SIDON SETS

ARMANBYEK SOLTANMURAT

Abstract. We provide both upper and lower bounds for Sidon sets. First, we establish an upper bound for Sidon subsets of the set $\{1, \ldots, n\}$. Then, using a specific construction, we demonstrate the existence of a Sidon set of size $p-1$ for a prime p. This construction also allows us to derive a lower bound for Sidon sets consisting of prime numbers less than n.

1. Introduction

Definition 1.1. A subset $S \subseteq \mathbb{N}$ is called a *Sidon set* if for all $a, b, c, d \in S$, the equation $a + b = c + d$ implies that $\{a, b\} = \{c, d\}$. In other words, all pairwise sums of elements in S are distinct.

Let $s(n)$ denote the maximum number of elements in a Sidon subset of $\{1, \ldots, n\}$. We now give upper and lower bounds for $s(n)$.

Theorem 1.2. *Let $S \subseteq \{1, \ldots, n\}$ be a Sidon set and let $s(n) = |S|$. Then*

$$s(n) < \sqrt{n} + \sqrt[4]{n} + 1.$$

Proof. The following proof is taken from Erdős and Surányi's book, *Topics in the Theory of Numbers* [1]. We divide the interval $[0, n]$ into $n + t$ subintervals as follows:

$$[-t + 1, 0], [-t + 2, 1], \ldots, [n, n + t - 1].$$

Assume that $A_1, \ldots, A_{n+t}$ are the number of elements from the Sidon set S that fall into these intervals. That is, $A_i = |S \cap [i - t, i - 1]|$. For each element $s \in S$, it appears in exactly t consecutive intervals. Therefore, $\sum_{i=1}^{n+t} A_i = ts$. We now count the number D of pairs $(a_i, a_j$ with $i > j$ which fall in the above intervals. Clearly,

$$D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \frac{1}{2} \sum_{i=1}^{n+t} A_i^2 - \frac{1}{2} \sum_{i=1}^{n+t} A_i$$

Date: May 18, 2025.

On the other hand, if the difference of a pair of elements is $a_i - a_j = d$, then this pair falls within $t - d$ intervals. Since the differences of pairs from Sidon set are distinct, then each d can occur at most once. Hence,

$$D \leq \sum_{d=1}^{t-1} (t-d) = \frac{t(t-1)}{2}$$

Comparing the above two results, we get

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \leq t(t-1) \tag{1}$$

By Cauchy-Schwartz inequality, we have

$$\sum_{i=1}^{n+t} A_i^2 \geq \frac{\left(\sum_{i=1}^{n+t} A_i\right)^2}{n+t} = \frac{t^2 s^2}{n+t}$$

Substituting into inequality (1) and multiplying by $\frac{n+t}{t^2}$ both sides, we get:

$$s^2 - s\left(\frac{n}{t} + 1\right) - \left(\frac{n}{t} + 1\right)(t-1) \leq 0$$

For the values of s satisfying this second-degree inequality, we have

$$\begin{aligned} s &\leq \frac{n}{2t} + \frac{1}{2} + s(n+t) + \frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4} \\ &= \frac{n}{2t} + \frac{1}{2} + s(n+t) + \left(\frac{n}{2t} - \frac{1}{2}\right)^2 - 1 \end{aligned} \tag{2}$$

We now choose $t = \sqrt[4]{n^3} + 1$, then the first term on the right-hand side is less than $\frac{1}{2}\sqrt[4]{n}$, while the last term is less than the square of $\sqrt{n} + \frac{1}{2}\sqrt[4]{n} + \frac{1}{2}$.

□

To give a lower bound, we present two clever constructions. Consider a modified version of Erdős and Turán's construction [2].

Theorem 1.3. *There exists a Sidon set $S \subseteq \{1, \ldots, n\}$ such that*

$$|S| \geq \frac{\sqrt{n}}{4}.$$

Another construction due to Ruzsa [3] improves the constant $\frac{1}{4}$.

