Sidon Sets

Armanbyek Soltanmurat

ELTE

June 5, 2025

What is a Sidon Set?

Definition

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.

Theorem

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

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

What is lower bound?

Theorem

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

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 of CRT-based Sidon Set

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 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, this means there is, for any c, 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

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

Proof.

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 $\bmod(p^2 - p)$, 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

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

Question

What is a lower bound for a Sidon set that contains only primes less than n?

Answer

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

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

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,

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

Answer

There exists some $i \in \mathbb{Z}_{p^2-p}$ such that

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

By a result of Baker, Harman and Pintz [4], for sufficiently large n, there exists a prime between N and $N + N^{\delta}$, where $\delta = 0.525$. Hence, 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:

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

References I

- P. Erdős, J. Surányi, *Topics in the Theory of Numbers*, 2003 Edition, Springer, Undergraduate Texts in Mathematics.
- 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.
- I. Z. Ruzsa, *Solving a linear equation in a set of integers*, Acta Arithmetica 65 (1993), 259–282.
- R. C. Baker, G. Harman, J. Pintz, *The difference between consecutive primes*, II, Proceedings of the London Mathematical Society. 83 (3) (2001), 532–562.