Bull. Aust. Math. Soc. **94** (2016), 224–235
doi:10.1017/S000497271600023X

ALMOST ALL PRIMES HAVE A MULTIPLE OF SMALL HAMMING WEIGHT

CHRISTIAN ELSHOLTZ

(Received 26 January 2016; accepted 4 February 2016; first published online 23 May 2016)

Abstract

We improve recent results of Bourgain and Shparlinski to show that, for almost all primes p, there is a multiple mp that can be written in binary as

$$mp = 1 + 2^{m_1} + \cdots + 2^{m_k}, \quad 1 \le m_1 < \cdots < m_k,$$

with $k = 6$ (corresponding to Hamming weight seven). We also prove that there are infinitely many primes p with a multiplicative subgroup $A = \langle g \rangle \subset \mathbb{F}_p^*$, for some $g \in \{2, 3, 5\}$, of size $|A| \gg p/(\log p)^3$, where the sum–product set $A \cdot A + A \cdot A$ does not cover $\mathbb{F}_p$ completely.

2010 *Mathematics subject classification*: primary 11N25; secondary 11A41, 11A63, 11B13, 11B50, 11P05.

Keywords and phrases: primes, additive bases, sumsets, distribution of integers with multiplicative constraints, Waring's problem and variants.

1. Introduction

Recently, Shparlinski [42] initiated the study of prime divisors of 'sparse integers', that is, integers which only use a few nonzero digits in a g-ary representation. Let $g \ge 2$ and $k \ge 1$ be integers, and let $\mathcal{D} = (d_i)_{i=0}^k$ be a sequence of $k + 1$ nonzero integers. Let $\mathcal{S}_{g,k}(\mathcal{D})$ be the set of integers n of the form

$$n = d_0 + d_1 g^{m_1} + \cdots + d_k g^{m_k}, \tag{1.1}$$

where $1 \le m_1 < \cdots < m_k$. Here, the d_i can be thought of as (but are not necessarily) the g-ary digits $d_i \in \{1, \ldots, g-1\}$ of n. Using exponential sums, Shparlinski [42] proved that, for any fixed $\delta \in (0, 1/2)$ and every $k > \max\{15, \delta^{-1} - 1\}$, for sufficiently large X and for almost all primes $p \le X$ (that is for all but $o(\pi(X))$ primes, where $\pi(X)$ denotes the number of primes $p \le X$), there exists $n \in \mathcal{S}_{g,k}(\mathcal{D})$ with $\log n \ll X^{1/2+\delta}$ and such that $p \mid n$.

Using new bounds for very short exponential sums, Bourgain [4, 6] proved the existence of much smaller n. Let $\delta > 0$ and $k > k_0(\delta)$ and let X be sufficiently large.

Then, for all but $o(\pi(X))$ primes $p \le X$, there exists $n \in \mathcal{S}_{g,k}(\mathcal{D})$ with $\log n \ll X^{\delta}$ and such that $p \mid n$ holds.

Shparlinski [43] writes that working out k_0 from Bourgain's approach would take 'significant efforts'. With an alternative approach, using incomplete exponential sums 'on average over primes', he worked out an explicit admissible value. If $0 < \delta < 1/2$, one can take

$$k_0(\delta) = \frac{16}{\delta^2} + 1.$$

One may wonder, how much this can be improved. It is clear that we must have $k \ge \delta^{-1}$. The number of sparse integers of the type (1.1) is of order of magnitude $C_{k,g}(\log n)^k \ll X^{\delta k}$, and this expression must be at least of the same order of magnitude as the number of primes, namely, $X/\log X$.

It seems that there is no result in the literature that tries to minimise k, even when allowing a larger value n. It follows, from the results cited above, that $k = 16$ and $k = 66$, respectively, are admissible. Here, we will show that, actually, $k = 6$ suffices. As it turns out, the proof, essentially, combines two types of tools from the literature:

(a) recent results on sumsets modulo a fixed prime p from additive combinatorics;

(b) an old result of Erdős stating that, for most primes, the powers of two generate at least $p^{1/2+o(1)}$ distinct residue classes, and variants due to Pappalardi [37], Erdős and Ram Murty [17].

Using these tools, the proof is actually quite short. However, it seems that the new point of view and the method of proof yield considerable progress on the problem.

2. Discussion of the case $g = 2$

The Hamming weight of an integer counts the number of ones in its binary representation. The Hamming weight appears in several recent investigations, such as determining primes p with all positive values of $p - 2^i$ composite (see [46]) and quadratic nonresidues with small Hamming weight (see [13]). In this article, we show that almost all primes have a nonzero multiple with a bounded Hamming weight of at most seven (corresponding to $k = 6$ above).

Let T_k denote the set of those primes p which divide some integer of the form $2^{a_1} + \cdots + 2^{a_k} + 1$, where $a_1, \ldots, a_k \in \mathbb{N}$, and let $T_k(X)$ denote the number of such primes $p \le X$.

