Studia Scientiarum Mathematicarum Hungarica 38 (2001), 367–375

AN ALMOST POLYNOMIAL SIDON SEQUENCE

I. Z. RUZSA

Abstract

It is a classical unsolved problem whether there is a polynomial with integral coefficients whose values at natural numbers form a Sidon set. In this note we prove the existence of a polynomial of degree 5, with real coefficients, such that the integer parts of the values form a Sidon set.

1. Introduction

A *Sidon set* is a set of integers with the property that the pairwise sums of elements are all distinct. It is conjectured that there is a polynomial with integer coefficients whose values at natural numbers form a Sidon set (Guy [1], F30 attributes this question to Erdős). Indeed, $f(x)=x^5$ may have this property (see [1], D1). However, this polynomial has the property that if there is a nontrivial solution of $f(x)+f(y)=f(u)+f(v)$ in integers, then by homogeneity there are arbitrarily large solutions, so a nonhomogeneous polynomial may be a safer bet. It is known that for $f(x)=x^4$ the corresponding equation has many solutions (Swinnerton-Dyer [3]).

In this note we find examples from somewhat larger class of functions.

Theorem 1. *There is a real number $\xi\in[0,1]$ such that the set*

$$A=\{n^5+[\xi n^4]:n>n_0\}$$

is a Sidon set for a suitable constant n_0.

Theorem 1 is a special case of the following more general one.

Theorem 2. *Let α, β be real numbers satisfying*

$$\alpha>4,\qquad \alpha>\beta>3+1/(\alpha-1). \tag{1.1}$$

2000 *Mathematics Subject Classification.* Primary 11B75; Secondary 11B34, 11K45, 05B10.

Key words and phrases. Sidon sets, random construction.

Supported by Hungarian National Foundation for Scientific Research Grants No. T 25617 and T 29759.

0081–6906/2001/$ 5.00

Write

$$f(n)=[n^{\alpha}+\xi n^{\beta}]. \tag{1.2}$$

For almost all $\xi\in[0,1]$ there is an n_0 (depending on α,β,ξ) such that the set

$$A=\{f(n):n>n_0\} \tag{1.3}$$

is a Sidon set.

2. Estimation of the probability

We assume that α,β are fixed real numbers satisfying (1.1). The Sidon property of the set A defined in (1.3) depends on the solutions of the equation

$$f(x)+f(y)=f(u)+f(v). \tag{2.1}$$

For given x,y,u,v equation (2.1) may or may not hold for different values of ξ. We will use $\mathbf{P}(\dots)$ to denote probability (which in our case simply means the measure of $\xi\in[0,1]$ having the property in parentheses). We are going to estimate

$$\mathbf{P}(f(x)+f(y)=f(u)+f(v)).$$

In the sequel, to avoid the distinction of subcases, we will apply the symbol $\asymp$ in a slightly extended sense; we will write $F\asymp G$ if F/G stays between positive constants, except those values where $F=G=0$.

Lemma 2.1. *For a given $\gamma>0$ we have*

$$a^{\gamma}-b^{\gamma}\asymp a^{\gamma-1}(a-b)=a^{\gamma}(1-b/a) \quad \textit{for } a\geqq b\geqq 0, \tag{2.2}$$

where the implied constants depend on γ but not on a,b.

Proof. For $0\leqq b<a/2$ both sides have the same order of magnitude as a^{γ}, for $a/2\leqq b<a$ we apply the mean value theorem and for $b=a$ both sides vanish. □

This lemma will be applied for $\gamma=\alpha,\beta$ and β/α.

Lemma 2.2. *Let $\delta\in(0,1)$ be fixed, and let X,Y,U,V be positive numbers satisfying*

$$X>U\geqq V>Y, \quad X+Y=U+V.$$

We have

$$D=U^{\delta}+V^{\delta}-(X^{\delta}+Y^{\delta})\asymp V^{\delta}(1-Y/U)(1-Y/V), \tag{2.3}$$

where the implied constants depend on δ but not on X, Y, U, V.

This lemma will be applied for $\delta = \beta/\alpha$.

