

Next, we extend the idea of freeness to the definition of (r, n)-free elements in a finite cyclic group.

Preliminaries

Characters

For a finite group G, a character of G is a homomorphism $\eta : G \to \mathbb{C}^*$. The map $g \mapsto 1 \in \mathbb{C}$ is the trivial character of G. The characters of $\mathbf{F}_q^*$ are the multiplicative characters of $\mathbf{F}_q$.

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 $\eta : g^k \mapsto e^{\frac{2\pi \cdot i \cdot k}{n}}$.

Theorem

Let η be a multiplicative character of $\mathbf{F}_q$ of order $r > 1$ and $F \in \mathbf{F}_q[x]$ not of the form $ag(x)^r$. Let z be the number of distinct roots of F in its splitting field over $\mathbf{F}_q$. Then

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

n-primitive elements

An element of $\mathbf{F}_q$ of order $(q-1)/n$ is called n-primitive. Recently these elements have started attracting attention due to their theoretical interest and because we have efficient algorithms that locate such elements. A challenging aspect of their study is their characterization.

Lemma (Carlitz, 1952)

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

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

n-primitive elements

By reordering of the terms in the latter, we obtain

$$\mathcal{O}_N(\omega) = \frac{\varphi(N)}{N} \sum_{t \mid q-1} \frac{\mu(t_{(n)})}{\varphi(t_{(n)})} \sum_{\mathrm{ord}(\eta)=t} \eta(w), \quad n = \frac{q-1}{N},$$

where $a_{(b)} = \frac{a}{\gcd(a,b)}$ and the inner sum is over all the multiplicative characters of order t.

Note that the above expression of the characteristic function for n-primitive elements is in fact a generalization of Vinogradov's formula.

Introducing (r, n)-free elements

The definition

Definition

Let Q be a positive integer and let $\mathcal{C}_Q$ be a cyclic group of order Q, written mutiplicatively. For $n \mid Q$ and $r \mid Q/n$, an element $h \in \mathcal{C}_Q$ is (r, n)-free if

(i) $\mathrm{ord}(h) | \frac{Q}{n}$, i.e., h is in the subgroup $\mathcal{C}_{Q/n}$ and

(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 $s = 1$.

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

Basic properties

Lemma

Let $n \mid Q$ and $r \mid Q/n$. Then $h \in \mathcal{C}_Q$ is (r, n)-free iff $h = g^n$ 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 iff $\gcd\left(rn, \frac{Q}{\mathrm{ord}(h)}\right) = n$.

The following is an obvious consequence of the above.

Lemma

Let n be a divisor of Q and r a divisor of Q/n. If r^* is the square-free part of r, then an element of $\mathcal{C}_Q$ is (r, n)-free if and only if it is (r^*, n)-free.

It follows that we may assume that r is square-free.

Characterizing (r, n)-free elements

Next, using the orthogonality relations, we prove that

$$\mathcal{I}_{r,n}(h) := \frac{\varphi(r)}{rn} \sum_{t \mid rn} \frac{\mu(t_{(n)})}{\varphi(t_{(n)})} \sum_{\mathrm{ord}(\eta)=t} \eta(h), \ h \in \mathcal{C}_Q.$$

is a character-sum expression of the characteristic function for (r, n)-free elements of $\mathcal{C}_Q$. Note that this is a generalization of Vinogradov's formula for r-free elements.

Proposition

Let $n \mid Q$ and $r \mid Q/n$. If $h \in \mathcal{C}_Q$, then

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

(r, n)-FREENESS THROUGH POLYNOMIAL VALUES

Main condition

For $f, F \in \mathbf{F}_q[x]$, 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 $y \in \mathbf{F}_q$.

1. It is only interesting to explore the case where $q - 1$ has proper divisors, that is, $q \geq 5$.
2. We avoid pathological situations by imposing the following mild condition: $f, F \in \mathbf{F}_q[x]$ are nonconstant squarefree polynomials such that f/F is not a constant.

Main condition

Theorem

Fix $q \geq 5$, let n, N be divisors of $q-1$ and let $r \mid \frac{q-1}{n}$ and $R \mid \frac{q-1}{N}$. Let $f, F \in \mathbf{F}_q[x]$ be nonconstant squarefree such that f/F is non-constant and let $D+1 \geq 2$ be the number of distinct roots of fF over its splitting field. Then the number $N_{f,F} = N_{f,F}(r,n,R,N)$ of elements $\theta \in \mathbf{F}_q$ such that $f(\theta)$ is (r,n)-free and $F(\theta)$ is (R,N)-free satisfies

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

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

Main condition

Corollary

Let q, r, R, n, N, f, F and D be as in the last theorem. If

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

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

The prime sieve

Next, we relax the above condition using the Cohen-Huczynska (2003) sieving technique.

Proposition (Sieving inequality)

Let $n, N \mid Q$ and $r \mid Q/n, R \mid Q/N$. 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 $p_1, \ldots, p_u$ distinct prime divisors of r and $l_1, \ldots l_v$ distinct prime divisors of R, write $r^* = k_r p_1 \cdots p_u$ and $R^* = k_R l_1 \cdots l_v$, where k_r and k_R are also square-free. Then

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

The prime sieve

Theorem

Assume the notation and conditions as above. Let $p_1, \ldots, p_u$ *be distinct primes dividing* r *and* $l_1, \ldots, l_v$ *be distinct primes dividing* R*. Write* $r^* = k_r P_r$*, where, for each* $i = 1, \ldots u$*,* $p_i | P_r$ *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*

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

The prime sieve

As a consequence, we get:

Theorem

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

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

We will refer to the primes $p_1, \ldots, p_u, l_1, \ldots, l_v$ as the sieving primes.