A result of Hasse [26] says that the Dirichlet density of primes $p \le x$ dividing a number of the form $2^a + 1$, where $a \in \mathbb{N}$, is $\frac{17}{24}$. This was later conjectured for natural density by Krishnamurty and eventually proved by Odoni [36]. In other words, $T_1(X) \sim \frac{17}{24}\pi(X) \sim \frac{17}{24}X/\log X$. There are extensions of this result to composite moduli, or to more general sequences such as $a^k + b^k$ due to Ballot [3], Moree [34], Odoni [36] and Wiertelak [49].

Skałba [44] made the following conjecture (see, also, [35]).

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

Conjecture 2.1 (Skałba). $T_2(X) \sim X/\log X$.

Skałba proved a partial result towards this conjecture. To formulate it, we first introduce some background. Let $\mathrm{ord}_p(a)$ denote the multiplicative order of a in $\mathbb{F}_p^*$. Erdős [16] (see also Bundshuh [8]) conjectured that, for each $0 < c < 1$, for almost all primes, $\mathrm{ord}_p(2) > p^c$ holds, and proved this for $c \le \frac{1}{2} - o(1)$. There have been several attempts to address this conjecture. On the generalised Riemann hypothesis (GRH), it is known that, for almost all primes p, $\mathrm{ord}_p(2) > p/f(p)$, where f tends (arbitrarily slowly) to infinity (see [37]). Unconditionally, refining work of Pappalardi [37], Erdős and Murty [17] proved that, for almost all primes $p \le x$ and for any function $\varepsilon(x)$ tending to zero as x tends to infinity,

$$\mathrm{ord}_p(2) \ge p^{1/2+\varepsilon(p)}$$

holds. Skałba gave a conditional proof of his conjecture using Weil's bounds [48] on the number of solutions of congruences.

Theorem 2.2 (Skałba [44]). *If* $\mathrm{ord}_p(2) > p^{0.8}$, *then there exist integers* a, b *such that*

$$2^a + 2^b + 1 \equiv 0 \pmod{p}$$

holds. In particular, if Erdős's conjecture holds with $c = 0.8$, *then Conjecture 2.1 holds.*

As progress on Erdős's conjecture has been very slow, it seems fair to say that Erdős's conjecture with $c = 0.8$ is currently very far from a solution. The currently known exponent $c = \frac{1}{2}$, combined with Skałba's method based on Weil estimates, seems insufficient to establish $T_k(X) \sim X/\log X$, for any fixed k.

We take a different approach to the problem. Combining methods from additive and multiplicative number theory, we prove a result towards Skalba's conjecture, where $2^a + 2^b + 1$ is replaced by $2^{a_1} + \cdots + 2^{a_6} + 1$. In other words, we prove that $T_6(x) \sim x/\log x$. This means that almost all primes p have a nonzero multiple mp with Hamming weight at most seven. Observe that the number of integers $n \le N$ with Hamming weight at most k is about

$$\sum_{i=0}^{k} \binom{t}{i} \quad \text{where } t \sim \frac{\log N}{\log 2}.$$

Hence there are about $O((\log N)^6)$ odd integers $n \le N$ of Hamming weight at most seven. For a given prime p, the corresponding multiple mp of small Hamming weight can, of course, be much larger than the prime. As the proof shows, the exponents a_i are bounded above by $p - 1$, and hence $mp \le k2^{p-1} + 1$. It seems possible to reduce the exponent by a small factor, following the techniques in [10, 19], but we do not make an attempt to do this.

One may wonder if this result, that almost all primes have a very sparse binary multiple, has any practical application. Of course, addition and multiplication with

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

sparse integers should be faster than with arbitrary integers, but it seems that one would actually need to find this sparse multiple in the first place and there could be several more issues to overcome.

We prove similar results, where $2^a + 2^b + 1$ is replaced by $2^{a_1}3^{b_1}5^{c_1} + 2^{a_2}3^{b_2}5^{c_2} + 1$. A more general formulation of these results is given in the next section.

In the opposite direction, Skałba proved the following theorem.

THEOREM 2.3 (Skałba [44]). *Let $\Omega(w)$ denote the number of prime factors of w, counted with multiplicity. If $\Omega(2^n - 1) < \log n/\log 3$, then there exists a prime divisor p of $2^n - 1$ such that there is no pair of integers (a, b), for which $2^a + 2^b + 1 \equiv 0 \pmod p$.*

We will extend this to a similar estimate with $2^a + 2^b$ replaced by a k-fold sum. One may conjecture that, for arbitrarily large k, there are infinitely many primes m such that no multiple of m can be written as $\sum_{i=1}^{k} 2^{s_i}$ for nonnegative integers s_i. This would, of course, follow if there exist an infinite number of Mersenne primes, but the condition $\Omega(2^n - 1) < \log n/\log k$ in Theorem 3.9 is much more modest.

In the last section of the paper, we study a restriction to sum–product estimates.