PROOF. We have

$$V^\delta - Y^\delta = \delta \int_Y^V t^{\delta-1}\,dt, \tag{2.4}$$

and

$$X^\delta - U^\delta = \delta \int_U^X t^{\delta-1}\,dt = \delta \int_Y^V (t+U-Y)^{\delta-1}\,dt. \tag{2.5}$$

Now if $Y \leqq U/2$, then $U - Y \geqq U/2 \geqq V/2 \geqq t/2$ on the whole range $t \in [Y, V]$ of integration, hence $t + U - Y \geqq (3/2)t$ and so

$$t^{\delta-1} - (t+U-Y)^{\delta-1} \begin{cases} \leqq t^{\delta-1}, \\ \geqq t^{\delta-1}\left(1 - \left(\frac{3}{2}\right)^{\delta-1}\right). \end{cases}$$

Consequently,

$$D \asymp \delta \int_Y^V t^{\delta-1}\,dt = V^\delta - Y^\delta \asymp V^\delta(1 - Y/V)$$

by Lemma 2.1. Since $1 - Y/U$ is between $1/2$ and 1, this is equivalent to (2.3).

If $Y > U/2$, then we substract (2.4) and (2.5) and apply

$$t^{\delta-1} - (t+U-Y)^{\delta-1} = (1-\delta) \int_Y^U (t+z-Y)^{\delta-2}\,dz$$

to obtain

$$D = \delta(1-\delta) \int_Y^V \int_Y^U (t+z-Y)^{\delta-2}\,dz\,dt.$$

Observe that

$$t + z - Y \begin{cases} \geqq Y \geqq U/2 \geqq V/2, \\ \leqq V + U - Y \leqq V + Y \leqq 2V, \end{cases}$$

thus the integrand is $\asymp V^{\delta-2}$ and so the integral is

$$\asymp V^{\delta-2}(V-Y)(U-Y) = V^\delta(1-Y/V)(1-Y/U)(U/V).$$

The last factor is $\geqq 1$ and $\leqq U/Y < 2$, so this is equivalent to (2.3). $\square$

For given y, u, v define $x_0 = x_0(y, u, v)$ by the equality

$$x_0^\alpha + y^\alpha = u^\alpha + v^\alpha \tag{2.6}$$

and

$$d = d(y, u, v) = v^\beta (1 - y/v)(1 - y/u). \tag{2.7}$$

LEMMA 2.3. *There are positive constants y_0 and c, depending on α and β, such that for integers x, y, u, v satisfying*

$$x > u \geqq v > y > y_0 \tag{2.8}$$

we have

$$p = \mathbf{P}(f(x) + f(y) = f(u) + f(v)) < cd^{-1} \tag{2.9}$$

and $p = 0$ if $|x - x_0| > cdu^{1-\alpha}$.

PROOF. In the sequel we will apply the ordo notations $\ll, \asymp, \gg$ in the following sense: the implied constants may depend on α, β, but not on ξ or the variables x, y, u, v.

If $f(x) + f(y) = f(u) + f(v)$, then clearly

$$|x^\alpha + y^\alpha - u^\alpha - v^\alpha + \xi(x^\beta + y^\beta - u^\beta - v^\beta)| < 2.$$

We introduce the notations

$$A = A(x, y, u, v) = x^\alpha + y^\alpha - u^\alpha - v^\alpha$$

and

$$B = B(x, y, u, v) = x^\beta + y^\beta - u^\beta - v^\beta.$$

Thus we have

$$p \leqq \mathbf{P}(|A + \xi B| < 2). \tag{2.10}$$

Write

$$B^* = B^*(x, y, u, v) = |B| + 2.$$

Clearly

$$\mathbf{P}(|A + \xi B| < 2) \begin{cases} = 0, & \text{if } |A| \geqq B^*, \\ \leqq 2/|B|, & \text{if } |A| < B^*. \end{cases} \tag{2.11}$$

We will compare B and B^* to

$$B_0 = B_0(y, u, v) = x_0^\beta + y^\beta - u^\beta - v^\beta.$$

First we show that

$$B_0 \asymp -d. \tag{2.12}$$

Indeed, an application of Lemma 2.2 to the numbers $X = x_0^\alpha$, $Y = y^\alpha$, $U = u^\alpha$, $V = v^\alpha$, $\delta = \beta/\alpha$ yields

$$-B_0 \asymp v^\beta (1 - y^\beta/v^\beta)(1 - y^\beta/u^\beta).$$

By Lemma 2.1 we infer that

$$(1 - y^\beta/v^\beta) \asymp 1 - y/v, \quad (1 - y^\beta/u^\beta) \asymp 1 - y/u$$

and we obtain (2.12).

