PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 1, January 2012, Pages 1–6
S 0002-9939(2011)10866-9
Article electronically published on May 3, 2011

DISTRIBUTION OF RESIDUES IN APPROXIMATE SUBGROUPS OF $\mathbb{F}_p^*$

NORBERT HEGYVÁRI AND FRANÇOIS HENNECART

(Communicated by Matthew A. Papanikolas)

Abstract. We extend a result due to Bourgain on the uniform distribution of residues by proving that subsets of the type $f(I) \cdot H$ are equidistributed (as p tends to infinity), where f is a polynomial, I is an interval of $\mathbb{F}_p$ and H is an approximate subgroup of $\mathbb{F}_p^*$ with size larger than polylogarithmic in p.

1. Introduction

During the last few decades, additive combinatorics has become a central topic in number theory. At the origin, there are several very powerful and important results such as Freiman's theorem, Szemerédi's theorem, Balog-Szemerédi-Gowers' theorem, etc. (see [12] for a detailed description of these results). Surprisingly, these results have many applications, not only in combinatorial additive number theory but also in various topics such as the estimation of exponential sums. In this paper, we consider the closely related question of the equidistribution of the elements of a given multiplicative subgroup of a finite field with prime cardinality. For δ a positive real number and g a nonzero element of the prime field with p elements, Bourgain obtained in [2], under some restricted condition on the order of g, an asymptotic equidistribution for the residues $xg^n \pmod p$, $0 \le x < p^\delta,\ n \ge 0$. The proof of Bourgain's result uses the three above-quoted theorems in combination with algebraic tools. In this paper, our aim is to extend this equidistribution result to less structured sets.

For any prime number p, we denote by $\mathbb{F}_p$ the finite field with p elements and let $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. By an interval in $\mathbb{F}_p$, we mean a subset in the form

$$I = \{ax + b \pmod p \mid 0 \le x \le |I| - 1\}$$

for some $(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p$.

Let $\epsilon > 0$. We say that a subset H of $\mathbb{F}_p$ is ϵ-equidistributed modulo p if for any interval J of $\mathbb{F}_p$, we have

$$\Big| \frac{|H \cap J|}{|H|} - \frac{|J|}{p} \Big| < \epsilon.$$

Received by the editors June 7, 2010 and, in revised form, October 26, 2010.
2010 *Mathematics Subject Classification.* Primary 11B75.
Research of the first author is partially supported by OTKA grants K 61908 and K 67676. He is grateful to the members of the LAMUSE (Laboratory of Mathematics of the University of Saint-Etienne) for their warm hospitality during his stay.

Using the Weyl criterion, ϵ-equidistribution modulo p follows from the following bound on trigonometric sums:

$$\max_{\substack{a\in\mathbb{Z}\\ p\nmid a}}\Big|\sum_{h\in H} e_p(ah)\Big| < \epsilon'|H|, \tag{1}$$

for some $\epsilon' > 0$ (depending on ϵ). Here we wrote $e_p(x)$ for $e^{2\pi i x/p}$.

Let H be a (multiplicative) subgroup of $\mathbb{F}_p^*$. In [3], it is shown that if

$$|H| > p^{(\log\log p)^{-c}},$$

where c is an explicit positive constant, then (1) holds true if p is large enough.

In another direction, Bourgain considered in [1] the question of the distribution of the values taken by a *sparse* polynomial formed by monomials which are, in some sense, sufficiently independent: for $a_1,\dots,a_d\in\mathbb{F}_p^*$,

$$\gcd(k_i,p-1),\gcd(k_i-k_j,p-1) < p^{1-\gamma} \Longrightarrow \Big|\sum_{x=1}^{p} e_p(a_1x^{k_1}+\cdots+a_dx^{k_d})\Big| < p^{1-\delta},$$

where $\delta=\delta(\gamma)>0$.