3. Results

3.1. Representation of residue classes and approximations to Skałba's conjecture.

THEOREM 3.1. *Let $r \geq 2$ and $m \neq 0$ be fixed integers. For almost all primes $p \leq x$, there is a solution of*

$$r^{a_1} + r^{a_2} + \cdots + r^{a_6} \equiv m \pmod p,$$

with integers $0 \leq a_1, \ldots, a_6 < p - 1$. More precisely, with $\varepsilon > 0$, the number of primes $p \leq X$ with no solution of

$$r^{a_1} + r^{a_2} + \cdots + r^{a_6} \equiv m \pmod p$$

is $O_r(X^{22/23+\varepsilon})$.

With $r = 2, m = -1$, we get the following approximation to Skałba's conjecture.

COROLLARY 3.2. *The following holds: $T_6(X) \sim X/\log X$.*

REMARK 3.3. In the special case that there exists some i with $2^i \equiv -1 \pmod p$, one can reduce the '6' in Theorem 3.1 above (with a different size of the exceptional set) to '5', in view of recent work of Shkredov [41, Theorem 2].

THEOREM 3.4. *Let $r \geq 2$. For almost all primes $p \leq X$, there are at least $p^{4/5}$ residue classes m which can be represented by*

$$r^{a_1} + r^{a_2} \equiv m \pmod p,$$

with integers $0 \leq a_1, a_2 < p - 1$.

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

Other approximations to Skałba's conjecture are as follows.

THEOREM 3.5. *Let $r, s \geq 2$ be coprime integers and let $m \neq 0$ be a fixed integer. For almost all primes $p \leq X$, there is a solution of*

$$r^{a_1} s^{a_2} + r^{a_3} s^{a_4} + r^{a_5} s^{a_6} \equiv m \pmod{p},$$

with integers $0 \leq a_1, \ldots, a_6 < p - 1$.

THEOREM 3.6. *Let $r, s, t \geq 2$ be mutually coprime integers and let $m \neq 0$ be a fixed integer. For almost all primes $p \leq X$, there is a solution of*

$$r^{a_1} s^{a_2} t^{a_3} + r^{a_4} s^{a_5} t^{a_6} \equiv m \pmod{p},$$

with integers $0 \leq a_1, \ldots, a_6 < p - 1$.

For completeness, we also state the following, which is a direct consequence of a result of [39].

COROLLARY 3.7. *Let $r \geq 2$. If $\mathrm{ord}_p(r) > p^{3/4}$, then, for some integers a_1, a_2,*

$$r^{a_1} + r^{a_2} + 1 \equiv 0 \pmod{p}.$$

In particular, if Erdős's conjecture holds with $c = 0.75$, then Conjecture 2.1 holds. This last result replaces $\frac{4}{5}$ in Skałba's Theorem (mentioned above) by $\frac{3}{4}$.

REMARK 3.8. Another approach to this problem could run as follows.

(a) Baker and Harman [2] proved that, for a positive proportion of primes, the largest prime factor P of $p - 1$ is large: that is, $P(p-1) \gg p^{0.677}$. This result is ineffective due to the use of Siegel zeros.

(b) Harman [23] also gave an effective result (that is, not depending on a Siegel zero), that for some positive (computable) density of the primes, the largest prime factor of $p - 1$ satisfies $P(p-1) \gg p^{0.6105}$.

From (a), one can deduce that, for a positive (ineffective) proportion of primes, $\mathrm{ord}_p(2) \gg p^{0.677}$ holds. In view of the large prime factor, we first consider the case in which 2 generates only $O(p^{1/3})$ residue classes. Here we know, from the Erdős conjecture with $c = \frac{1}{2}$ (see also Lemma 4.1), that this case rarely happens. In the other case, 2 generates a subgroup of size at least $cp^{0.677}$ residue classes (see, also, [31, Lemma 20]). This would imply (by Lemma 4.5) that, for these primes, $2^a + 2^b + 2^c + 1 \equiv 0 \pmod{p}$ has a solution. However, in its current form, this consequence would be much weaker than Hasse's result, namely, that, for a density of 17/24 of the primes, even $2^a + 1 \equiv 0 \pmod{p}$ has a solution. Therefore we do not pursue this path further.

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

3.2. Primes without multiples of small Hamming weight. As an extension of Skałba's second theorem with regard to multiple sums, and thus a limitation or partial converse to the type of results above, we prove the following theorem.

THEOREM 3.9. *If*

$$\Omega(2^n - 1) < \frac{\log n}{\log k},$$

then there is some prime factor $q \mid 2^n - 1$ *such that*

$$2^{a_1} + \cdots + 2^{a_{k-1}} + 1 \not\equiv 0 \pmod{q},$$

for all integer choices of a_i. *Hence all multiples of* q *have Hamming weight at least* $k + 1$.

