Sumsets being squares

Andrej Dujella, Christian Elsholtz

March 4, 2013

Abstract

Alon, Angel, Benjamini and Lubetzky recently studied an old problem of Euler on sumsets for which all elements of $A + B$ are integer squares. Improving their result we prove:

1. There exists a set A of 3 positive integers and a corresponding set $B \subset [0, N]$ with $|B| \gg (\log N)^{15/17}$, such that all elements of $A + B$ are perfect squares.
2. There exists a set A of 3 integers and a corresponding set $B \subset [0, N]$ with $|B| \gg (\log N)^{9/11}$, such that all elements of the sets A, B and $A + B$ are perfect squares.

The proofs make use of suitably constructed elliptic curves of high rank.

1 Introduction

Let A and B be sets of integers. In this paper we study the size of sumsets $A+B = \{a+b : a \in A, b \in B\}$ being a subset of the set of integer squares S. Let us briefly review what is known: If $|A| = 2$, then the size of $|B|$ is bounded by a divisor function. This means, that $|B|$ is finite, but depending on A can be arbitrarily large: if $A, B \subset [1, N]$, then $|B| \leq \exp\left((\log 2 + o(1))\frac{\log N}{\log\log N}\right)$.

This connection to the number of divisors can be seen as follows: $a_1+b_i = x_i^2, a_2+b_i = y_i^2$. $a_2 - a_1 = y_i^2 - x_i^2 = (y_i - x_i)(y_i + x_i)$. Thus, if $a_2 - a_1 = d_1d_2$ (say), with $d_1 \leq d_2$, then $x_i = \frac{d_2-d_1}{2}, y_i = \frac{d_1+d_2}{2}$. Hence the number of possible values of b_i corresponds to the number of divisors of $a_2 - a_1$. The

2010 Mathematics Subject Classification: Primary 11P70, Secondary: 11B75, 11G05.
Key words: sumsets, squares, elliptic curves of high rank.

bound follows from the well known upper bound on the values of divisor functions, due to Wigert [20].

Recently Alon, Angel, Benjamini and Lubetzky [1] studied the case of larger $|A|$. They proved: There exists a set A of 3 elements and a corresponding set $B \subset [-N, N]$ with $|B| \gg (\log N)^{5/7}$.

If $|A| \geq 4$ they observed that a result of Caporaso, Harris and Mazur says, that, assuming the deep Bombieri-Lang conjecture on curves of genus $g > 1$, the size of $|B|$ is uniformly bounded. A related observation was made by Solymosi [19].

Alon et al. also point out that the question of sumsets in the set of squares has already been studied by Euler. This should serve as a motivation to study the problem. On the other hand Alon et al. apply the results to questions from additive combinatorics, on sums and products, (for details we refer to their Theorem 2(3)). For further literature on the question of sumsets in the set of integer squares we refer to [2, 3, 5, 6, 12, 13, 17, 18].

In this note we improve the above mentioned lower bound by Alon et al.

Theorem 1.1. *There exists a set A of 3 positive integers and a corresponding set $B \subset [0, N]$ with $|B| \gg (\log N)^{15/17}$, such that all elements of $A + B$ are perfect squares.*

Note that $\frac{15}{17} = 0.882\ldots$ and that $\frac{5}{7} = 0.714\ldots$.

Proof. We follow Alon et al. [1, Section 4]. Their construction starts with rational squares a_1, a_2 and a_3, (so that $X = 0$ is one solution of the system $Y_i^2 = X + a_i$). They define

$$\alpha = \frac{-\sum_i a_i^2 + \sum_{i<j} a_i a_j}{3a_3^2}, \quad \beta = \frac{2\sum_i a_i^3 - 3\sum_{i\neq j} a_i^2 a_j + 12 a_1 a_2 a_3}{27 a_3^3},$$

and consider the elliptic curve

$$E : \ y^2 = x^3 + \alpha x + \beta.$$

Using properties of the canonical height of elliptic curves, they showed that if $\mathrm{rank}\,(E(\mathbb{Q})) = r$, then for $A = \{a_1', a_2', a_3'\}$, where the a_i'-s are square multiples of the a_i-s, there exists a set B such that $A + B \subset S$, $B \subset [-N, N]$ and $|B| \gg (\log N)^{r/(r+2)}$. By taking $a_1 = 3^2, a_2 = 34^2, a_3 = 89^2$ (there is a misprint in [1]: they write $a_1 = 3, a_2 = 34, a_3 = 89$), they obtain the curve of rank 5, and so the exponent $5/7$.

