An improved lower bound related to the Furstenberg-Sárközy theorem

Mark Lewko*

Department of Mathematics
University of California, Los Angeles
Los Angeles CA 90095–1555, U.S.A.

mlewko@gmail.com

Submitted: Sep 1, 2014; Accepted: Dec 31, 2014; Published: Feb 16, 2015
Mathematics Subject Classification: 05D10

Abstract

Let $D(n)$ denote the cardinality of the largest subset of the set $\{1, 2, \ldots, n\}$ such that the difference of no pair of elements is a square. A well-known theorem of Furstenberg and Sárközy states that $D(n) = o(n)$. In the other direction, Ruzsa has proven that $D(n) \gtrsim n^{\gamma}$ for $\gamma = \frac{1}{2}\left(1 + \frac{\log 7}{\log 65}\right) \approx 0.733077$. We improve this to $\gamma = \frac{1}{2}\left(1 + \frac{\log 12}{\log 205}\right) \approx 0.733412$.

1 Introduction

The following theorem, first conjectured by Lovász, was proven independently by Furstenberg [5] and Sárközy [14], [15], [16] around 1977:

Theorem 1. *Every subset of the natural numbers of positive upper density contains two distinct elements whose difference is a square.*

One can reformulate this theorem as follows. Let $D(n)$ be the cardinality of the largest subset of the set $\{1, 2, \ldots, n\}$ such that the difference of no pair of elements is a square. Then:

$$D(n) = o(n). \tag{1}$$

The best known quantitative form of (1) is the following bound of Pintz, Steiger, and Szemerédi [11] from 1988:

$$D(n) \lesssim n \frac{1}{(\log n)^{\frac{1}{4}\log\log\log n}}. \tag{2}$$

Erdős originally conjectured that $D(n) \lesssim x^{1/2}\log^{c}(x)$ for some positive constant c. This was disproved by Sárközy [15], who put forth the weaker conjecture that $D(n) \lesssim_{\epsilon} n^{1/2+\epsilon}$ for every $\epsilon > 0$. This was disproved by Ruzsa [12] in 1984. More precisely, he proved the following:

*This work was supported by a NSF postdoctoral fellowship, DMS-12042.

Theorem 2. *In the notation above,*

$$D(n) \gtrsim n^{\gamma}$$

where $\gamma = \frac{1}{2}\left(1 + \frac{\log 7}{\log 65}\right) \approx 0.733077.$

It is perhaps insightful to compare these results with the known progress on Roth's theorem. Let $R(n)$ denote the largest subset of $\{1, 2, \ldots, n\}$ that does not contain a (non-trivial) three term arithemetic progression. Roth's theorem states that $R(n) = o(n)$. The known proofs of Roth's and the Furstenberg-Sárköy theorem are based on very similar considerations, although the later case is somewhat simpler. For instance, see the recent proofs of Layla [8] and Tao, Green and Ziegler [17]. The best known quantitative form of Roth's theorem is due to Bloom [2] (see also Sanders [13]) and states that:

$$R(n) \lesssim n\frac{(\log\log n)^4}{\log n}. \tag{3}$$

In the other direction, an example of Behrend from 1946 shows that

$$R(n) \gtrsim n\frac{1}{2^{c\sqrt{\log n}}} \tag{4}$$

for some universal c. The nature of the constant c has been recently refined by Elkin [3] and Green and Wolf [7]. Note that both the known upper and lower bounds are considerably smaller for $D(n)$ than $R(n)$. Indeed, while Behrend's example rules out the possibility of extending Roth's theorem to polynomial sparse sets (in other words, obtaining a power savings in the estimate (3)), such a possibility has not been ruled out in the context of the Furstenberg-Sárköy theorem (1).

The purpose of the current work is to obtain a slight improvement to Ruzsa's Theorem 2. More specifically, we prove the following theorem:

Theorem 3. *In the notation above,*

$$D(n) \gtrsim n^{\gamma}$$

where $\frac{1}{2}\left(1 + \frac{\log 12}{\log 205}\right) \approx 0.733412.$

More generally, let $D_k(n)$ denote the cardinality of the largest subset of $\{1, 2, \ldots, n\}$ such that the difference of no pair of elements is a k-th power. Thus $D(n) = D_2(n)$. With this notation, Ruzsa also obtained $D_3(n) \gtrsim n^{\gamma_3}$ for $\gamma_3 = \frac{2}{3} + \frac{\log 3}{3\log 7} \approx 0.854858$. We are also able to slightly improve this as follows.