3.3. A restriction on sum–product estimates. Suppose a k-fold sum $r^{a_1} + \cdots + r^{a_k}$ covers all residue classes, in particular, the class zero; here, without loss of generality, $a := a_k \le \cdots \le a_1$. Dividing by r^a, one obtains that $r^{a_1-a} + \cdots + r^{a_{k-1}-a} + 1 \equiv 0 \pmod{p}$. The related question has also been studied, concerning the minimal number d such that the mixed d-fold sum–product set $dAB := \{a_1b_1 + \cdots + a_db_d : a_i \in A, b_i \in B\}$ covers all residue classes.

For random sets $A \subset \mathbb{Z}/p\mathbb{Z}$ with $|A| \ge C_\varepsilon p^{1/2+\varepsilon}$, one may expect that $A + A = \mathbb{Z}/p\mathbb{Z}$. See, for example, some discussion (with too optimistic conjectures) in [9, 25, 38]. The last authors observed that some kind of restriction must occur. They write about subsets $A \subset \mathbb{F}_q$: 'Due to the misbehavior of the zero element it is not possible for $A \cdot A + A \cdot A = \mathbb{F}_q$ unless A is a positive proportion of the elements of $\mathbb{F}_q$'.

It may be worth recalling that, for a prime $p \equiv 3 \pmod 4$, the set A of (nonzero) quadratic residues has positive density, but $0 \notin AA + AA$. The set of squares are, of course, an explicit example of a large multiplicative subgroup of $\mathbb{F}_p^*$ with restricted sumsets in $\mathbb{F}_p$. On the other hand, this example of size $|A| = \frac{1}{2}(p-1)$ is extremal, as, for any set A with $|A| \ge \frac{1}{2}(p+1)$, the Cauchy–Davenport theorem guarantees that $A + A = \mathbb{F}_p$.

The set of squares is generated by the square g^2 of a primitive root g. But, as g^2 is not a fixed element, following the viewpoint of this paper, one can ask if there exist such examples generated by a fixed element, for example $g = 2$ and $A = \{2^i \pmod p : 1 \le i \le \mathrm{ord}_p(2)\}$. The answer is probably yes, but, unconditionally, we can only prove a slightly weaker result.

Let us first describe an explicit and 'large' example, where, however, we cannot prove that this type of example will occur an infinite number of times. We then describe a slightly weaker example, which occurs quite frequently.

Let a be fixed, and p be a prime with $\mathrm{ord}_p(a) = \frac{1}{2}(p-1)$, where $\frac{1}{2}(p-1)$ is odd. Let $A = B = \{a^i : 1 \le i \le \frac{1}{2}(p-1)\}$. Then $|A|\,|B| \sim \frac{1}{4}p^2$ and $2AB = A^2 + A^2 = A + A$. But $0 \notin A + A$, as, otherwise, $a^i \equiv -a^j \pmod p$ and -1 is not in the multiplicative subgroup generated by a, as a has odd order. The size of $|A| = \frac{1}{2}(p-1)$ is, of course, much larger than $p^{1/2+\varepsilon}$. For $a = 2$, such primes are $p = 7, 23, 47, 71, 79, 103, 167, 191, 199, \ldots$.

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

Alternatively, one can take primes $p \equiv 3 \pmod 4$, with 2 as primitive root, and $A = \{4^i : 1 \le i \le \frac{1}{2}(p-1)\}$. Such primes are $3, 11, 19, 59, 67, 83, 107, 131, 139, 163, 179, \ldots$. Artin's conjecture on primitive roots (known only on GRH; see [29]) predicts that such sets of primes have a positive density in the set of primes.

Unconditionally, we are able to prove the existence of an infinite number of primes with a restricted sumset for the following slightly weaker variant.

THEOREM 3.10. *For a given prime p, let $s = s(p)$ and $w = w(p)$ be defined by $p = 2^s w + 1$, where w is odd. For almost all positive square-free numbers $a > 1$, with at most three exceptions (or almost all primes, with at most two exceptions), there exist positive constants c and c_1, and there exist at least $c_1 x/(\log x)^2$ many primes $p \le x$, such that the multiplicative subgroup*

$$A = \{(a^{2^s})^i : 1 \le i \le \mathrm{ord}_p(a^{2^s})\} \subset \mathbb{F}_p^*$$

has the following properties:

(a) $|A| > cp/(\log p)^3$*; and*

(b) $A \cdot A + A \cdot A = A + A \ne \mathbb{F}_p$.

REMARK 3.11. In this situation, $A = A \cdots A$, but, as $|A \cdot A|$ is typically much larger than $|A|$, we state it in the form above.

Let us mention a related result by Alon and Bourgain [1]: there is an absolute constant $c > 0$ so that there are infinitely many primes p and a multiplicative subgroup $A \subset \mathbb{F}_p^*$, with $|A| \ge cp^{1/3}$, such that there are no $x, y, z \in A$ with $x + y = z$.