Let us observe that the curve E has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The largest known rank for curves with such torsion is 15, and the corresponding curve was found by Elkies in 2009 [10] (see [8] for details on the

curve). By translating Elkies' curve to the form of [1, Section 4], we get $a_1 = 943498641882610^2$, $a_2 = 301995932074265^2$, $a_3 = 3677942688600458^2$, with the corresponding elliptic curve with rank 15. Hence, we conclude that for a set of the form

$$A = \{943498641882610^2t^2, 301995932074265^2t^2, 3677942688600458^2t^2\},$$

there exists a set $B \subset [-N, N]$ with $|B| \gg (\log N)^{15/17}$, such that all elements of $A + B$ are perfect squares.

We now show that one can even take $B \subset [0, N]$.

Let A be a set of 3 integers, as defined above, with $a_1 < a_2 < a_3$ and $B \subset [-N, N]$ such that $A + B$ consists of positive integer squares. Note that the elements of A are positive by construction.

As $0 < a_1 < a_2 < a_3$ the least element b_1 of B is larger than $-a_1$, and we make the following translation: $A' = A-(a_1-1) = \{1, a_2-a_1+1, a_3-a_1+1\}$, $B' = B + (a_1 - 1)$. Note that $A + B = A' + B'$ and that all elements of A' and B' are nonnegative. □

2 Elements of A and B are also squares

In this section we consider a variant of "sumsets being squares" problem, where the elements of the sets A and B are also squares. Actually, there is no loss of generality in assuming that one of the sets, say A, consists of squares, since we may assume, by translation, that $0 \in B$. Thus, in the examples given in the previous section, the set A contains three squares. But now we will impose the additional condition that B also contains only squares. This problem is related to Pythagorean triples, and certain problems of placing points in the plane at integer distances, e.g. a problem of Erdős and Rosenfeld [11] (see also [14]).

Again, we will take a set A with $|A| = 3$ and ask how large a set $B \subset [0, N]$ with the required properties can be. Since B contains only squares, we may take $a_1 = 0$, $a_2 = c_2^2$, $a_3 = c_3^2$. Now, any element $b \in B$ is the x-coordinate of a point on the elliptic curve

$$E' : \ y^2 = x(x + c_2^2)(x + c_3^2).$$

Moreover, for points $(x, y) \in 2E'(\mathbb{Q})$ the value $x + a_i$ is a rational square for $i = 1, 2, 3$. It is well known that elliptic curves of this form are exactly elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (note that $(0, 0) \in 2E'(\mathbb{Q})$, more precisely $(0, 0) = 2(c_2c_3, c_2c_3(c_2 + c_3)$, so the point $(c_2c_3, c_2c_3(c_2 + c_3)$

is of order 4). The largest known rank for such curves is 9, given by the example found recently by Dujella and Peral (see [8, 9]):

$$\begin{aligned} y^2 &= x^3 + x^2 - 614100573770591167151980664421796984 0x \\ &\quad + 585743317734880315858628578592963147780809517115906318 8. \end{aligned}$$

This example, by the translation, gives $a_1 = 0$, $a_2 = 28678999^2$, $a_3 = 43105370^2$. By applying again the results of [1, Section 4], we obtain the following result.

Theorem 2.1. *There exists a set A of 3 integers and a corresponding set $B \subset [0, N]$ with $|B| \gg (\log N)^{9/11}$, such that all elements of the sets A, B and $A + B$ are perfect squares.*

Note that $\frac{9}{11} = 0.818...$.