Theorem 4. *In the notation above,*

$$D_3(n) \gtrsim n^{\gamma_3}$$

where $\gamma_3 = \frac{2}{3} + \frac{\log 14}{3\log 91} \approx 0.861681.$

The proofs of Theorems 2, 3 and 4 are based on an observation of Ruzsa which states roughly (see Lemma 5) that if one can find a square-free natural number m and a large subset A of the residue mod m such that the difference of no two distinct elements in A is a square mod m, then one can use this example to construct a large subset B of $\{1, 2, \ldots, N\}$ such that the difference of no two distinct elements of B is an integral square. Using this lemma, Ruzsa proved Theorem 2 by exhibiting an explicit set of 7 residues mod 65 with the desired property. Our proof of Theorem 3 will follow by exhibiting an explicit set of 12 residues mod 205. Similarly, our proof of Theorem 4 is based on a set of 14 residues mod 91.

2 Ruzsa's Lemma

Our starting point is the following result of Ruzsa [12].

Lemma 5. *Let m denote a square-free positive integer, and let $r_k(m)$ denote the maximal number of residues mod m such that the difference of no two such elements is a k-th power residue. Moreover, define*

$$\gamma(k, m) := 1 - \frac{1}{k} + \frac{\log r_k(m)}{k \log(m)}.$$

Then,

$$D_k(x) \geqslant \frac{x^{\gamma(k,m)}}{m}.$$

3 Proof of Theorem 3

Given lemma 5, it suffices to demonstrate a set A of 12 residues mod 205 whose difference set (the set of pairwise differences, $A - A$) contains no square. We claim that

$$\{7, 21, 50, 64, 76, 83, 106, 120, 139, 182, 193, 199\}$$

is such a set. Indeed, to enable the reader to independently verify this for herself, Table 1 shows the difference set of A. More specifically, the element in the row labeled i and column labeled j is the value $i - j$ mod 205. One may the check this against the following list of squares mod 205:

$$\{0, 1, 4, 5, 9, 10, 16, 20, 21, 25, 31, 36, 39, 40, 41, 45, 46, 49, 50, 51, 59,$$

$$61, 64, 66, 74, 80, 81, 84, 86, 90, 91, 100, 105, 114, 115, 119, 121, 124,$$

$$125, 131, 139, 141, 144, 146, 154, 155, 156, 159, 160, 164, 165, 166,$$

$$169, 174, 180, 184, 185, 189, 195, 196, 200, 201, 204\}.$$

	7	21	50	64	76	83	106	120	139	182	193	199
7	0	191	162	148	136	129	106	92	73	30	19	13
21	14	0	176	162	150	143	120	106	87	44	33	27
50	43	29	0	191	179	172	149	135	116	73	62	56
64	57	43	14	0	193	186	163	149	130	87	76	70
76	69	55	26	12	0	198	175	161	142	99	88	82
83	76	62	33	19	7	0	182	168	149	106	95	89
106	99	85	56	42	30	23	0	191	172	129	118	112
120	113	99	70	56	44	37	14	0	186	143	132	126
139	132	118	89	75	63	56	33	19	0	162	151	145
182	175	161	132	118	106	99	76	62	43	0	194	188
193	186	172	143	129	117	110	87	73	54	11	0	199
199	192	178	149	135	123	116	93	79	60	17	6	0

Table 1: The difference set of A

4 Proof of Theorem 4

Again using lemma 5, it suffices to demonstrate a set A of 14 residues mod 91 whose difference set (the set of pairwise differences, $A - A$) contains no cube. We claim that

$$\{3, 19, 23, 25, 29, 35, 41, 47, 66, 72, 78, 84, 88, 90\}$$

is such a set. The difference set mod 91 is as follows.

	3	19	23	25	29	35	41	47	66	72	78	84	88	90
3	0	75	71	69	65	59	53	47	28	22	16	10	6	4
19	16	0	87	85	81	75	69	63	44	38	32	26	22	20
23	20	4	0	89	85	79	73	67	48	42	36	30	26	24
25	22	6	2	0	87	81	75	69	50	44	38	32	28	26
29	26	10	6	4	0	85	79	73	54	48	42	36	32	30
35	32	16	12	10	6	0	85	79	60	54	48	42	38	36
41	38	22	18	16	12	6	0	85	66	60	54	48	44	42
47	44	28	24	22	18	12	6	0	72	66	60	54	50	48
66	63	47	43	41	37	31	25	19	0	85	79	73	69	67
72	69	53	49	47	43	37	31	25	6	0	85	79	75	73
78	75	59	55	53	49	43	37	31	12	6	0	85	81	79
84	81	65	61	59	55	49	43	37	18	12	6	0	87	85
88	85	69	65	63	59	53	47	41	22	16	10	4	0	89
90	87	71	67	65	61	55	49	43	24	18	12	6	2	0

