Additive Patterns in Multiplicative Subgroups

Noga Alon * Jean Bourgain †

Abstract

The study of sum and product problems in finite fields motivates the investigation of additive structures in multiplicative subgroups of such fields. A simple known fact is that any multiplicative subgroup of size at least $q^{3/4}$ in the finite field F_q must contain an additive relation $x + y = z$. Our main result is that there are infinitely many examples of sum-free multiplicative subgroups of size $\Omega(p^{1/3})$ in prime fields F_p. More complicated additive relations are studied as well. One representative result is the fact that the elements of any multiplicative subgroup H of size at least $q^{3/4+o(1)}$ of F_q can be arranged in a cyclic permutation so that the sum of any pair of consecutive elements in the permutation belongs to H. The proofs combine combinatorial techniques based on the spectral properties of Cayley sum-graphs with tools from algebraic and analytic number theory.

1 Introduction

Some of the most interesting developments in the recent extensive work in Additive Combinatorics deal with the interplay between the two operations sum and product in finite fields. The basic result here, motivated by a similar phenomenon that holds for real numbers, as discovered by Erdős and Szemerédi in [11], is the intriguing fact that not-too-large subsets of prime finite fields that are nearly closed under multiplication, are far from being closed under sum. This has first been proved in [7] and has led to applications in several areas including incidence geometry, analytic number theory, group theory, theoretical computer science and more. In the present paper we study an extremal version of this phenomenon, studying additive relations in subsets of finite fields that are completely closed under multiplication, namely, multiplicative subgroups. It is easy and well known (see, e.g., [29]) that if a subgroup of F_q^* is of size at least $q^{3/4}$, then it must contain relations of the form $x + y = z$, (equivalently, it must contain relations of the form $a + b = 1$). Our main result here is that there are infinitely many examples showing that this is not necessarily the case for multiplicative subgroups of size $\Theta(p^{1/3})$ in prime fields F_p.

*Sackler School of Mathematics and Blavatnik School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel and Institute for Advanced Study, Princeton, New Jersey, 08540, USA. Email: nogaa@tau.ac.il. Research supported in part by an ERC Advanced grant, by a USA-Israeli BSF grant, by an ISF grant, by the Israeli I-Core program and by the Simonyi Fund.

†Institute for Advanced Study, Princeton, New Jersey, 08540, USA. Email: bourgain@ias.edu.

Theorem 1.1 *There is an absolute constant $c > 0$ so that there are infinitely many examples of a prime p and a multiplicative subgroup A in the finite field F_p such that $|A| \geq cp^{1/3}$ and there are no $x, y \in A$ so that $x + y \in A$.*

We also consider more complicated additive patterns in multiplicative subgroups. A representative example is the following.

Theorem 1.2 *There exists an absolute positive constant c so that for any prime power q and for any multiplicative subgroup A of the finite field F_q of size*

$$|A| = d \geq c\frac{q^{3/4}(\log q)^{1/2}(\log\log\log q)^{1/2}}{\log\log q}$$

there is a numbering $a_0, a_1, \ldots, a_{d-1}$ of the elements of A so that $a_i + a_{i+1} \in A$ for all i, where the indices are reduced modulo d.

In particular this implies that for any sufficiently large prime p there is a cyclic permutation of all $k = (p-1)/2$ quadratic residues modulo p so that the sum of any two adjacent elements in the permutation is also a quadratic residue modulo p. A recent conjecture of Sun [30] asserts that this is the case for all $p > 13$. This is indeed correct, as shown in Theorem 2.1 below.

It is worth noting that for proper prime powers q there are known examples of much bigger multiplicative subgroups of finite fields F_q which contain no relation of the form $x + y = 1$. These are called cyclic caps in projective spaces, and have been studied extensively, see, for example, [31], [33], [13] and the references therein. In particular, by modifying the construction in [33] we can prove the following.

Proposition 1.3 *For every integer $k \geq 0$ if $q = 2^{4^{k+1}}$ and*

$$d = (2^{2\cdot 4^k} + 1)(2^{2\cdot 4^{k-1}} + 1)\cdots(2^2 + 1)\ (= \Omega(q^{2/3})\ )$$

then the multiplicative subgroup of order d in F_q contains no solution to $x + y = 1$.

A proof appears in the appendix. The case of prime fields treated in Theorem 1.1 above seems more difficult, and we are not aware of any earlier results for prime fields.

The problem of ensuring a single relation of the form $x+y = z$ with $x, y, z \in A$ seems more natural than that of ensuring a cyclic permutation of all elements with all sums of consecutive pairs in the group. The following known result can be proved by standard techniques.

Proposition 1.4 (see, e.g., [29]) *Let q be a prime power and let A be a multiplicative subgroup of the finite field F_q of size $|A| = d \geq q^{1/2}$. Then, for any two subsets $B, C \subset F_q$ satisfying $|B||C| \geq \frac{q^3}{d^2}$ there are $x \in B$ and $y \in C$ so that $x + y \in A$. In particular, if $|A| \geq q^{3/4}$ there are $x, y, z \in A$ so that $x + y = z$.*

We prefer to formulate some of our proofs here using eigenvalues of Cayley sum-graphs. This is essentially equivalent to the standard harmonic analysis approach, but is useful for establishing more involved additive relations, by combining the basic spectral approach with graph theoretic arguments. This can provide more complicated (though less natural) additive structures in multiplicative groups. Here are two examples.

Proposition 1.5 *For any multiplicative subgroup A of the finite field F_q that satisfies $|A| \geq q^{1-1/(2r-2)}$ and for any subset B of the field satisfying $|B| \geq 2\frac{q^{(2r-1)/2}}{|A|^{r-1}}$ there are r distinct elements $a_1, a_2, \ldots, a_r \in B$ so that for all $1 \leq i < j \leq r$, $a_i + a_j \in A$. In particular, if $|A| > 2^{1/r} q^{1-1/(2r)}$ there are such $a_1, a_2 \ldots, a_r$ in A.*

Proposition 1.6 *If q is a sufficiently large prime power and $d > q^{11/12}(\log q)^{1/5}$ is divisible by 3 and divides $q-1$, then the elements of the multiplicative subgroup A of size d in the finite field F_q can be partitioned into $d/3$ disjoint triples so that all sums of pairs of elements in the same triple belong to A.*

The rest of this paper is organized as follows. In Section 2 we prove that large multiplicative subgroups must contain various additive structures. Section 3 contains the proof of Theorem 1.1 and several stronger variants. Section 4 contains some concluding remarks, extensions and open problems, and the proof of Proposition 1.3 appears in the appendix.

2 Finding additive structures

2.1 Quadratic residues

In this subsection we prove the following statement, conjectured in [30].