Remark 2.2. The above curve with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank 9 is induced by a Diophantine triple, i.e. a set of three non-zero rationals with the property that the product of any two of them increased by 1 is a perfect square. Thus, the curve has the form

$$y^2 = (ax + 1)(bx + 1)(cx + 1),$$

where $ab + 1$, $ac + 1$ and $bc + 1$ are perfect squares. In [7], it was shown that if

$$a = \frac{\alpha T + 1}{T - \alpha},\ b = \frac{\alpha - T}{\alpha T + 1},\ c = \frac{4\alpha T}{(\alpha T + 1)(T - \alpha)},$$

then the curve has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and positive rank. By finding subfamilies with higher rank and the sieving based on the Mestre-Nagao sums, in [9], the parameters $\alpha = -1997/3434$, $T = 83/136$ were detected as corresponding to potentially large rank, and Cremona's program `mwrank` [4] gave that the rank is equal to 9.

Acknowledgement

A. Dujella was supported by the Ministry of Science, Education, and Sports, Republic of Croatia, grant 037-0372781-2821. C. Elsholtz acknowledges partial support by the Austrian Science Fund (FWF), P24574 and W1230.

References

[1] N. Alon, O. Angel, I. Benjamini and E. Lubetzky, Sums and products along sparse graphs, *Israel J. Math.*, **188** (2012), 353–384.

[2] Y. Bugeaud and K. Gyarmati, On generalizations of a problem of Diophantus, *Illinois J. Math.*, **48** (2004), no. 4, 1105–1115.

[3] P. Csikvári, Subset sums avoiding quadratic nonresidues, *Acta Arith.*, **135** (2008), no. 1, 91–98.

[4] J. Cremona, Algorithms for Modular Elliptic Curves. Cambridge University Press, Cambridge, 1997.

[5] R. Dietmann and C. Elsholtz, Hilbert cubes in progression-free sets and in the set of squares, *Israel J. Math.*, **192** (2012), 59–66.

[6] R. Dietmann and C. Elsholtz, Hilbert cubes in progression-free sets and in the set of squares II, preprint.

[7] A. Dujella, On Mordell-Weil groups of elliptic curves induced by Diophantine triples, *Glas. Mat. Ser. III*, **42** (2007), 3–18.

[8] A. Dujella, High rank elliptic curves with prescribed torsion, `http://web.math.hr/∼duje/tors/tors.html`

[9] A. Dujella and J. C. Peral, High rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples, preprint.

[10] N. D. Elkies, Personal communication, 2009.

[11] P. Erdős and M. Rosenfeld, The factor-difference set of integers, *Acta Arith.*, **79** (1997), 353–359.

[12] K. Gyarmati, On a problem of Diophantus, *Acta Arith.*, **97** (2001), no. 1, 53–65.

[13] K. Gyarmati, A. Sárközy and C. L. Stewart, On sums which are powers. *Acta Math. Hungar.*, **99** (2003), no. 1-2, 1–24.

[14] J. Jiménez-Urroz, A note on a conjecture of Erdős and Rosenfeld, *J. Number Theory*, **78** (1999), 140–143.

[15] J.-F. Mestre, Construction de courbes elliptiques sur $\mathbb{Q}$ de rang ≥ 12, *C. R. Acad. Sci. Paris*, Ser. I **295** (1982), 643–644.

[16] K. Nagao, An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20, *Proc. Japan Acad. Ser. A Math. Sci.*, **69** (1993), 291–293.

[17] J. Rivat, A. Sárközy and C.L. Stewart, Congruence properties of the Ω-function on sumsets, *Illinois J. Math.*, **43** (1999), no. 1, 1–18.

[18] A. Sárközy, On additive decompositions of the set of quadratic residues modulo p, *Acta Arith.*, **155** (2012), 41–51.

[19] J. Solymosi, Elementary Additive Combinatorics. In "Additive Combinatorics", CRM Proceedings & Lecture Notes, vol. 43 (2007), 29–38.

[20] S. Wigert, Sur l'ordre de grandeur du nombre des diviseurs d'un entier, *Arkiv for matematik, astronomi och fysik*, **3** (1907), no. 18, 1-9.

Andrej Dujella,
Department of Mathematics, University of Zagreb,
Bijenička cesta 30, 10000 Zagreb, Croatia
email: duje@math.hr

Christian Elsholtz,
Institut für Mathematik A, Technische Universität Graz,
Steyrergasse 30/II, A-8010 Graz, Austria
email: elsholtz@math.tugraz.at