Bourgain also investigated in [2] a mixed question and showed that $I\cdot H := \{xh \mid x\in I,\ h\in H\}$ is ϵ-equidistributed modulo p if I is an interval of $\mathbb{F}_p$ of size $\geq p^\delta$ and H is a subgroup of $\mathbb{F}_p^*$ such that $|H| > (\log p)^A$ for some large A depending on the positive real numbers ϵ and δ. It means that $I\cdot H$ *becomes equidistributed* when p tends to infinity if one assumes more precisely that

$$\frac{\log|H|}{\log\log p}\to\infty. \tag{2}$$

In Section 2, we combine these two Bourgain statements and obtain a result (cf. Proposition 1) on equidistribution for sets $f(I)\cdot H$, where H is a subgroup of $\mathbb{F}_p^*$, I is an interval of $\mathbb{F}_p$, $|I|\geq p^\delta$ and f is a nonconstant polynomial.

Note that H is a coset of a subgroup of $\mathbb{F}_p^*$ if and only if $|H\cdot H|=|H|$. By relaxing this condition, namely if the doubling constant of H defined by $\sigma(H)=|H\cdot H|/|H|$ satisfies $\sigma(H)<K$ $(K>1)$, the Green-Ruzsa theorem (i.e. Freiman's theorem in arbitrary abelian groups) implies that H is well-structured (cf. [6]). In this paper, we will focus on such subsets of $\mathbb{F}_p^*$ with doubling constant $\sigma(H)<2$. In this restricted case, we will obtain more elaborated information from the famous Kneser theorem. It suggests the following definition: we say that a subset of $\mathbb{F}_p^*$ is an *approximate subgroup* if $|H\cdot H|<2|H|$. It is not difficult to see that Bourgain-Glibichuk-Konyagin's result (cf. [3]) quoted above can be easily extended to an approximate subgroup. In section 3, we show our main result (cf. Theorem 3) by extending Proposition 1 to the case where H is an approximate subgroup.

In the last section, we investigate the question of the existence of residues of a given small subgroup of $\mathbb{F}_p^*$ in the sumset $A+B$ for two arbitrary subsets of $\mathbb{F}_p$.

We stress the fact that Bourgain's condition (2) on the polylogarithmic size of H is essential in our proofs. By taking $p=2^q-1$ as a Mersenne prime, we can observe that the multiplicative subgroup H generated by 2 has cardinality $q=\log(p+1)/\log 2>\log p$. Nevertheless, H is not ϵ-distributed modulo p since $H\cap((p+1)/2,p)=\varnothing$. Moreover, if I is the interval $(1,2^{\delta q})$ in $\mathbb{F}_p^*$ with $0<\delta<1/2$, then $I\cdot\{2^j,\ 0\leq j\leq(1-\delta)q-1\}\subset(0,(p+1)/2)$. This implies that $|(I\cdot H)\cap((p+1)/2,p)|\leq 2^{\delta q}|I|=o(|I||H|)$; thus $I\cdot H$ is not ϵ-equidistributed when

p is large enough (assuming the Mersenne conjecture, which asserts that there are infinitely many Mersenne primes; see e.g. [5]).

These questions are related to results and problems quoted in [4].

In order to prove our results, we will argue by induction on the degree of f, on the back of Bourgain's result, using a squaring operation on trignometric sums and Kneser's theorem on the structure of small *doubling* sets in Abelian groups.

2. A result of asymptotic equidistribution for subgroups of $\mathbb{F}_p^*$

Let H be a subset of $\mathbb{F}_p^*$ and I be an interval of $\mathbb{F}_p$; that is

$$I = \{ax + b \pmod p \mid 0 \le x \le |I| - 1\}$$

for some $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. We also fix a polynomial f of degree ≥ 1. We first consider the question of equidistribution modulo p of the set of residues