Theorem 2.1 *For any prime $p > 13$ there is a numbering $a_0, a_1, \ldots, a_{k-1}$ of the $k = \frac{p-1}{2}$ quadratic residues of F_p so that $a_i + a_{i+1}$ is also quadratic residue modulo p for all $0 \leq i < k-1$, and so is $a_{k-1} + a_0$.*

The proof is rather simple, but as we wish to get the result for all primes $p > 13$ it involves some computation that can be avoided if we only wish to prove the result for sufficiently large primes. We need the following result of Jackson.

Lemma 2.2 ([21]) *For each integer $r \geq 2$, any 2-connected r-regular graph with $m \leq 3r$ vertices is Hamiltonian.*

We also need the following simple lemma.

Lemma 2.3 *Let $p \geq 5$ be a prime, let Q denote the set of the $(p-1)/2$ quadratic residues modulo p, and let $\chi : F_p \mapsto \{0, -1, 1\}$ denote the quadratic character defined by $\chi(0) = 0$, $\chi(x) = 1$ if x is a quadratic residue and $\chi(x) = -1$ if x is a quadratic nonresidue. Then:*
(i) For each $x \in Q$ there are exactly

$$r = \frac{p - 6 - \chi(-1) - 2\chi(2)}{4}$$

$y \in Q - \{x\}$ so that $x + y \in Q$.
(ii) For any two subsets $X, Y \in Z_p$ satisfying $|X|(|Y| - 1)^2 > |Y|(p - |Y| + 1)$ there are $x \in X$ and $y \in Y$ so that $x + y \in Q$.

Proof. Clearly

$$\sum_{x \in F_p} \chi(x) = 0. \tag{1}$$

Similarly, for every two distinct $y, y' \in F_p$,

$$\sum_{x \in F_p} \chi(x+y)\chi(x+y') = \sum_{x \in F_p, x \neq -y} \chi(\frac{x+y'}{x+y}) = \sum_{x \in F_p, x \neq -y} \chi(1 + \frac{y'-y}{x+y}) = -1, \tag{2}$$

where the last equality holds, since $y' - y \neq 0$, and hence as x ranges over all elements of $F_p - \{-y\}$ the quantity $1 + \frac{y'-y}{x+y}$ ranges over all elements in $F_p - \{1\}$.

(i) Given $x \in Q$, note that the quantity

$$\frac{(\chi(y)+1)(\chi(x+y)+1)}{4}$$

is 1 iff both y and the sum $x + y$ lie in Q, and is zero iff either y or $x + y$ is a quadratic non-residue. Therefore the number d of $y \in Q - \{x\}$ so that $x + y \in Q$ satisfies

$$d = \sum_{y \in F_p} \frac{(\chi(y)+1)(\chi(x+y)+1)}{4} - \frac{(\chi(0)+1)(\chi(x)+1)}{4} - \frac{(\chi(-x)+1)(\chi(0)+1)}{4} - \frac{(\chi(x)+1)(\chi(2x)+1)}{4}$$

$$= \sum_{y \in F_p} \frac{(\chi(y)+1)(\chi(x+y)+1)}{4} - \frac{5 + \chi(-1) + 2\chi(2)}{4}.$$

By (1), (2) we conclude that

$$\sum_{y \in F_p} \frac{(\chi(y)+1)(\chi(x+y)+1)}{4} = \frac{p-1}{4}$$

implying the assertion of (i).

(ii) Suppose there are no $x \in X$ and $y \in Y$ so that $x + y \in Q$. Then for each $x \in X$ and each $y \in Y$ either $x + y = 0$ or $\chi(x + y) = -1$. This means that for each $x \in X$ $(\sum_{y \in Y} \chi(x + y))^2 \geq (|Y| - 1)^2$. Therefore, using (2),

$$|X|(|Y| - 1)^2 \leq \sum_{x \in X} (\sum_{y \in Y} \chi(x + y))^2 \leq \sum_{x \in F_p} (\sum_{y \in Y} \chi(x + y))^2$$

$$\leq \sum_{x \in F_p} (|Y| + \sum_{y \neq y' \in Y} \chi(x + y)\chi(x + y')) = p|Y| - |Y|(|Y| - 1) = |Y|(p - |Y| + 1),$$

as needed. □

Proof of Theorem 2.1 Let $p > 13$ be a prime, and let Q denote the set of all $k = (p - 1)/2$ quadratic residues modulo p. Let G be the graph whose vertices are the elements of Q, where $x, y \in Q$ are connected iff $x + y \in Q$. By Lemma 2.3, G is r-regular, where $r = \frac{p-6-\chi(-1)-2\chi(2)}{4} \geq \frac{p-9}{4}$. If $p \geq 29$ then $k = (p - 1)/2 \leq 3(p - 9)/4 \leq 3r$, that is, in this case the graph G satisfies the degree condition in Lemma 2.2.

We next show that if $p \geq 29$ then the graph G is 2-connected. Assume this is false, and there is a vertex v of G so that $G - v$ is disconnected. Let X be the smallest connected component of $G - v$. Since the degree of every vertex in G is r, each vertex u of X has at least $r - 1$ neighbors in X, and hence $|X| \geq r \geq \frac{p-9}{4}$. Put $Y = Q - (X \cup \{v\})$ and note that there are no edges between X and Y. Thus, by Lemma 2.3, part (ii) $|X|(|Y| - 1)^2 \leq |Y|(p - |Y| + 1)$. Since $|X| + |Y| + 1 = |Q| = \frac{p-1}{2}$ it is not difficult to check that the maximum possible value of the left hand side in the last inequality for $|X| \geq \frac{p-9}{4}$ and $p \geq 29$ is obtained when $|X| = \frac{p-9}{4}$ and $|Y| = \frac{p+3}{4}$. As the right hand side is clearly at most $\frac{(p+1)^2}{4}$ we conclude that

$$\frac{p - 9}{4}(\frac{p - 1}{4})^2 \leq \frac{(p + 1)^2}{4},$$

that is $(p - 9)(p - 1)^2 \leq 16(p + 1)^2$. However, it is easy to check that this is incorrect for all $p \geq 29$. By Lemma 2.2 it follows that the graph G is Hamiltonian for all primes $p \geq 29$. It remains to check the cases $p \in \{17, 19, 23\}$. For $p = 19$, by quadratic reciprocity (or directly), the degree of regularity of the graph G is $r = \frac{19-6-\chi(-1)-2\chi(2)}{4} = 4$ and its number of vertices is $|Q| = \frac{19-1}{2} = 9 \leq 3 \cdot 4$ hence it satisfies the degree condition in Lemma 2.2. If there is a vertex v of G so that $G - v$ is disconnected, then any connected component of $G - v$ must be of size at least 4, hence there are two components, each of size 4. But this is impossible, as it implies that all vertices of $G - v$ have at most 3 neighbors in their components, and hence all must be connected to v, contradiction, as G is 4-regular.