4. Proofs

We observe that Erdős's conjecture only makes a statement about the number of residue classes of the form $r^i \pmod p$ (for fixed r and p), but not about its algebraic structure. Observing that these classes are a multiplicative subgroup of $\mathbb{F}_p^*$, we now study sumsets of multiplicative subgroups in $\mathbb{F}_p^*$. In recent years, there has been a considerable number of papers concerned with sumsets modulo primes. Of the many results available, we choose those results that seem best suited for our application.

4.1. Lemmas. In the proof, we use the first two lemmas below coming from multiplicative number theory and several very recent quantitative versions of results from additive combinatorics.

LEMMA 4.1 (Erdős-Murty [17, Theorem 5], Pappalardi [37]). *Let $\Gamma \subseteq \mathbb{Q}^*$ be a multiplicative subgroup of rank d. Suppose that Γ is generated by the mutually coprime numbers $b_1, \ldots, b_d$. For all primes p not dividing the denominators of $b_1, \ldots, b_d$, we define $f_\Gamma(p)$ to be the order of $\Gamma \pmod p$. Let $\varepsilon(x)$ be any function tending to zero as $x \to \infty$. For all but $o(x/\log x)$ primes $p \le x$,*

$$f_\Gamma(p) \ge p^{d/(d+1)+\varepsilon(p)}.$$

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

The number of exceptional primes can be bounded from above more precisely (see, for example, [18, 30]). However, for our situation, a method of Matthews, worked out in detail by Pappalardi, is suitable. Here $b_1, \dots, b_d$ are multiplicatively independent integers, which are not squares, and are not ± 1.

Lemma 4.2 (Pappalardi [37, Lemma 1.2], Matthews [33]). *Suppose that d is a function of t such that dt^{-d} is bounded. Then*

$$|\{p : f_\Gamma(p) \le t\}| \ll \frac{t^{1+1/d}}{\log t} 2^d d \sum_{i=1}^{d} \log b_i$$

uniformly with respect to t, d and $\{b_1, \dots, b_d\}$.

Our application will only need the special case $d = 1$.

A slightly weaker version of Lemma 4.1 goes back to Erdős [16], and one can give the following very simple proof. The sequence $(2^i \pmod p), i = 1, \dots, n$, is periodic. The order, $\mathrm{ord}_p(2)$, is, by definition, the length of the period, and one has $2^{\mathrm{ord}_p(2)} \equiv 1 \pmod p$. This implies that

$$\prod_{p<y} p^{\lfloor n/(\mathrm{ord}_p(2))\rfloor} \le \prod_{i=1}^{n} (2^i - 1) \le 2^{n(n+1)/2},$$

where the product on the left-hand side runs over the primes, up to some level y, specified below. Taking logarithms, one sees that

$$\sum_{p<y} \log p \left\lfloor \frac{n}{\mathrm{ord}_p(2)} \right\rfloor \le Cn^2, \tag{4.1}$$

for some positive constant C. Assuming that $\mathrm{ord}_p(2) \le y^{1/2-\varepsilon}$ for at least $\delta y/\log y$ of the primes $p \le y$ (for some $\delta > 0$), then

$$\sum_{p<y} \log p \left(\frac{n}{\mathrm{ord}_p(2)} - 1 \right) \ge \frac{\delta y}{\log y} \left(\frac{n}{y^{1/2-\varepsilon}} - 1 \right) \ge \delta n \frac{y^{1/2+\varepsilon}}{\log y} - \frac{y}{\log y}.$$

For $y = n^2$ this contradicts (4.1), proving that, for most primes $p < n^2$, the powers $1, 2, 4, \dots, 2^n$ occupy more than $y^{1/2-\varepsilon} > p^{1/2-\varepsilon}$ distinct residue classes modulo p. For more general discussions, see [14].

We now come to the additive ingredients, which are more modern and much deeper.

Lemma 4.3 (Hart [24]). *Let $R \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup such that $|R| \ge p^\kappa$, where $\kappa > \frac{11}{23}$. Then, for all sufficiently large p, $6R := R + R + R + R + R + R \supseteq \mathbb{F}_p^*$.*

An earlier version with exponent $\frac{41}{83}$ appeared in [39, Theorem 4.1], and with $\frac{55}{112}$ in [40, Corollary 32]. See, also, [11, 12, 15] for a number of related results on Waring's problem modulo p.

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

Lemma 4.4 (Hart [24, Theorem 10]). *Let R be a multiplicative subgroup of $\mathbb{F}_p^*$ with $|R| \ll p^{5/9-\varepsilon}$. Then $|R+R| \gg |R|^{8/5}(\log|R|)^{-3/10}$.*

Lemma 4.5 (Schoen and Shkredov [39, Theorem 2.6, $l=3$]). *Let R be a multiplicative subgroup of $\mathbb{F}_p^*$, with $|R| > p^{2/3}$. Then $3R := R+R+R \supseteq \mathbb{F}_p^*$.*

Lemma 4.6 (Schoen and Shkredov [39, Theorem 2.6, $l=2$]). *Let R be a multiplicative subgroup of $\mathbb{F}_p^*$, with $|R| > p^{3/4}$. Then $2R := R+R \supseteq \mathbb{F}_p^*$.*

For the case of a twofold sum, there was important earlier work by Heath-Brown and Konyagin [28]. Let R be a multiplicative subgroup of $\mathbb{F}_p^*$, with $|R| \gg p^{2/3}$. Then $|R+R| \gg p$. Also, several related results of this type of theorem are due to Bourgain [5], Glibichuk [20, 21], Glibichuk and Rudnev [22], Cochrane and Pinner [11], Hart and Iosevich [25] and Bourgain *et al.* [7].