$$f(I) \cdot H := \{f(z)h \mid z \in I,\ h \in H\}$$

as p tends to infinity. We prove

Proposition 1. *Let k be positive integer, c be a positive real number and $\epsilon, \delta \in (0, 1]$ be real numbers. Then there exist $p_0 = p_0(k, c, \epsilon, \delta)$, $A = A(k, c, \epsilon, \delta)$ such that for any prime $p \ge p_0$, any subgroup H^* of $\mathbb{F}_p^*$ with $|H^*| > (\log p)^A$, any $u \in \mathbb{F}_p^*$, any subset H of uH^* with $|H| > c|H^*|$, any interval $I \subset \mathbb{F}_p$ with $|I| \ge p^\delta$ and any $f(x) \in \mathbb{F}_p[x]$ with $\deg f = k$, one has*

$$\Big| \sum_{h \in H} \sum_{z \in I} e_p\big(hf(z)\big) \Big| \le \epsilon |H||I|.$$

For any $a \in \mathbb{F}_p^*$ and any subset X of $\mathbb{F}_p^*$, we denote

$$N(X, a, \gamma) := \big|\{x \in X \mid |ax|_p < p^{1-\gamma}\}\big|, \tag{3}$$

where $|x|_p$ means the unique nonnegative integer less than $p/2$ congruent to $|x|$ modulo p.

Let $\gamma > 0$. Our aim is to use Bourgain's result on the distribution of g^n modulo p, $n \ge 0$, where $g \in \mathbb{F}_p^*$ is fixed (cf. [2]). It implies that if the size of H^* is sufficiently large, namely

$$\frac{\log |H^*|}{\log \log p} > A_1,$$

where A_1 is a computable large constant in terms of ϵ, c and γ, then one has

$$\max_{a \in \mathbb{F}_p^*} N(H^*, a, \gamma) \le \frac{\epsilon c |H^*|}{2}$$

for any sufficiently large prime number p.

By assumption on H, we deduce that $\max_{a \in \mathbb{F}_p^*} N(H, a, \gamma) \le \frac{\epsilon |H|}{2}$.

We assume that $|I| \ge p^\delta$. Then for any integer $r \in (1, p-1)$, we have

$$T_r := \Big| \sum_{h \in H} \sum_{z \in I} e_p\big(rf(z)h\big) \Big| \le \epsilon |I||H|.$$

Indeed, we get for $f(z) = az + v$, $a \in \mathbb{F}_p^*$ and $v \in \mathbb{F}_p$,

$$\begin{aligned} T_r &\leq \sum_{h\in H} \Big| \sum_{z\in I} e_p\big(razh\big)\Big| \leq \sum_{h\in H} \min(|I|, \|arh/p\|^{-1}) \\ &\leq |I|N(H, ar, \gamma) + p^\gamma |H| \leq \epsilon |I||H|, \end{aligned} \tag{4}$$

if one chooses $\gamma = \delta/2$ and if p is large enough. By letting $A(1, c, \epsilon, \delta) = A_1$ we get the result for $k = 1$.

For a general nonconstant polynomial $f(x) \in \mathbb{Z}[x]$, we argue by induction on $k \geq 1$. For $k = 1$, it has been done above. Assume now that the property holds for some $k \geq 1$. Let f be of degree $k + 1$. By letting

$$S(h) = \sum_{z\in I} e_p(hf(z)),$$

we have

$$\sum_{h\in H} |S(h)|^2 = \sum_{h\in H} \sum_{x,y\in I} e_p(h(f(x) - f(y))) \leq |H||I| + 2\sum_{z\in I} \Big| \sum_{h\in H} \sum_{y\in I} e_p(hg_z(y))\Big|,$$

where $g_z(y) := f(y + z) - f(y)$ is a polynomial of degree k. By the inductive hypothesis, we get

$$\sum_{h\in H} |S(h)|^2 \leq 3\epsilon |H||I|^2.$$

Thus the set

$$H' := \{h \in H \mid |S(h)| > \epsilon^{1/3}|I|\}$$

has cardinality satisfying

$$\epsilon^{2/3}|H'||I|^2 < 3\epsilon |H||I|^2,$$

yielding $|H'| < 3\epsilon^{1/3}|H|$. It follows that

$$\begin{aligned} \Big| \sum_{h\in H} S(h)\Big| &\leq \sum_{h\in H'} |S(h)| + \sum_{h\in H\smallsetminus H'} |S(h)| \\ &\leq |H'||I| + |H|\epsilon^{1/3}|I| < 4\epsilon^{1/3}|I||H|. \end{aligned}$$

The result is proved.