For $p = 17$ the graph G is 2-regular, and is in fact a cycle: $(1, 8, 13, 2, 16, 9, 4, 15)$ (note that all sums of adjacent elements in this cycle are quadratic residues). For $p = 23$ the set of quadratic residues is $Q = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$, the corresponding graph is 4-regular and it is not difficult to find in it a Hamilton cycle: $(1, 2, 16, 8, 4, 9, 3, 6, 18, 13, 12)$.

This completes the proof. □

2.2 Smaller subgroups

In this subsection we prove Theorem 1.2 as well as Propositions 1.5 and 1.6. We also present a simple proof of the known Proposition 1.4 using our graph theoretic terminology. This proof is essentially equivalent to the known standard ones, but the description given here is useful as the same basic approach yields more sophisticated results when combined with additional graph theoretic arguments. We need several known results about the spectral properties of Cayley sum-graphs of Abelian groups and about the relation between the spectrum of a graph and its structure.

A graph G is called an (n, d, λ)-graph if it is d-regular, has n vertices, and the absolute value of each nontrivial eigenvalue of its adjacency matrix is at most λ. This notion was introduced by the first author in the 80s, motivated by the observation that such graphs in which λ is much smaller than d exhibit strong pseudo-random properties. See [24] for a survey about the properties of such graphs (and other pseudo-random graphs).

The following simple lemma is proved in [2].

Lemma 2.4 *Let G be an (n, d, λ)-graph and let $U \subset V$ be a set of vertices of G. Then the number of edges $e(U)$ in the induced subgraph of G on U satisfies*

$$|e(U) - \frac{|U|^2 d}{2n}| \leq \lambda |U|(1 - \frac{|U|}{n}) \ (\ < \lambda |U|).$$

A similar argument gives the following, sometimes called the expander mixing lemma (c.f., e.g., [5], Corollary 9.2.5).

Lemma 2.5 *Let G be an (n, d, λ)-graph and let U and W be two subsets of vertices of G. Then the number of edges $e(U, W)$ with an end point in U and another in W (where edges with both endpoints in $U \cap W$ are counted twice) satisfies*

$$|e(U, W) - \frac{|U||W|d}{n}| < \lambda \sqrt{|U||W|}.$$

A crucial ingredient in the proof of Theorem 1.2 is the following result of Krivelevich and Sudakov.

Lemma 2.6 ([23]) *Let G be an (n, d, λ) graph and assume n is sufficiently large. If*

$$\lambda < (\log \log n)^2 d/(1000 \log n \log \log \log n)$$

then G is Hamiltonian.

For an abelian group B and a subset $T \subset B$, the *Cayley sum graph* $G = G(B, T)$ of B with respect to T is the graph whose set of vertices is B, in which yz is an edge for each $y, z \in B$ satisfying $y + z \in T$. It is easy and well known (c.f., e.g., [3]) that the eigenvalues of G can be expressed in terms of T and the characters of B. Indeed, the eigenvalues of the square of the adjacency matrix of G are all the expressions $|\sum_{s \in T} \chi(s)|^2$, where χ is a character of B, and the characters are the corresponding

eigenvectors. Therefore each nontrivial eigenvalue of the graph $G = G(B, T)$ is, in absolute value, $|\sum_{s \in T} \chi(s)|$ for some nontrivial character χ of B.

For our purpose here we consider Cayley sum-graphs $G = G(F_q, A)$, where F_q is the finite field with q elements and A is a multiplicative subgroup of F_q. In this case, the nontrivial character sums providing the eigenvalues of G can be bounded using Weil's Theorem [32] (the special case of a multiplicative subgroup is simpler than the general case and can be proved directly by expressing the sums in terms of Gauss sums). This gives the following.

Lemma 2.7 *Let A be a multiplicative subgroup in the finite field F_q and let $G = G(F_q, A)$ be the Cayley sum-graph of F_q with respect to A. Thus $x, y \in F_q$ are adjacent iff $x + y \in A$. Then G is a $(q, |A|, q^{1/2})$-graph, that is, it has q vertices, is regular of degree $|A|$ and every nontrivial eigenvalue of it has absolute value at most $q^{1/2}$.*

Note that the graph $G = G(F_q, A)$ may have loops, indeed if $2x \in A$ then (x, x) is a loop at the vertex x. There can be at most one loop in each vertex, and such a loop contributes 1 to the degree of the vertex.

The proofs of Theorem 1.2 and Propositions 1.4, 1.5 and 1.6 are now simple consequences of the above lemmas. The details follow.

Proof of Theorem 1.2 Let $G = G(F_q, A)$ denote the Cayley sum-graph of F_p with respect to A. By Lemma 2.7 this is a $(q, d, q^{1/2})$-graph. Let H be the induced subgraph of G on the set of vertices A. It is clear that H is regular, since if $x + y = z$ for some $x, y, z \in A, x \neq y$ and $g \in A$, then $gx + gy = gz$. The mapping $f(y) = gy$ is a bijection between the neighbors of x in H and the neighbors of gx in H. Let r denote the degree of regularity of H. By Lemma 2.4, and since by assumption $q^{3/2} = o(d)$, it follows that $r = (1 + o(1))\frac{d^2}{q}$. By interlacing of eigenvalues it follows that H is a $(d, r, q^{1/2})$-graph. For an appropriate choice of the constant c in Theorem 1.2 this graph thus satisfies the assumption of Lemma 2.6 and it is therefore Hamiltonian, providing the assertion of Theorem 1.2. □

Proof of Propositions 1.4, 1.5 and 1.6 As before, consider the Cayley sum-graph $G = G(F_q, A)$, which is a $(q, d, q^{1/2})$-graph, by Lemma 2.7. By Lemma 2.5 the number of edges in this graph connecting a vertex of B and a vertex of C is bigger than

$$\frac{|B||C|d}{q} - q^{1/2}\sqrt{|B||C|} \geq 0,$$

where the last inequality follows from the assumption that $|B||C| \geq \frac{q^3}{d^2}$. Thus there is an edge connecting some $x \in B$ and $y \in C$, implying the assertion of Proposition 1.4.

The proof of Proposition 1.5 follows from the same reasoning, by applying the fact proved in [4] (Lemma 2.1) that asserts that any set of at least

$$\frac{(\lambda + 1)n}{d}(1 + \frac{n}{d} + \ldots + (\frac{n}{d})^{r-2})$$

vertices in an (n, d, λ)-graph contains a complete graph on r vertices. Thus, in our case any set B of size at least

$$\frac{(q^{1/2}+1)q}{|A|}(1+\frac{q}{|A|}+\ldots(\frac{q}{|A|})^{r-2})$$

contains r elements with all sums of pairs in A, as claimed in Proposition 1.5.