Special points on elliptic curves

An application on elliptic curves

Next, 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 $\mathbf{F}_q$, with $f \in \mathbf{F}_q[x]$ being a square-free cubic, we study the existence of $\mathbf{F}_q$-primitive points on $\mathcal{C}$.

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

$$N_f := N_{x,f(x)}(q-1, 1, (q-1)/2, 2) > 0$$

Notice that $x, f(x)$ are squarefree polynomials and the ratio $x/f(x)$ is not a constant. Thus, an able condition for $N_f > 0$ is

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

With the help of the SageMath software, we show the following generic result.

Theorem

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

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 $f_a(x) = x^3 - ax$, $a \in \mathbf{F}_q^*$.

We repeat the same steps and we obtain that if $q > 16763671$, then the elliptic curve $\mathcal{C} : y^2 = f_a(x)$ has some $\mathbf{F}_q$-primitive point. In the range $3 \leq q \leq 16763671$ there are 11041 odd prime powers that may not possess this property.

The above, along with experimental data, enable us to conjecture the following.

Conjecture

Let q be an odd prime power let $a \in \mathbf{F}_q^*$. If $f_a(x) = x^3 - ax$, then the elliptic curve $\mathcal{C} : y^2 = f(x)$ has some $\mathbf{F}_q$-primitive point, unless $q = 3, 5, 7, 9, 13, 17, 25, 29, 31, 41, 49, 61, 73, 81, 121$ and 337.

The elliptic curve $\mathcal{C} : y^2 = x^3 \pm x$

We repeat the same procedure for two special 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 the following complete results.

Theorem

Let $q \neq 3, 7, 13, 17, 25, 49$ and 121 be an odd prime power. There exist $\mathbf{F}_q$-primitive points on the elliptic curve $\mathcal{C} : y^2 = x^3 - x$.

Theorem

Let $q \neq 5, 9, 17, 41$ and 49 be an odd prime power. There exist $\mathbf{F}_q$-primitive points on the elliptic curve $\mathcal{C} : y^2 = x^3 + x$.

References

References

A. R. Booker, S. D. Cohen, N. Sutherland and T. Trudgian.
Primitive values of a quadratic polynomial in a finite field.
Math. Comp. 88 (2019) 1903–1912.

L. Carlitz.
Primitive roots in finite fields.
Trans. Amer. Math. Soc. 73 (1952) 373–382.

C. Carvalho, J. P. Guardieiro, V. G. L. Neumann and G. Tizziotti.
On special pairs of primitive elements over a finite field.
Finite Fields Appl. 73 (2021) 101839, 10pp.

S. D. Cohen.
The orders of related elements of a finite field.
Ramanujan J. 7 (2003) 169–183.

S. D. Cohen and S. Huczynska.
The primitive normal basis theorem – without a computer.
J. London Math. Soc. 67 (2003) 41–56.

S. D. Cohen and G. Kapetanakis.
Finite field extensions with the line or translate property for r-primitive elements.
J. Aust. Math. Soc.. to appear (2020) 7pp.

S. D. Cohen and G. Kapetanakis.
The trace of 2-primitive elements of finite fields.
Acta Arith. 192 (2020) 397–419.

References

S. D. Cohen and G. Kapetanakis.
The translate and line properties for 2-primitive elements in quadratic extensions.
Int. J. Number Theory 16 (2020) 2027–2040.

S. D. Cohen, T. Oliveira e Silva, N. Sutherland and T. Trudgian.
Linear combinations of primitive elements of a finite field.
Finite Fields Appl. 51 (2018) 388–406.

S. D. Cohen, T. Oliveira e Silva and T. Trudgian.
A proof of the conjecture of Cohen and Mullen on sums of primitive roots.
Math. Comp. 84 (2015) 2979–2986.

S. Gao.
Elements of provable high orders in finite fields.
Proc. Amer. Math. Soc. 127 (1999) 1615–1623.

S. Huczynska, G. L. Mullen, D. Panario and D. Thomson.
Existence and properties of k-normal elements over finite fields'
Finite Fields Appl. 24 (2013) 170–183.

G. Kapetanakis and L. Reis.
Variations of the primitive normal basis theorem.
Des. Codes Cryptogr. 87 (2019) 1459–1480.

S. Lang and H. Trotter.
Primitive points on elliptic curves.
Bull. Amer. Math. Soc. 83 (1977) 289–292.

References

R. Lidl and H. Niederreiter.
Finite Fields.
Cambridge University Press, Cambridge, 1996.

F. E. B. Martínez and L. Reis.
Elements of high order in Artin-Schreier extensions of finite fields $\mathbb{F}_q$.
Finite Fields Appl. 41 (2016) 24–33.

G. L. Mullen and D. Panario.
Handbook of Finite Fields.
CRC Press, Boca Raton, 2013.

R. Popovych.
Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$.
Finite Fields Appl. 19 (2013) 96–92.

This work is available at:

arXiv:2108.07373 [math.NT]

Thank You!