Theorem 1.4. *Let p be a prime number. Then there exists a Sidon set in the set $\mathbb{Z}_{p^2-p}$ with exactly $p-1$ elements.*

Proof. Let g be a primitive element modulo p. Consider the following system of congruences:

$$\begin{cases} x \equiv i \pmod{p-1}, \\ x \equiv g^i \pmod{p}. \end{cases}$$

By the Chinese Remainder Theorem, this system has a unique solution modulo $p^2 - p$. Denote this solution by a_i. We will show that the elements $a_1, \ldots, a_{p-1}$ form a Sidon set modulo $p^2 - p$. In other words, the congruence

$$a_i + a_s \equiv a_r + a_j \pmod{p^2 - p}$$

has only trivial solutions where $\{a_i, a_s\} = \{a_r, a_j\}$. This means there is for any c there is exactly one i and j such that

$$c \equiv a_i + a_j \pmod{p^2 - p}$$

Due to the condition of a_i, we have

$$\begin{cases} c \equiv i + j \pmod{p-1}, \\ c \equiv g^i + g^j \pmod{p}. \end{cases}$$

By Fermat's little theorem, we have

$$g^c \equiv g^i g^j \pmod{p}$$

from the first congruence. We now consider the quadratic equation

$$(x - g^i)(x - g^j) = x^2 - (g^i + g^j)x + g^{i+j} \equiv x^2 - cx + g^c \pmod{p}.$$

This implies that the residue classes $(g^i)_p$ and $(g^j)_p$ are uniquely defined since these are the roots of the quadratic equation.

By assigning a congruent natural number to each residue class mod $(p^2 - p)$, we may get a Sidon set in $\{1, 2, \ldots, p^2 - p\}$. Thus, if n is of the form $p^2 - p$, we see that

$$S(n) \geq p - 1 = \frac{1}{2}(\sqrt{4n+1} - 1) > \sqrt{n} - 1.$$

□

Continuing this process, we give a lower bound for a Sidon set that contains only primes less than n. Denote it by $S(\mathbb{P})$. Let $\mathbb{P}$ be the set of prime numbers, and let $\mathbb{A} \subset \mathbb{Z}_{p^2-p}$ be a Sidon set with $p - 1$ elements, as constructed above. For $c \in \mathbb{Z}_{p^2-p}$, define the shifted set

$$\mathbb{A} + c := \{a + c : a \in \mathbb{A}\}.$$

Then $\mathbb{A}+c \subset \mathbb{Z}_{p^2-p}$ and is also a Sidon set. Therefore, we obtain p^2-p Sidon sets in $\mathbb{Z}_{p^2-p}$, namely:

$$\mathbb{A},\ \mathbb{A}+1,\ \ldots,\ \mathbb{A}+(p^2-p-1).$$

Every prime $q \in \mathbb{P}$ appears in exactly $p-1$ of these sets. Thus,

$$\sum_{c\in\mathbb{Z}_{p^2-p}} |(\mathbb{A}+c)\cap\mathbb{P}| = |\{(q,c) : q \in (\mathbb{A}+c)\cap\mathbb{P}\}| = \pi(p^2-p)\cdot(p-1) \approx \frac{(p^2-p)(p-1)}{\log(p^2-p)},$$

where we have used the Prime Number Theorem approximation $|\mathbb{P} \cap [1, p^2-p]| \approx \frac{p^2-p}{\log(p^2-p)}$.

By the pigeonhole principle, there exists some $i \in \mathbb{Z}_{p^2-p}$ such that

$$|(\mathbb{A}+i)\cap\mathbb{P}| \geq \frac{p-1}{\log(p^2-p)}.$$

Since $p^2-p \leq n$, it follows that

$$p \leq \frac{1}{2} + \sqrt{n+\frac{1}{4}}.$$

On the other hand, by a result of Baker, Harman and Pintz [4], for sufficiently large n, there exists a prime between N and $N+N^{\delta}$, where $\delta = 0.525$. Applying this result with $N = \sqrt{n}$, we can choose a prime p such that

$$\sqrt{n} - n^{0.2625} < p \leq \sqrt{n}.$$

Therefore, we can express the right-hand side in terms of n as follows:

$$|(\mathbb{A}+i)\cap\mathbb{P}| \geq \frac{\sqrt{n}-n^{0.2625}}{\log n}.$$

We are currently trying to obtain a non-trivial upper bound for Sidon sets containing only primes which is subset of $\{1, 2, \ldots, N\}$.

References

[1] P. Erdős, J. Surányi, *Topics in the Theory of Numbers*, 2003 Edition, Springer, Undergraduate Texts in Mathematics.
[2] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory and related problems*, Journal of the London Mathematical Society 16 (1941), 212–215.
[3] I. Z. Ruzsa, *Solving a linear equation in a set of integers*, Acta Arithmetica 65 (1993), 259–282.
[4] R. C. Baker, G. Harman, J. Pintz, *The difference between con- secutive primes*, II, Proceedings of the London Mathematical Society. 83 (3) (2001), 532–562.