The proof of Proposition 1.6 proceeds as in the proof of Theorem 1.2. As in that proof, the induced subgraph of $G(F_q, A)$ on A is a $(d, r, q^{1/2})$-graph, with $r = (1+o(1))\frac{d^2}{q}$. The result now follows from the main result of [25] that asserts that any (n, d, λ)-graph in which the number of vertices is divisible by 3, n is sufficiently large and

$$\lambda = o(\frac{d^3}{n^2 \log n})$$

contains $n/3$ pairwise vertex disjoint triangles. Since by assumption here

$$q^{1/2} = o(\frac{r^3}{q^2 \log q}),$$

the desired result follows. □

3 Sum-free subgroups

In this section we prove Theorem 1.1 and several more precise statements, as follows.

Theorem 3.1 *For any positive integer d which is not divisible by 6 there is a set $E(d)$ of at most $\frac{d^2}{\log d}$ primes so that for any prime $p \equiv 1 (\mathrm{mod}\ d)$ which does not belong to $E(d)$, there are no x, y, z in the subgroup H of cardinality d of Z_p^* that satisfy $x + y = z$ (equivalently, there are no $x', y' \in H$ with $x' + y' = 1$.) Every member of $E(d)$ is smaller than 3^d and in addition the following holds.*

(i) For most values of d that are not divisible by 6 the smallest prime $p \equiv 1 (\mathrm{mod}\ d)$, $p \notin E(d)$ satisfies $p = O(d^3)$. The same assertion holds for most primes d. Here "most d" means that the proportion of values of d in the range $[D, 2D]$ for which the above assertion fails is $o(D)$.

(ii) For every integer d which is not divisible by 6 the smallest prime $p \equiv 1 (\mathrm{mod}\ d)$, $p \notin E(d)$ satisfies $p = O(d^5)$.

(iii) There is a fixed $\epsilon > 0$ so that for every integer d which is not divisible by 6 and does not have a prime factor that exceeds d^ϵ, the smallest prime $p \equiv 1 (\mathrm{mod}\ d)$, $p \notin E(d)$ satisfies $p = O(d^3)$.

The assumption that d is not divisible by 6 in the above theorem is essential, as shown by the following simple observation.

Claim 3.2 *If d is divisible by 6 then any multiplicative subgroup H of size d in any finite field F_q contains a solution to $x + y = 1$.*

Proof. Since the multiplicative group of a finite field is cyclic, so is its subgroup H, and it thus contains an element z of order 6. Therefore $z^3 = -1$ and hence

$$z + z^5 - 1 = z + z^5 + z^3 = z(1 + z^2 + z^4) = \frac{z(z^6 - 1)}{z^2 - 1} = 0,$$

showing that $x = z$ and $y = z^5$ satisfy $x + y = 1$. □

We proceed with the proof of the theorem. Let d be an integer not divisible by 6. Put $\xi = e^{2\pi i/d}$, let $K = Q[\xi]$ be the cyclotomic field obtained by adjoining ξ to the rationals Q, and let $O = O_K$ denote the ring of integers in K. Hence the degree of the extension $[K : Q] = \phi(d)$ is the Euler ϕ function.

For $0 < j < d$ define $z_j = \xi^j - 1$ and for $0 < j_1 \leq j_2 < d$ define $z_{j_1,j_2} = \xi^{j_1} + \xi^{j_2} - 1$. Each z_j is clearly nonzero. Note that since d is not divisible by 6, each number z_{j_1,j_2} is also nonzero. Indeed, any solution of the equation $x + y = 1$ with $x = a + ib$, $y = a' + ib'$ of absolute value 1 must satisfy $b' = -b$ and hence $|a| = |a'|$ $(= \sqrt{1 - b^2})$. Since $a + a' = 1$ this shows that the only solution is

$$\{x, y\} = \{\frac{1 + i\sqrt{3}}{2}, \frac{1 - i\sqrt{3}}{2}\} = \{e^{2\pi i/6}, e^{-2\pi i/6}\},$$

and these numbers are not powers of ξ.

Define

$$A = A(\xi) = \prod_{0<j<d} z_j \prod_{0<j_1,j_2<d} z_{j_1,j_2}. \tag{3}$$

Note that A is invariant under Galois conjugation, since $A(\xi) = A(\xi^r)$ for $(r, d) = 1$. Therefore A is a nonzero integer and is divisible by each of the norms $N_j = \mathrm{Norm}_{K/Q}(z_j)$ and $N_{j_1,j_2} = \mathrm{Norm}_{K/Q}(z_{j_1,j_2})$ (recall that the norm of each element of K is the product of its $\phi(d)$ conjugates).

Clearly $|A| < 2^d 3^{d^2}$ and therefore it has at most $d^2/\log d$ prime factors. (We note, in passing, that the absolute value of the first product $\prod_{0<j<d} z_j$ is exactly d, and it can in fact be ignored, but this is not crucial for our purpose here). Moreover, every prime dividing A must divide one of the norms N_j or N_{j_1,j_2}, and each of those is smaller than 3^d. Let $E(d)$ denote the set of all prime divisors of A which are 1 modulo d, then $|E(d)| \leq \frac{d^2}{\log d}$ (with room to spare) and each member of $E(d)$ is smaller than 3^d.

Let p be a prime that does not divide A and satisfies $p \equiv 1 (\mathrm{mod}\ d)$. Then $x^d - 1 \in F_p[x]$ factors into linear factors (c.f., e.g., [26], Theorem 2.47) and therefore the ideal (p) in O_K factors in prime ideals of degree 1. Fix such an ideal P above (p), then the quotient O_K/P is isomorphic to the finite field F_p. Let $\pi : O_K \mapsto O_K/P$ be the residue map. Since by construction p does not divide any of the norms N_j and N_{j_1,j_2} it follows that P is coprime with (z_j) and (z_{j_1,j_2}) and hence

$$\pi(\xi)^j - 1 \neq 0 \ \text{ for } \ 0 < j < d$$

and

$$\pi(\xi)^{j_1} + \pi(\xi)^{j_2} - 1 \neq 0 \ \text{ for } \ 0 < j_1 \leq j_2 < d.$$

Thus $\pi(\xi)$ generates in $(O_K/P)^*$ (which is isomorphic to F_p^*) a group of size d without any relation $x+y=1$ (or $x+y=z$).

It is worth noting that an equivalent more explicit description of the above procedure, avoiding the discussion of prime ideals, is to simply define $\pi(\xi)=g$, where g is an element of order d in Z_p^*, extend this mapping to a ring homomorphism from $Z_p[\xi]=O_K/(p)$ to Z_p, and observe that none of the quantities $\xi^{j_1}+\xi^{j_2}-1$ belongs to its kernel, as by multiplying it by all its conjugates we get an integer which is not divisible by p and hence is not mapped to 0 in Z_p.

It remains to check how small we can take p, that is, to prove the claims in parts (i),(ii) and (iii) of the theorem. Recall the condition that p does not divide A and $p \equiv 1 (\mathrm{mod}\ d)$. This is basically Linnik's problem, with the (minor) difference that we also need to produce sufficiently many primes in the desired progression to ensure $p \notin E(d)$, that is, we need some $\frac{d^2}{\log d}$ primes.