We can derive from the proof that Proposition 1 holds uniformly for any polynomial of degree less than $k(\epsilon) = \frac{\log\log(1/\epsilon)}{\log 3}$.

3. Extension to approximate multiplicative subgroups

We recall that an *approximate* subgroup of $\mathbb{F}_p^*$ is any subset H of $\mathbb{F}_p^*$ such that $|H \cdot H| < 2|H|$. By Kneser's Theorem, we get the following structure for such a subset:

Lemma 2. *Let $\eta > 0$ and $H \subset \mathbb{F}_p^*$. If $|H \cdot H| < (2 - \eta)|H|$, then there exist a positive integer $m \leq 1/\eta$, a subgroup H^* of $\mathbb{F}_p^*$ and $u_1, \ldots, u_m \in H$ such that*

$$H \subset \bigcup_{i=1}^{m} u_i H^*$$

and

$$\frac{|H|}{m} \leq |H^*| \leq \frac{2 - \eta}{2m - 1}|H|.$$

We can now generalize Bourgain's result to an approximate subgroup by multiplying the image of an interval by a polynomial.

Theorem 3. *Let H be an approximate subgroup of $\mathbb{F}_p^*$ with size larger than polylogarithmic in p and let f be a polynomial. Then for any interval I in $\mathbb{F}_p$ of size p^δ, $f(I)\cdot H$ is equidistributed modulo p as p tends to infinity.*

Let $\epsilon, \delta, \eta > 0$ be positive real numbers and k be a positive integer. We assume that $|H\cdot H| \le (2-\eta)|H|$ and $|H| > (\log p)^B/\eta$, where $B = A(k, \epsilon\eta, \epsilon, \delta)$ is defined in Proposition 1. By the previous lemma, we may write

$$H = \bigcup_{i=1}^{m} H_i,$$

where $H_i = u_i H^* \cap H$, $i = 1, \dots, m$. Let

$$\Lambda = \{i \le m \mid |H_i| \le \epsilon |H^*|/m\}$$

and $\Lambda' = \{1, 2, \dots, m\} \smallsetminus \Lambda$.

For $j \in \Lambda'$, we have both $|H_j| > \epsilon|H^*|/m \ge \epsilon\eta|H^*|$ and $|H^*| \ge |H|/m > (\log p)^B$. Since Proposition 1 holds for cosets of a multiplicative subgroup as well, we obtain

$$\begin{aligned}\Big|\sum_{h\in H}\sum_{z\in I} e_p\big(hf(z)\big)\Big| &\le \sum_{i=1}^{m}\Big|\sum_{h\in H_i}\sum_{z\in I} e_p\big(hf(z)\big)\Big| \\ &\le \sum_{i\in\Lambda}|H_i||I| + \sum_{i\in\Lambda'}\epsilon|I||H_i| \\ &\le \epsilon|\Lambda||I||H^*| + \epsilon|I||H| \le 3\epsilon|I||H|.\end{aligned}$$

4. Remarks

It is worth mentioning that a close question related to multiplicative subgroups of $\mathbb{F}_p^*$ can be considered: is the equation $a+b=h$, $(a,b,h)\in A\times B\times H$ solvable for any subsets A, B of $\mathbb{F}_p$ and any subgroup of $\mathbb{F}_p^*$? Of course, A, B and H must be large enough in terms of p. This type of question takes its origin in [9] and has been heavily investigated since then (see e.g. [11], [10] and [8]).