Next we observe that

$$B - B_0 = x^\alpha - x_0^\alpha \asymp (x - x_0) \max(x, x_0)^{\beta - 1}, \tag{2.13}$$

by Lemma 2.1. Similarly

$$A = x^\alpha - x_0^\alpha \asymp (x - x_0) \max(x, x_0)^{\alpha - 1}. \tag{2.14}$$

A comparison of (2.13) and (2.14) shows that

$$|B - B_0| \ll |A| \max(x, x_0)^{\beta - \alpha} \leqq |A| y_0^{\beta - \alpha}.$$

In particular, if y_0 is large enough (in terms of α and β), then we have

$$|B - B_0| \leqq |A|/3, \tag{2.15}$$

whenever (2.8) holds. Hence if $|A| < B^*$, then

$$|A| < |B| + 2 \leqq |B_0| + |B - B_0| + 2 \leqq |B_0| + |A|/3 + 2,$$

that is,

$$|A| < \frac{3}{2}|B_0| + 3. \tag{2.16}$$

We can get rid of the constant term by observing that

$$1 - \frac{y}{u} \geqq 1 - \frac{y}{v} \geqq 1 - \frac{v-1}{v} = \frac{1}{v},$$

thus

$$d \geqq v^{\beta - 2} > y_0^{\beta - 2},$$

and this will be large if y_0 is large. Since $|B_0| \gg d$, a suitable choice of y_0 ensures that $|B_0| > 6$, and then (2.16) implies

$$|A| < 2|B_0| < c_1 d. \tag{2.17}$$

Since

$$|A| \gg |x - x_0| \max(x, x_0)^{\alpha-1} > |x - x_0| u^{\alpha-1},$$

we can immediately conclude that $|x - x_0| \ll u^{1-\alpha} d$, the second claim of Lemma 2.3.

To get the first claim we observe that

$$|B - B_0| \leqq |A|/3 < \frac{2}{3}|B_0|$$

by (2.15) and (2.17), thus

$$|B| \geqq |B_0| - |B - B_0| > \frac{1}{3}|B_0| \gg d.$$

The result now follows from (2.10) and (2.11). □

3. Proof of the Theorems

We will prove Theorem 2, which contains Theorem 1 as a special case.

We assume that α, β are fixed real numbers satisfying (1.1). If A of (1.3) is not a Sidon set, then there are integers $x, y, u, v > n_0$ such that (x, y) is not a permutation of (u, v) and

$$f(x) + f(y) = f(u) + f(v). \tag{3.1}$$

If x, y, u, v form a solution, then so do the quadruples obtained by exchanging the pairs (x, y) and (u, v), or by exchanging the elements within a pair. Hence without restricting generality we may assume that x is the largest of the four numbers and that $u \geqq v$. Since f is monotonic, this implies that y is the smallest, that is, $x \geqq u \geqq v \geqq y$. However, $x = u$ would yield $f(y) = f(v)$ and hence $y = v$, not a proper solution of (3.1); similarly we can exclude $v = y$. Thus we may assume

$$x > u \geqq v > y. \tag{3.2}$$

First we deduce a bound for u in terms of v and y. Since

$$f(x) - f(u) = f(v) - f(y) < f(v) < 2v^\alpha$$

and

$$f(x) - f(u) \geqq f(u+1) - f(u) \geqq (u+1)^\alpha - 1 - u^\alpha > \alpha u^{\alpha-1} - 1,$$

we obtain

$$\alpha u^{\alpha-1} < 2v^\alpha + 1 \leqq 3v^\alpha < \alpha v^\alpha,$$

whence

$$u < v^{\alpha/(\alpha-1)}. \tag{3.3}$$

(This could be improved to $u \ll v(v-y)^{1/(\alpha-1)}$, but this would not affect the final result.)

We will establish that

$$\sum_{x>u\geqq v>y>y_0} \mathbf{P}(f(x)+f(y)=f(u)+f(v)) < \infty \tag{3.4}$$

for a suitable y_0, depending on α and β. By the Borel–Cantelli lemma, this implies that for almost all ξ equation (3.1) has only finitely many solutions with $y > y_0$. If we define n_0 as the largest integer that occurs in these solutions, then $\{f(n) : n > n_0\}$ will indeed be a Sidon set.