Any treatment of Linnik's problem on the least prime in a progression results from an asymptotic estimate for the function $\psi(x;d,a)$ which provides a weighted count of the primes (and prime powers) in the progression $a(\mathrm{mod}\ d)$ that do not exceed x. Recall that

$$\psi(x;q,a)=\sum_{n\le x, n\equiv a(\mathrm{\ mod\ }\ q)} \Lambda(n),$$

where $\Lambda(n)$ is $\log p$ if $n=p^k$ is a prime power, and $\Lambda(n)=0$ otherwise. As the contribution from the proper powers of primes is negligible, and in view of the asympototics $\psi(x;d,1)=(1+o(1))\frac{x}{\phi(d)}$ for x sufficiently large, the best estimate for the smallest possible p we can hope for in our problem is $p=O(d^3)$. This can be achieved on average in d by invoking the Bombieri-Vinogradov Theorem (see, e.g., [20], page 420).

Theorem 3.3 (Bombieri-Vinogradov)

$$\sum_{q\le Q} max_{a,(a,q)=1}|\psi(x;q,a)-\frac{x}{\phi(q)}| < c_A \frac{x}{(\log x)^A} \tag{4}$$

for any $A>0$, with $Q=x^{1/2}(\log x)^{-B}$ where $B=B(A)$.

Fix a range $D\le d\le 2D$, and apply (4) with $x=cD^3$. It follows that for most d in this range (and also for most primes d in this range)

$$|\psi(x;d,1)-\frac{x}{\phi(d)}| < c\frac{x}{D(\log D)^2} \tag{5}$$

and in particular

$$\psi(x;d,1)=(1+o(1))\frac{x}{\phi(d)} > c'd^2. \tag{6}$$

By the preceding discussion, this supplies the assertion of (i).

The proof of part (ii), which deals with individual values of d, is similar. Returning to Linnik's problem, Heath-Brown (see [16], sections 13-15) proved that

$$\sum_{p\equiv 1(\bmod\ d), d^{5.5-0.6}<p<d^{5.5}} \frac{\log p}{p} \geq \Omega(\frac{\log d}{\phi(d)}). \tag{7}$$

Hence

$$\psi(d^{5.5}; d, 1) \geq \Omega(d^{4.5-0.6}) > cd^2.$$

The estimate 5.5 has been improved to 5.2 in [34] and to 5 in [35]. This implies the assertion of (ii).

It remains to prove (iii) which asserts that if d has only small prime factors, one may recover the estimate $p = O(d^3)$. We proceed with a sketch of this proof.

As noted in section 1 of [16], one has

$$\psi(x; d, a) = (1 + o(1))\frac{x}{\phi(d)} \tag{8}$$

for $x > d^{12/5+\epsilon}$, $(a, d) = 1$, provided

(*) All Dirichlet functions $L(s, \chi)$ to the modulus d are zero-free in the region

$$1 \geq \text{Re } s > 1 - \frac{C(\epsilon)}{\log[d(2 + |\text{Im } s|)]}. \tag{9}$$

The exponent 12/5 here is imposed by the density estimate

$$\sum_{\chi(\bmod\ d)} N(\sigma, T, \chi) < C_\epsilon (dT)^{(\frac{12}{5}+\epsilon)(1-\sigma)} \tag{10}$$

where

$$N(\sigma, T, \chi) = |\{\rho = \alpha + i\beta : L(\rho, \chi) = 0, \sigma < \alpha < 1, |\beta| < T\}|$$

resulting from the work of Jutila [22] and Huxley [18].

In case d is composed of a fixed set of prime factors (9) was proven by Gallagher [12] and Iwaniec [19], in the much larger range

$$\text{Re } s > 1 - \frac{c}{[\log(d(2 + |\text{Im } s|))]^\theta}$$

for some constant $\theta < 1$.

More generally, it results from the work of Graham and Ringrose [14] and Iwaniec [19] that (8) holds provided d has prime factors bounded by $d^{\delta(\epsilon)}$ (see Chang [8] for a unified treatment), except for a possible Siegel zero. Recall that this is a real zero β_0 of an L-function $L(s, \psi)$ (mod d), for a real character ψ, which is close to 1, say

$$\beta_0 \geq 1 - \frac{1}{3 \log d}.$$

If such Siegel zero β_0 exists, it is unique and one obtains, assuming $x > d^{12/5+\epsilon}$

$$\psi(x;d,1) = \frac{x}{\phi(d)}(1 - \frac{x^{\beta_0-1}}{\beta_0} + O(x^{-\epsilon C(\epsilon)/\log d})) \geq \frac{x}{\phi(d)}(\frac{1}{\eta} + O(x^{-\epsilon C(\epsilon)/\log d})) \tag{11}$$

where we denoted

$$\frac{1}{\eta} = (1-\beta_0)\log d. \tag{12}$$

Hence, if η is at most $O(1)$, (11) is conclusive by taking $C(\epsilon)$ large enough. On the other hand, if η is large, we invoke Heath-Brown's result [15], Theorem 2, according to which

$$|\{p \leq x; p \equiv 1 (\mathrm{mod}\ d)\}| > \frac{x}{\phi(d)\log x}(\frac{4}{3}\log\frac{5}{4} - \delta) \tag{13}$$

provided $d^{2+\delta} \leq x < d^{400}$ and $\eta > \eta(\delta)$. In particular, it follows from the discussion above that

$$\psi(x;d,1) \geq \frac{x}{\phi(d)\log x} \quad \text{for} \quad x > d^{12/5+\epsilon} \tag{14}$$

if d has no prime factor exceeding $d^{\delta(\epsilon)}$. This implies (iii) and completes the proof of Theorem 3.1. □

4 Concluding remarks and open problems

We have shown that there are infinitely many examples of sum-free multiplicative subgroups of size $\Theta(p^{1/3})$ in prime fields F_p, whereas it is known that any subgroup of F_q^* of size at least $q^{3/4}$ cannot be sum-free, that is, it must contain relations of the form $x + y = z$.

It will be interesting to close the gap between the upper and lower bounds. A natural heuristic argument suggests that the right threshold may be $d = \Theta(q^{1/2})$, since if a subgroup H of size d behaves randomly, the expected number of solutions of the equation $x + y = 1$ with $x, y \in H$ should be

$$\Theta(q \cdot (\frac{d}{q})^2) = \Theta(\frac{d^2}{q})$$

which is 1 for $d = \Theta(q^{1/2})$. However, the known constructions mentioned in the introduction, which provide bigger examples of sum-free multiplicative subgroups for non-prime fields, indicate that there may be similar examples in the prime case as well. The threshold size for ensuring the existence of a Hamilton cycle in a subgroup, as in Theorem 1.2, may well be close to that ensuring a single relation $x + y = 1$, as random graphs with degrees logarithmic in the number of vertices are already hamiltonian with high probability.