One may check this against the following list of cubes mod 91:

$$\{0, 1, 8, 13, 14, 21, 27, 34, 57, 64, 70, 77, 78, 83, 90\}.$$

5 Further remarks

In light of lemma 5, it is tempting to computationally search of favorable sets of residues. Indeed, this is how we found those presented above. We were able to exhaustively check all moduli (strictly) less than 533 with a brute-force search. This took about a month of computing time on a modern desktop computer. Given a square-free modulus m the problem of finding the largest subset whose difference set contains no squares is equivalent to the problem of finding the maximal clique in a dense graph. In complete generality, this problem is known to be NP complete. There are, however, non-trivial algorithms available for this problem. Using the graph algorithm of Konc and Janezic [9] implemented in C by Konc [10] we were able to extend this range up to $m \leqslant 733$. Indeed, the set of 12 residues mod 205 given below gives the optimal result among sets within this range.

It is natural to ask what the limitations of this method are. As above, let $r_2(m)$ denote the cardinality of the largest set of residues mod m whose difference set does not contain a square. It is well known (see [4], for instance) that $r_2(p) \leqslant p^{1/2}$ for all primes p. Ruzsa has conjectured that $r_2(m) \leqslant m^{1/2}$ for square-free m. This would imply that $\gamma \leqslant \frac{3}{4}$ would be the limitation of this method. Ruzsa's conjecture remains open; indeed it does not seem to be known if there exists a $\delta > 0$ such that $r_2(m) \leqslant m^{1-\delta}$ for all square-free m. We note that the paper [5] claims the inequality $r_2(m) \lesssim_\epsilon m^{1/2+\epsilon}$ for square-free m, however the referee of this note has pointed out that the proof presented there contains a serious error.

It is unclear, at least to the author, what one should expect the true order of $D(n)$ to be.

References

[1] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression. Proc. Nat. Acad. Sci. U. S. A., 32:331–332, 1946.

[2] T. Bloom, A quantitative improvement for Roth's theorem on arithmetic progressions, Preprint, 2014. arXiv:1405.5800

[3] M. Elkin, An improved construction of progression-free sets. Israel J. Math. 184 (2011), 93–128.

[4] J. Fabrykowski, On maximal residue difference sets modulo p. Canad. Math. Bull. 36 (1993), no. 2, 144–146.

[5] J. Fabrykowski, On quadratic residues and nonresidues in difference sets modulo m. Proc. Amer. Math. Soc. 122 (1994), no. 2, 325–331.

[6] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions, J. d'Analyse Math. 31 (1977), 204–256.

[7] B. Green and J. Wolf, A note on Elkin's improvement of Behrend's construction. Additive number theory, 141–144, Springer, New York, 2010.

[8] N. Lyall, A new proof of Sárközy's theorem. Proc. Amer. Math. Soc. 141 (2013), no. 7, 2253–2264.

[9] J. Konc and D. Janezic, An improved branch and bound algorithm for the maximum clique problem. MATCH Commun. Math. Comput. Chem., 2007, 58, 569–590.

[10] J. Konc, Maximum Clique Algorithm. http://www.sicmm.org/~konc/maxclique/

[11] J. Pintz, W. L. Steiger, E. Szemerédi, On sets of natural numbers whose difference set contains no squares, J. London Math. Soc. 37 (1988), 219–231.

[12] I. Ruzsa, Difference sets without squares. Period. Math. Hungar. 15 (1984), no. 3, 205–209.

[13] T. Sanders, On Roth's theorem on progressions. Ann. of Math. (2) 174 (2011), no. 1, 619–636.

[14] A. Sárközy, On difference sets of integers I, Ada Math. Acad. Sci. Hungar. 31 (1978) 125–149.

[15] A. Sárközy, On difference sets of integers II, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 21 (1978), 45–53.

[16] A. Sárközy, On difference sets of sequences of integers. III. Acta Math. Acad. Sci. Hungar. 31 (1978), no. 3-4, 355–386.

[17] T. Tao, A Fourier-free proof of the Furstenberg-Sarkozy theorem. http://terrytao.wordpress.com/2013/02/28/a-fourier-free-proof-of-the-furstenberg-sarkozy-theorem