To prove (3.4) we apply Lemma 2.3. For fixed y, u, v we learn that, with the quantity d defined by (2.7), each probability is $\ll 1/d$ and we have a nonzero probability only for $|x - x_0| \ll du^{1-\alpha}$ with a certain x_0, given by equation (2.6). Hence the number of nonzero summands is $\ll 1 + du^{1-\alpha}$, and we conclude that

$$\sum_x \mathbf{P}(\dots) \ll d^{-1} + u^{1-\alpha}.$$

The second term is easily settled. Indeed, as $y < v \leqq u$, for a given u the number of possible choices of y, v is at most u^2, thus

$$\sum_{u,v,y} u^{1-\alpha} \leqq \sum_u u^{3-\alpha} < \infty$$

since $\alpha > 4$.

Now we prove that

$$\sum_{u,v,y} \frac{1}{d} = \sum \frac{v^{1-\beta}}{v-y} \frac{u}{u-y} < \infty.$$

First we estimate the sum over u, with v and y fixed. If $u > 2y$, then $u/(u-y) < 2$, so this part of the sum is $\ll v^{\alpha/(\alpha-1)}$ by virtue of the bound (3.3). We estimate the part belonging to $u \leqq 2y$ by

$$\sum_{u=y+1}^{2y} \frac{u}{u-y} \leqq 2y \sum_{i=1}^{y-1} \frac{1}{i} \ll y \log y \ll v \log v.$$

This is smaller than the contribution of large values of u, and we find that

$$\sum 1/d \ll \sum_{v,y} v^{\alpha/(\alpha-1)+1-\beta} \frac{1}{v-y}.$$

Since, for fixed v, we have

$$\sum_{y<v} \frac{1}{v-y} = \sum_{i=1}^{v-1} \frac{1}{i} \ll \log v,$$

the whole sum is

$$\ll \sum_{v} v^{\alpha/(\alpha-1)+1-\beta} \log v < \infty$$

as soon as $\alpha/(\alpha-1)+1-\beta<-1$, which is the second part of condition (1.1). $\square$

4. Remarks and problems

The condition on β is of a technical nature and can probably be relaxed by a more careful treatment. It comes from our estimate of the number of admissible values of x. If the condition $|x-x_0|<\dots$ specifies an interval of length <1, we used 1 as an estimate; in most cases the correct number is 0, and this can probably be utilized by studying the distribution of the fractional part of x_0.

The series we obtain will be divergent if $\alpha \leqq 4$. This suggests that probably for almost all ξ the corresponding set will not have the Sidon property; a proof seems to be feasible with Janson's inequality, but I did not work this out. Thus likely if a denser regular Sidon set exists, it must be based on a special "lucky" construction.

No doubt this method works for other types of formulas as well, though the calculation may be rather different. In particular, the following should not be very difficult.

CONJECTURE 4.1. *For almost all $\alpha>4$ there is an n_0, depending on α, such that the set $A=\{[n^\alpha]:n>n_0\}$ is a Sidon set.*

Concerning the possibility to find a Sidon set generated by a polynomial of integral coefficients, a quadratic polynomial cannot do this. This follows from a classical result of Erdős on the density of infinite Sidon sequences (see in [2]). I think that cubic polynomials do not work either.

CONJECTURE 4.2. *No polynomial of degree* 3 *generates a Sidon set.*

I have some informal reasoning to support this. About degree 4 I do not have any credible argument in any direction.

REFERENCES

[1] GUY, R. K., *Unsolved problems in number theory*, Problem Books in Mathematics, Unsolved Problems in Intuitive Mathematics, **1**, Springer-Verlag, New York–Berlin, 1981. *MR* **83k**:10002

[2] Halberstam, H. and Roth, K. F., *Sequences*, Clarendon Press, Oxford, 1966. *MR* **35** #1565; 2nd ed., Springer-Verlag, New York–Berlin, 1983. *MR* **83m**:10094
[3] Swinnerton-Dyer, H. P. F., $A^4+B^4=C^3+D^4$ revisited, *J. London Math. Soc.* **43** (1968), 149–151. *MR* **37** #2685

(Received June 5, 2000)

MTA RÉNYI ALFRÉD MATEMATIKAI KUTATÓINTÉZETE
POSTAFIÓK 127
H–1364 BUDAPEST
HUNGARY

ruzsa@renyi.hu