4.2. Proofs of the Theorems. After this preparation, the Theorems are straightforward consequences. The sets

$$R = \{r^i : 1 \le i \le \mathrm{ord}_p(r)\}, \quad R = \{r^i s^j : 1 \le i \le \mathrm{ord}_p(r), 1 \le j \le \mathrm{ord}_p(s)\}, \text{ etc.}$$

are multiplicative subgroups of $\mathbb{F}_p^*$ so that the corresponding lemmas apply, as follows.

Proof of Theorem 3.1. The result follows from Lemma 4.1, with $d=1$, $b_1 = r$, and Lemma 4.3. Observe that $\frac{11}{23} < \frac{1}{2}$. It suffices to estimate how often $\mathrm{ord}_p(r) \le p^{11/23+\varepsilon}$ holds. It follows, from Lemma 4.2, with $d=1, b_1 = r, t = x^{11/23+\varepsilon/2}$, that

$$|\{p : \mathrm{ord}_p(r) \le p^{11/23+\varepsilon/2}\}| \le |\{p : \mathrm{ord}_p(r) \le x^{11/23+\varepsilon/2}\}| \ll_r \frac{x^{22/23+\varepsilon}}{\log x}. \qquad \square$$

Proof of Theorem 3.4. The result follows from Lemma 4.1, with $d=1$, $b_1 = r$, and from Lemma 4.4, with $|R| \ge p^{1/2+\varepsilon}$, and by observing that $p^{8\varepsilon/5}/(\log p)^{3/10} \gg p^{\varepsilon}$. $\square$

Proof of Theorem 3.5. Use Lemma 4.1, with $d=2$, and Lemma 4.5. $\square$

Theorem 3.6. Use Lemma 4.1, with $d=3$, and Lemma 4.6. $\square$

Proof of Corollary 3.7. Use Lemma 4.6. $\square$

Proof of Theorem 3.9. Every multiple of an integer of the form $M = 2^n - 1$ has Hamming weight at least n (see [45, Theorem 2.1] or [47]). Moreover, if

$$R := \Omega(2^n - 1) < \frac{\log n}{\log k},$$

then some prime factor $q \mid 2^n - 1$ also has this property. To see this, we adapt Skałba's argument. Let $M = 2^n - 1 = \prod_{i=1}^{r} q_i^{t_i}$. Suppose all q_i have some multiple $w_i q_i$ which is a sum of at most k powers of two: that is,

$$w_i q_i = \varepsilon_{1,i} 2^{s_1(q_i)} + \cdots + \varepsilon_{k,i} 2^{s_k(q_i)},$$

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

with $\varepsilon_{j,i} \in \{0, 1\}$ (not all of them being zero). On the one hand,

$$P := \prod_{i=1}^{r} (w_i q_i)^{t_i} = \prod_{i=1}^{r} (\varepsilon_{1,i} 2^{s_1(q_i)} + \cdots + \varepsilon_{k,i} 2^{s_k(q_i)})^{t_i}$$

is a multiple of M and thus has Hamming weight at least n. On the other hand, P is a sum of at most $k^{\sum_{i=1}^{r} t_i} = k^{\Omega(2^n-1)} = k^R < n$ powers of two, which is a contradiction. Hence there is some prime divisor $q \mid 2^n - 1$ for which

$$\varepsilon_i 2^{s_1(q)} + \cdots + \varepsilon_k 2^{s_k(q)} \not\equiv 0 \pmod{q},$$

and hence all nonzero multiples of q have Hamming weight at least $k + 1$. □

Proof of theorem 3.10. In the proof below, the c_i are suitably chosen positive constants. By Heath-Brown's work [27, Corollary 3] on Artin's primitive root conjecture, for any fixed bound x and any four distinct positive square-free numbers a_1, a_2, a_3, a_4 (not being one), or for any three distinct primes, one of these, say, a, is a primitive root (that is, $\operatorname{ord}_p(a) = p - 1$) for at least $c_1 x/(\log x)^2$ such primes $p \le x$. Hence, for suitable x, there are at least $c_2 x/(\log x)^2$ such primes with $\frac{1}{2}x < p \le x$. Write $p - 1 = 2^s w$, where w is odd, and $y = \frac{1}{4} c_2 p/(\log p)^3$. As there are at most

$$y \frac{\log x}{\log 2} < \frac{c_2}{2} \frac{x}{(\log x)^2}$$

such primes with $w \le y$, there are at least $\frac{1}{2} c_2 x/(\log x)^2$ many primes p with $\operatorname{ord}_p(a^{2^s}) = w \gg p/(\log p)^3$. Observe that all elements of the form $a^{2^s i}$ have odd order and that, therefore, -1 is not of this type. As $a^{2^s i} + 1 \not\equiv 0 \pmod{p}$, it follows that the set $A = \{a^{2^s i} : 1 \le i \le \operatorname{ord}_p(a^{2^s})\}$ is of size $|A| \gg p/(\log p)^3$, but $0 \notin A + A = A^2 + A^2$. □

5. Open problems

Finally, we state some open questions.