It is worth noting that if we assume square root cancellation in the Fourier coefficients of multiplicative subgroups, as conjectured in [28], we would get that subgroups of size $cq^{2/3}$ of F_q^* must contain a solution to $x + y = 1$, as these coefficients are exactly the nontrivial eigenvalues of the corresponding Cayley sum-graphs. In view of the existing examples in the non-prime case it may be

that the tight threshold for ensuring a solution to the equation $x+y=z$ in a multiplicative subgroup of a finite field F_q (for prime or non-prime q) is $q^{2/3+o(1)}$ and not $q^{1/2+o(1)}$. Another comment relevant here is that in the proof of Theorem 3.1 we used the fact that the number $A = A(\xi)$ defined in (3) is smaller than $2^d 3^{d^2}$ to conclude that the number of primes $p \equiv 1 (\mathrm{mod}\ d)$ that divide it does not exceed $d^2/\log d$. One may suspect that in fact only a fraction of roughly $1/\phi(d)$ of the primes dividing A are $1(\mathrm{mod}\ d)$. We have not been able to prove that this is the case, but if true this would improve the $\Omega(p^{1/3})$ lower bound in Theorem 1.1 to $p^{1/2-o(1)}$.

The proofs in Section 2 can be easily modified to provide additional additive structures in large multiplicative subgroups A of finite fields. Indeed, one can either apply the results known about (n,d,λ)-graphs to the Cayley sum-graph of F_q with respect to the elements of A, or apply those to its induced subgraph on A. Thus, for example, by the known result that any (n,d,λ)-graph with $d-\lambda \geq 2$ and an even number of vertices contains perfect matching (see [24] Theorem 4.3), we conclude that the elements of any multiplicative subgroup A of even order $d \geq cq^{3/4}$ of F_q can be partitioned into disjoint pairs so that the sums of elements in each pair lie in A. Similarly, it is known (see [24], Proposition 4.12), that for any fixed k, any (n,d,λ)-graph that satisfies $\lambda^{2k-1} \leq \epsilon(k)d^{2k}/n$ contains a cycle of length $2k+1$. This implies that any multiplicative subgroup A of size at least $C(k)q^{6k+1/8k}$ contains $2k+1$ elements $a_0, a_1, \ldots, a_{2k}$ so that all sums $a_i + a_{i+1}$, where indices are reduced modulo $2k+1$, lie in A. Another statement follows from the known result (see [24], Theorem 4.10) that for any fixed graph $H=(U,E)$ with maximum degree Δ, any set of $m > c(H)\lambda(\frac{n}{d})^{\Delta}$ vertices in an (n,d,λ)-graph contains a copy of H. This implies that any multiplicative subgroup A of size at least $c(H)q^{1-\frac{1}{2\Delta+2}}$ in F_q contains a collection $\{a_u : u \in U\}$ of $|U|$-elements so that all sums $a_u + a_v$ for $uv \in E$ lie in A. Finally, in a very recent paper of Allen et. al. [1] the authors show that any (n,d,λ)-graph G with $\lambda = o(d^{5/2}/n^{3/2})$ contains a square of a Hamilton cycle, and if $\lambda = o(d^{3k/2}n^{1-3k/2})$ then G contains a $k-th$ power of a Hamilton cycle. This implies an extension and a strenthening of the statement in Proposition 1.6.

The simple proof of Proposition 1.4, combined with more sophisticated character-sum estimates, yields some nontrivial results for much smaller multiplicative subgroups as well. Indeed, the second author proved in [6] that if H is a multiplicative subgroup of size p^{δ} of the prime field F_p, then for every $0 < a < p$

$$|\sum_{h \in H} e^{2\pi i a h/p}| \leq p^{-e^{-C/\delta}}|H|,$$

for some constant $C > 1$. This implies that for any such H, if B and C are two subsets of F_p and

$$|B||C| \geq p^{-2e^{-C/\delta}}p^2$$

then there are $b \in B$ and $c \in C$ with $b + c \in H$.

An old result of Chvatál and Erdős [9] asserts that any graph whose connectivity is at least as large as its independence number is hamiltonian. This can also be combined with the character-sum estimates

and the basic approach in Section 2 to prove the following statement (in which we make no attempt to optimize the absolute constants):

Let A be a mutiplicative subgroup of size $|A| = d$ in a the finite field F_q, and let B be an arbitrary subset of m elements of F_q so that $|(b-A) \cap B| > \frac{md}{2q}$ for all $b \in B$, and $m > \frac{6q^{5/2}}{d^2}$. Then the elements of B can be numbered $b_0, b_1, \ldots b_{m-1}$, so that for all i, $b_i + b_{i+1} \in A$.

The proof proceeds as follows. The Cayley sum-graph G of F_q with respect to A is a $(q, d, q^{1/2})$-graph, and hence by a theorem of Hoffman [17] its independence number is smaller than $q^{3/2}/d$. Let T be the induced subgraph of G on B. By the assumption $|(b - A) \cap B| > \frac{md}{2q}$ for all $b \in B$, the minimum degree in T is bigger than $\frac{md}{2q}$. We claim that this implies that the connectivity of T is at least $\frac{md}{6q}$. Indeed, otherwise we can delete from T a set of at most $\frac{md}{6q}$ vertices and disconnect it. Let U be the set of vertices of the smallest connected component after this deletion. Then $|U| \geq \frac{md}{3q}$, as the minimum degree of any vertex in the component is at least $\frac{md}{2q} - \frac{md}{6q} = \frac{md}{3q}$. There are no edges between U and the rest of the disconnected graph, which has at least $m/3$ vertices. Thus, by Lemma 2.5

$$\frac{md}{3q}\frac{m}{3} \leq \frac{q}{d^2}q^2,$$

that is, $m < \frac{3q^2}{d^{3/2}}$, contradicting the assumption that $m > \frac{6q^{5/2}}{d^2}$. Thus, the connectivity of T is at least $\frac{md}{6q}$, as claimed. Its independence number does not exceed that of G, which is at most $q^{3/2}/d$, as mentioned above. The desired result thus follows from the Chvatál-Erdős result, as $\frac{md}{6q} > q^{3/2}/d$, by assumption. In the special case that A is the set of all quadratic residues of a field F_q the above statement implies that the elements of every subset B of F_q of size $|B| = m > 25\sqrt{q}$ so that $|(b - A) \cap B| > \frac{m}{4}$ for all $b \in B$ can be arranged in a cycle so that all sums of adjacent elements are quadratic residues.

The proof in Section 3 together with the known results about solutions of equations in roots of unity, extending the basic result of Mahler [27], can provide large multiplicative subgroups in finite fields with no solutions of more general equations like $x + y + z = w$ and similar ones. Here is a sketch of the argument. For simplicity we only consider the equations $x + y = z$ and $x + y + z = w$ together, but it will be clear that the same method can work for other cases.