By the use of Fourier analysis in $\mathbb{F}_p^*$ with ingredients of [11] (see also [10]), it can be shown that it is the case if

$$|A| > p^\epsilon, \quad |B| > p^{1/2+\epsilon}, \quad |H| > p^{1-\delta}, \tag{5}$$

where $\delta = \delta(\epsilon) > 0$. The proof runs as follows. The number of solutions of the equation $a+b=h$ is equal to

$$N = \frac{|A||B||H|}{p-1} + \frac{1}{p-1}\sum_{r=1}^{p-2}\sum_{(a,b)\in A\times B}\chi_r(a+b)\sum_{h\in H}\overline{\chi_r}(h),$$

where χ_r denotes the multiplicative character modulo p defined by

$$\chi_r(x) = \exp\left(\frac{2\pi i r\ \mathrm{ord}(x)}{p-1}\right),$$

and $\mathrm{ord}(x)$ denotes the discrete logarithm of x in base g for some fixed primitive root g modulo p. The summation on h is $|H|$ or 0 according to whether r divides $|H|$ or not. Hence

$$N = \frac{|A||B||H|}{p-1} + \frac{|H|}{p-1} \sum_{s=1}^{(p-1)/|H|-1} \sum_{(a,b)\in A\times B} \chi_{s|H|}(a+b).$$

By Shparlinski's result (cf. eq. 14 in [11]), the summation on (a,b) is $O(|A||B|p^{-\delta'})$ for any s; hence $N > 0$ by (5) if we consider $\delta < \delta'$ and p sufficiently large.

The same result with a stronger assumption on $|A|$ and $|B|$ and by relaxing the one on $|H|$ is a consequence of the corollary to Theorem 2.4 of [7]:

$$a + b = h \text{ is solvable if } \quad |A||B| > p^{2-\epsilon}, \quad |H| > p^{1/3+\delta},$$

where $\epsilon \to 0$ as $\delta \to 0$.

References

[1] Bourgain, J.; Mordell's exponential sum estimate revisited. *J. Amer. Math. Soc.* **18** (2005), no. 2, 477–499. MR2137982 (2006b:11099)

[2] Bourgain, J.; On the distribution of the residues of small multiplicative subgroups of $\mathbb{F}_p$. *Israel J. of Math.* **172** (2009), 61–74. MR2534239 (2010i:11017)

[3] Bourgain, J.; Glibichuk, A.; Konyagin S.; Estimate for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc.* **73** (2006), 380–398. MR2225493 (2007e:11092)

[4] Chang, M.-C.; Some problems in combinatorial number theory. *Integers* **8** (2008), no. 2, A1, 11 pp. MR2438286 (2009d:11015)

[5] Dickson, L.E.; History of the theory of numbers. Chelsea Publishing, New York, 1971.

[6] Green, B.J; Ruzsa, I.Z.; Freiman's theorem in an arbitrary abelian group. *J. London Math. Soc. (2)* **75** (2007), 163–175. MR2302736 (2007m:20087)

[7] Hegyvári, N.; Some remarks on multilinear exponential sums with an application. Preprint, 2010.

[8] Hegyvári, N.; Hennecart F.; Explicit construction of extractors and expanders, *Acta Arith.* **140** (2009), 233–249. MR2564464 (2010j:11017)

[9] Sárközy, A.; On sums and products of residues modulo p. *Acta Arith.* **118** (2005), 403–409. MR2165553 (2006f:11023)

[10] Shkredov, I.D., On monochromatic solutions of some non linear equations. Preprint (2009).

[11] Shparlinski, I.E.; On the solvability of bilinear equations in finite fields. *Glasg. Math. J.* **50** (2008), no. 3, 523–529. MR2451747 (2009j:11189)

[12] Tao, T; Vu, V.H.; Additive combinatorics. Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006. MR2289012 (2008a:11002)

Institute of Mathematics, Eötvös University, H-1117 Pázmány st. 1/c, Budapest, Hungary

E-mail address: hegyvari@elte.hu

Université de Lyon and Université Jean-Monnet, 23, rue Michelon, 42023 Saint-Étienne, France

E-mail address: francois.hennecart@univ-st-etienne.fr