(1) For primes $p \notin T_2$, does $\operatorname{ord}_p(2) \le c_\varepsilon p^{1/2+\varepsilon}$ hold, for all $\varepsilon > 0$ and some constant c_ε?

(2) For $h \to \infty$, what can one say about primes $p \notin T_h$, that are not Mersenne numbers? (For some heuristics on Mersenne numbers see also [32].)

(3) How can one algorithmically find a 'sparse' representation of a multiple of p? Can this be used for other complexity questions?

Finally, we note that there are 231 primes $p \le 4 \times 10^6$ which are not in T_2, whereas there are 283 146 primes below 4 million. On the other hand, as conjectured by Skałba [44], proving that there are infinitely many such primes remains an open problem.

Acknowledgements

I would like to thank Rainer Dietmann, Igor Shparlinski and the referees for useful comments.

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

References

[1] N. Alon and J. Bourgain, 'Additive patterns in multiplicative subgroups', *Geom. Funct. Anal.* **24**(3) (2014), 721–739.

[2] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.* **83**(4) (1998), 331–361.

[3] C. Ballot, 'Density of prime divisors of linear recurrences', *Mem. Amer. Math. Soc.* **115**(551) (1995).

[4] J. Bourgain, 'New bounds on exponential sums related to the Diffie–Hellman distributions', *C. R. Math. Acad. Sci. Paris* **338**(11) (2004), 825–830.

[5] J. Bourgain, 'Mordell's exponential sum estimate revisited', *J. Amer. Math. Soc.* **18** (2005), 477–499.

[6] J. Bourgain, 'Estimates on exponential sums related to the Diffie–Hellman distributions', *Geom. Funct. Anal.* **15**(1) (2005), 1–34.

[7] J. Bourgain, N. Katz and T. Tao, 'A sum–product estimate in finite fields, and applications', *Geom. Funct. Anal.* **14**(1) (2004), 27–57.

[8] P. Bundschuh, 'Solution of problem 618', *Elem. Math.* **26** (1971), 43–44.

[9] J. Chapman, M. Erdoğan, D. Hart, A. Iosevich and D. Koh, 'Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum–product estimates', *Math. Z.* **271**(1) (2012), 63–93.

[10] J. Cilleruelo and A. Zumalacárregui, 'An additive problem in finite fields of powers of elements of large multiplicative order', *Rev. Mat. Complut.* **27**(2) (2014), 501–508.

[11] T. Cochrane and C. Pinner, 'Sum-product estimates applied to Waring's problem mod p', *Integers* **8** (2008), A46, 18 pp.

[12] T. Cochrane, D. Hart, C. Pinner and C. Spencer, 'Waring's number for large subgroups of $\mathbb{Z}_p^*$', *Acta Arith.* **163**(4) (2014), 309–325.

[13] R. Dietmann, C. Elsholtz and I. Shparlinski, 'On gaps between primitive roots in the Hamming metric', *Q. J. Math.* **64**(4) (2013), 1043–1055.

[14] C. Elsholtz, 'The distribution of sequences in residue classes', *Proc. Amer. Math. Soc.* **130**(8) (2002), 2247–2250.

[15] C. Elsholtz, 'The number $\Gamma(k)$ in Waring's problem', *Acta Arith.* **131** (2008), 43–49.

[16] P. Erdős, 'Bemerkungen zu einer Aufgabe in den Elementen', *Arch. Math. (Basel)* **27**(2) (1976), 159–163.

[17] P. Erdős and M. Ram Murty, 'On the order of $a \pmod p$', in: *Number Theory (Ottawa, 1996)*, CRM Proceedings and Lecture Notes, 19 (American Mathematical Society, Providence, RI, 1999), 87–97.

[18] K. Ford, 'The distribution of integers with a divisor in a given interval', *Ann. of Math. (2)* **168** (2008), 367–433.

[19] M. Z. Garaev and K. L. Kueh, 'Distribution of special sequences modulo a large prime', *Int. J. Math. Math. Sci.* **50** (2003), 3189–3194.

[20] A. A. Glibichuk, 'Additive properties of product sets in an arbitrary finite field', Preprint, arXiv:0801.2021, 2008.