For nonzero rationals $a_1, \ldots, a_n$, a solution $(\xi_1, \ldots, \xi_n)$ of the equation $a_1\xi_1 + \ldots + a_n\xi_n = 1$ in roots of unity $\xi_1, \ldots \xi_n$ is non-degenerate if no proper subsum $\sum a_i\xi_i$ vanishes. Conway and Jones [10] showed that for any such non-degenerate solution $(\xi_1, \ldots, \xi_n)$, $\xi_1^s = \xi_2^s = \cdots = \xi_n^s = 1$, where s is a product of distinct primes $p_1, \ldots, p_\ell$ so that $\sum_{i=1}^{\ell}(p_i - 2) \leq n - 1$. For the special case of the equation $x + y + z = 1$, if each variable is a power $\xi = e^{2\pi i/d}$ and d is odd, it is clear that any solution is non-degenerate, since -1 is not a power of ξ, and hence no subsum can vanish. Thus, by the result of [10] there is a finite number C_0 (that we can compute explicitly), so that for every d which is coprime with C_0 and is not divisible by 6, the equation $\xi^{i_1} + \xi^{i_2} + \xi^{i_3} = 1$ (as well as the equation $\xi^{i_1} + \xi^{i_2} = 1$)

has no solution. We can now repeat the strategy of the proof in Section 3. Define

$$B = \prod_{1 \le i_< d} (\xi^i - 1) \prod_{1 \le i_1, i_2 < d} (\xi^{i_1} + \xi^{i_2} - 1) \prod_{1 \le i_1, i_2, i_3 < d} (\xi^{i_1} + \xi^{i_2} + \xi^{i_3} - 1)$$

and observe that this is an integer of absolute value smaller than 3^{d^3}. Therefore there are at most $d^3/\log d$ distinct primes that divide it. If $p \equiv 1 (\mathrm{mod}\ d)$ does not divide B then by the reasoning in Section 3 there is a multiplicative subgroup of size d in Z_p^* which contains neither solutions to $x + y = z$ nor solutions to $x + y + w = 1$. By the known results about Linnik's problem we can ensure the existence of such a prime p of size at most $O(d^4)$ for most d, or for smooth numbers d, and a prime of size $O(d^5)$ for each d coprime with C_0.

Acknowledgment We thank S. Kopparty, T. Szőnyi and Z. W. Sun for helpful comments.

References

[1] P. Allen, J. Bötcher, H. Hán, Y. Kohayakawa and Y. Person, Powers of Hamilton cycles in pseudorandom graphs, preprint, 2014.

[2] N. Alon and F. R. K. Chung, Explicit construction of linear sized tolerant networks, Discrete Math. 72(1988), 15-19. (Proc. First Japan Conf. on Graph Theory and Applications, Hakone, Japan, 1986.)

[3] N. Alon, Large sets in finite fields are sumsets, J. Number Theory 126 (2007), 110-118.

[4] N. Alon and M. Krivelevich, Constructive bounds for a Ramsey-type problem, Graphs and Combinatorics 13 (1997), 217-225.

[5] N. Alon and J. H. Spencer, *The Probabilistic Method, Third Edition*, Wiley, 2008, xv+352 pp.

[6] J. Bourgain, Multilinear exponential sums in prime fields under optimal entropy condition on the sources, GAFA 18 (2009), 1477-1502.

[7] J. Bourgain, N. Katz and T. Tao, A sum-product estimate in finite fields, and applications, Geom. Funct. Anal. 14 (2004), no. 1, 27–57.

[8] M. C. Chang, Short character sums for composite moduli, arXiv:1201.0299v1, 2012.

[9] V. Chvátal and P. Erdős, A note on Hamiltonian circuits, Discrete Math. 2 (1972), 111–113.

[10] J. H. Conway and A. J. Jones, Trigonometric Diophantine equations (On vanishing sums of roots of unity), Acta Arith. 30 (1976), no. 3, 229–240.

[11] P. Erdős and E. Szemerédi, On sums and products of integers, in: Studies in pure mathematics, Birkhäuser, Basel, 1983, 213–218.

[12] P. X. Gallagher, Primes in progressions to prime-power modulus, Invent. Math. 16 (1972), 191-201.

[13] M. Giulietti, On cyclic caps in 4-dimensional projective spaces, Des. Codes Cryptogr. 47(2008), 135–143.

[14] S. W. Graham and C. J. Ringrose, Lower bounds for least quadratic non- residues, In: Analytic number theory (Allerton Park, IL, 1989), Progr. Math., 85, Birkhauser, Boston, MA, (1990), 269-309.

[15] D. R. Heath-Brown, Siegel zeros and the least prime in an arithmetic progression. Quart. J. Math. Oxford Ser. (2) 41 (1990), no. 164, 405–418.

[16] D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression, Proc. London Math. Soc. (3) 64, no. 2 (1992), 265-338.

[17] A. J. Hoffman, On eigenvalues and colorings of graphs, B. Harris Ed., Graph Theory and its Applications, Academic, New York and London, 1970, 79-91.

[18] M. N. Huxley, Large values of Dirichlet polynomials, III, Acta Arith. 26 (1974), 435-444.

[19] H. Iwaniec, On zeros of Dirichlets L series, Invent. Math. 23 (1974), 97-104.

[20] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence RI, (2004).

[21] B. Jackson, Hamilton cycles in regular 2-connected graphs, J. Combin. Theory B 29 (1980), 27–46.

[22] M. Jutila, On Linnik's constant, Math. Scand. 41 (1977), 45-62.

[23] M. Krivelevich and B. Sudakov, Sparse pseudo-random graphs are Hamiltonian, J. Graph Theory 42 (2003), 17-33.

[24] M. Krivelevich and B. Sudakov, Pseudo-random graphs, in: More Sets, Graphs and Numbers, Bolyai Society Mathematical Studies 15, Springer, 2006, 199-262.

[25] M. Krivelevich, B. Sudakov and T. Szabó, Triangle factors in pseudo-random graphs, Combinatorica 24 (2004), 403-426.

[26] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, 1983.

[27] K. Mahler, Zur Approximation algebraischer Zahlen. I. (German), Math. Ann. 107 (1933), no. 1, 691–730.

[28] H. L. Montgomery, R. C. Vaughan and T. D. Wooley, Some remarks on exponential sums associated with k-th powers, Math. Proc. Cambridge Philos. Soc. 118 (1995), no. 1, 21–33.

[29] A. Sárkőzy, On products and shifted products of residues modulo p. Integers 8 (2008), no. 2, A9, 8 pp.

[30] Z. W. Sun, Some new problems in additive combinatorics, arXiv 1309.1679v3, 2013.

[31] T. Szőnyi, On cyclic caps in projective spaces, Des. Codes Cryptogr. 8 (1996), 327–332.

[32] A. Weil, Sur les courbes algébriques et les variéstés qui sèn déduisent, Actualités Sci. Ind., 1041 (1948), Herman, Paris.