[21] A. A. Glibichuk, 'Sums of powers of subsets of an arbitrary finite field', *Izv. Ross. Akad. Nauk Ser. Mat.* **75**(20) (2011), 35–68 (in Russian); translation in *Izv. Math.* **75**(2) (2011), 253–285.

[22] A. A. Glibichuk and M. Rudnev, 'On additive properties of product sets in an arbitrary finite field', *J. Anal. Math.* **108** (2009), 159–170.

[23] G. Harman, 'On the greatest prime factor of $p-1$ with effective constants', *Math. Comp.* **74**(252) (2005), 2035–2041.

[24] D. Hart, 'A note on sumsets of subgroups in $\mathbb{Z}_p^*$', *Acta Arith.* **161** (2013), 387–395.

[25] D. Hart and A. Iosevich, 'Sums and products in finite fields: an integral geometric viewpoint', in: *Contemporary Mathematics,* 464 (American Mathematical Society, Providence, RI, 2008), 129–135.

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press

[26] H. Hasse, 'Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist', *Math. Ann.* **166** (1966), 19–23.
[27] D. R. Heath-Brown, 'Artin's conjecture for primitive roots', *Q. J. Math. Oxford Ser. 2* **37**(1) (1986), 27–38.
[28] D. R. Heath-Brown and S. Konyagin, 'New bounds for Gauss sums derived from kth powers and for Heilbronn's exponential sum', *Q. J. Math.* **51**(2) (2000), 221–235.
[29] C. Hooley, 'On Artin's conjecture', *J. reine angew. Math.* **225** (1967), 209–220.
[30] K.-H. Indlekofer and N. M. Timofeev, 'Divisors of shifted primes', *Publ. Math. Debrecen* **60** (2002), 307–345.
[31] P. Kurlberg and C. Pomerance, 'On the periods of the linear congruential and power generators', *Acta Arith.* **119**(2) (2005), 149–169.
[32] F. Luca and P. Stanica, 'Prime divisors of Lucas sequences and a conjecture of Skałba', *Int. J. Number Theory* **1**(1) (2005), 583–591.
[33] C. R. Matthews, 'Counting points modulo p for some finitely generated subgroups of algebraic groups', *Bull. Lond. Math. Soc.* **14** (1982), 149–154.
[34] P. Moree, 'On the divisors of $a^k + b^k$', *Acta Arith.* **80**(3) (1997), 197–212.
[35] P. Moree, 'Artin's primitive root conjecture—a survey', *Integers* **12A** A13 (2012).
[36] R. W. K. Odoni, 'A conjecture of Krishnamurthy on decimal periods and some allied problems', *J. Number Theory* **13**(3) (1981), 303–319.
[37] F. Pappalardi, 'On the order of finitely generated subgroups of Q^* (mod p) and divisors of $p - 1$', *J. Number Theory* **57**(2) (1996), 207–222.
[38] M. Rudnev, 'An improved estimate on sums of product sets', arXiv:0805.2696v1, 2008.
[39] T. Schoen and I. D. Shkredov, 'Additive properties of multiplicative subgroups of $\mathbb{F}_p$', *Q. J. Math.* **63**(3) (2012), 713–722.
[40] I. D. Shkredov, 'Some new inequalities in additive combinatorics', *Mosc. J. Comb. Number Theory* **3**(3–4) (2013), 189–239.
[41] I. D. Shkredov, 'On exponential sums over multiplicative subgroups of medium size', *Finite Fields Appl.* **30** (2014), 72–87.
[42] I. E. Shparlinski, 'Prime divisors of sparse integers', *Period. Math. Hungar.* **46**(2) (2003), 215–222.
[43] I. E. Shparlinski, 'Exponential sums and prime divisors of sparse integers', *Period. Math. Hungar.* **57**(1) (2008), 93–99.
[44] M. Skałba, 'Two conjectures on primes dividing $2^a + 2^b + 1$', *Elem. Math.* **59**(4) (2004), 171–173.
[45] K. B. Stolarsky, 'Integers whose multiples have anomalous digital frequencies', *Acta Arith.* **38** (1980), 117–128.
[46] T. Tao, 'A remark on primality testing and decimal expansions', *J. Aust. Math. Soc.* **91**(3) (2011), 405–413.
[47] S. Wagstaff Jr., 'Prime numbers with a fixed number of one bits or zero bits in their binary representation', *Experiment. Math.* **10**(2) (2001), 267–274.
[48] A. Weil, 'Numbers of solutions of equations in finite fields', *Bull. Amer. Math. Soc.* **55** (1949), 497–508.
[49] K. Wiertelak, 'On the density of some sets of primes. IV', *Acta Arith.* **43**(2) (1984), 177–190.

CHRISTIAN ELSHOLTZ, Institute of Analysis and Number Theory,
Graz University of Technology, Kopernikusgasse 24, A-8010 Graz, Austria
e-mail: elsholtz@math.tugraz.at

https://doi.org/10.1017/S000497271600023X Published online by Cambridge University Press