[33] S. Yekhanin, A note on plane pointless curves, Finite Fields Appl 13 2007), 418–422.

[34] T. Xylouris, On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions, Acta Arith. 150 (2011), no. 1, 65–91.

[35] T. Xylouris, Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression [The zeros of Dirichlet L-functions and the least prime in an arithmetic progression], Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011, Bonner Mathematische Schriften [Bonn Mathematical Publications], 404. Universität Bonn, Mathematisches Institut, Bonn, 2011, 110 pp.

5 Appendix: sum-free subgroups in characteristic 2

In this appendix we present the proof of Proposition 1.3 following the approach of Yekhanin in [33]. Throughout the appendix, q is always some power of 2. We start with the following known lemma, for completeness we include a simple proof.

Lemma 5.1 *Let q be a power of 2 and suppose that $x, y, z \in F_{q^4}^*$ satisfy*

$$x^{q+1} + y^{q+1} + z^{q+1} = 0. \tag{15}$$

Then $(\frac{x}{y})^{q+1} \in F_q$ (and similarly $(\frac{x}{z})^{q+1}, (\frac{y}{z})^{q+1} \in F_q$.)

Proof. By (15),

$$x^{q+1} + y^{q+1} = z^{q+1}$$

and hence also

$$x^{q^3+q^2} + y^{q^3+q^2} = z^{q^3+q^2}$$

Multiplying and using the fact that for any $t \in F_{q^4}^*$, $T(t) = t^{q^3+q^2+q+1} \in F_q$ we get that

$$T(x) + T(y) + T(x)(\frac{y}{x})^{q+1} + T(y)(\frac{x}{y})^{q+1} = T(z).$$

This means that for $w = (\frac{x}{y})^{q+1}$ $(\neq 0)$ there are $a, b, c \in F_q$ so that $aw + b/w = c$, that is, w satisfies a quadratic equation $aw^2 - cw + b = 0$ over F_q. It follows that $w \in F_{q^2}^*$. Thus

$$w = (\frac{x}{y})^{q+1} \in F_{q^2},$$

and also

$$(\frac{x}{y})^{q^2+1} \in F_{q^2}$$

(as raising it to the power $q^2 - 1$ we get 1). It follows that

$$(\frac{x}{y})^2 = (\frac{x}{y})^{\gcd\,(q+1, q^2+1)} \in F_{q^2}$$

and since the mapping $f(t) = t^2$ is a bijection of F_{q^2}, as the characteristic is 2, it follows that $\frac{x}{y} \in F_{q^2}$ and hence that $(\frac{x}{y})^{q+1} \in F_q$, as needed. □

Corollary 5.2 *If $X, Y, Z \in F_{q^4}^*$ lie in the same coset of a multiplicative subgroup which is a subset of $\{w^{q+1} : w \in F_{q^4}^*\}$, and $X + Y + Z = 0$ then the ratios $X/Y, X/Z$ and Y/Z are all in F_q.*

Proof. By assumption $X = \rho x^{q+1}, Y = \rho y^{q+1}$ and $Z = \rho z^{q+1}$ for some $\rho, x, y, z \in F_{q^4}^*$, and

$$\rho x^{q+1} + \rho y^{q+1} + \rho z^{q+1} = 0.$$

The result thus follows from Lemma 5.1. □

Corollary 5.3 *If $X, Y, Z \in F_{q^4}^*$ lie in the same coset of the multiplicative subgroup $\{x \in F_{q^4}^* : x^{q^2+1} = 1\}$ then $X + Y + Z \neq 0$.*

Proof. Assume, for contradiction, that $X + Y + Z = 0$. Note that each element of the subgroup $\{x \in F_{q^4}^* : x^{q^2+1} = 1\}$ is $g^{q^2-1} = [g^{q-1}]^{q+1}$ for some $g \in F_{q^4}^*$. Thus, by Corollary 5.2, there is a $\rho \in F_{q^4}^*$ and $\alpha, \beta, \gamma \in F_q^*$ so that $X = \rho\alpha, Y = \rho\beta, Z = \rho\gamma$. Since X, Y, Z are in the same coset of the subgroup $\{x \in F_{q^4}^* : x^{q^2+1} = 1\}$ this implies that $X^{q^2+1} = Y^{q^2+1} = Z^{q^2+1}$. However, $X^{q^2+1} = \rho^{q^2+1}\alpha^{q^2+1} = \rho^{q^2+1}\alpha^2$, and together with the analogous expressions for Y^{q^2+1} and Z^{q^2+1} we conclude that $\alpha^2 = \beta^2 = \gamma^2$. Hence $\alpha = \beta = \gamma$ and thus $3\alpha = 0$ and $\alpha = 0$, contradiction. □

Lemma 5.4 *Define*

$$S_q = \{x \in F_{q^4}^* : x^{(q^2+1)(q-1)} = 1\}$$

Then every coset tS_q of S_q, for $t \in F_{q^4}^*$, can be partitioned into q^2+1 pairwise disjoint sets

$$tS_q = \cup_{i=1}^{q^2+1} C_i$$

so that each set C_i is $c_i F_q^*$ for some $c_i \in F_{q^4}^*$ and if $a+b+c=0$ for some $a,b,c \in tS_q$, then there exists an i so that $a,b,c \in C_i$.

Proof. We have to show that the ratios $a/b, a/c$ and b/c are all in F_q^*, and this follows from Corollary 5.2. □

We can now prove Proposition 1.3. Recall that $q = 2^{4 \cdot 4^k}$ and

$$d = (2^{2 \cdot 4^k} + 1)(2^{2 \cdot 4^{k-1}} + 1) \cdots (2^2 + 1).$$

Let H be the multiplicative subgroup of order d in F_q. We have to show that there are no $X, Y, Z \in H$ so that $X + Y + Z = 0$. This is equivalent to the assertion that for any nonzero coset of H in F_q there are no X, Y, Z in the coset with $X + Y + Z = 0$. We prove this fact by induction on k. For $k = 0$ this follows from Corollary 5.3 (with $q = 2$). Assuming the assertion for $k-1$, we prove it for k. Suppose this is false and $X + Y + Z = 0$. By Lemma 5.4 X, Y, Z lie in the same coset of $F_{2^{4^k}}^*$ and hence also in the same coset of $H \cap F_{2^{4^k}}^*$. However, any element x in $F_{2^{4^k}}^*$ satisfies

$$x^{2^{2 \cdot 4^k}+1} = x^2$$

and thus

$$H \cap F_{2^{4^k}}^* = \{x : x^{2(2^{2 \cdot 4^{k-1}}+1)\cdots(2^2+1)} = 1\} = \{x : x^{(2^{2 \cdot 4^{k-1}}+1)\cdots(2^2+1)} = 1\},$$

(where here we used that in characteristic 2, $z^2 = 1$ implies that $z = 1$). The desired contradiction now follows from the induction hypothesis. This completes the proof. □