Laudatio for Professor András Sárközy

C.L.Stewart

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada

Debrecen, July 7, 2022

Professor András Sárközy is an exceptional mathematician and a wonderful person. I have had the good fortune to know him for the last 40 years and I count him as a close friend. I am honoured to give this laudatio for him and am sorry that I am not able to present it in person.

I would like to thank Professor Lajos Hajdu for his help with the delivery of this lecture.

Professor András Sárközy, an emeritus professor at Eötvös Loránd University, is a full member of the Hungarian Academy of Sciences. He was awarded the Széchenyi Prize in 2010.

András is a number theorist who works mainly in analytic and combinatorial number theory. He has written over 260 papers and has a large number of coauthors. I will list now those who have at least 10 papers with András according to MathSciNet.

Paul Erdős (62), Christian Mauduit (42), Katalin Gyarmati (28), Cameron Stewart (20), Joël Rivat (18), Endre Szemerédi (17), Cécile Dartyge (15), Jean-Louis Nicolas (14), Carl Pomerance (10), Vera Sós (10)

A few notes about the list. András has more joint papers with Erdős than any other mathematician. While I am fourth on András' list he is first on mine. He is very generous with his ideas and we had great fun working together over the years. Although he often complained, in a good natured way, when I engaged in "illegal thinking", ie. speculating on new problems before we had finished our task at hand.

FIGURE: Hungary,1984

I would like now to highlight some of the results obtained by András over the course of his career. I will begin with two of his papers which have had an extraordinary impact. The first is his paper On difference sets of sequences of integers,I which appeared in 1978 and the second is his paper with Christian Mauduit On finite pseudorandom binary sequences I: Measure of randomness, the Legendre symbol which appeared in 1997.

Let N be a positive integer and let $A = (a_n)_{n=1}^{\infty}$ be an increasing sequence of positive integers. Let $A(N)$ denote the number of terms of A which are at most N. Lovász conjectured that if

$$\overline{\lim} \frac{A(N)}{N} > 0,$$

then there exist i, j with $i \neq j$ such that $a_i - a_j$ is the square of an integer. András proved Lovász' conjecture by means of the Hardy-Littlewood method as elaborated by Roth in his work on sets of integers which do not contain three term arithmetical progressions. Furstenberg gave another proof of Lovász' conjecture using ergodic theory.

In fact, András proved a quantitative refinement of Lovász' conjecture. He showed that if there is no difference which is a square then

$$\frac{A(N)}{N} = O\left(\frac{(\log\log N)^{2/3}}{(\log N)^{1/3}}\right).$$

This was sharpened by Pintz, Steiger and Szemerédi who proved that

$$\frac{A(N)}{N} = O\left((\log N)^{-(\log\log\log\log N)/12}\right).$$

Recently Bloom and Maynard have obtained a further refinement. They proved that there is a positive number c such that

$$\frac{A(N)}{N} = O\left((\log N)^{-(c \log\log\log N)}\right).$$

András also proved that if A has the property that $a_i - a_j$ is never of the form $p - 1$ with p a prime then A has upper density 0 and, in fact, that

$$\frac{A(N)}{N} = O\left(\frac{(\log_3 N)^3 \log_4 N}{(\log_2 N)^2}\right);$$

where $\log_1 N = \log N$ and $\log_i N = \log(\log_{i-1} N)$ for $i = 2, 3, \ldots$. This was subsequently refined by Lucier, by Ruzsa and Sanders and by Wang and, very recently, by Green who proved that there is a positive number c such that

$$\frac{A(N)}{N} = O\left(N^{-c}\right).$$

András' paper sparked a resurgence of interest in the density increment argument of Roth and it has led to many important developments in number theory. In parallel with these developments have been extensions of the ergodic theoretic approach of Furstenberg. It shows the importance of good questions in mathematics.

The next slide is a picture of András with his daughter Andrea and my wife Ellen and daughter Elisa. It was taken in Elmira, Ontario.

FIGURE: András, Gábor and family at Christmas dinner, Waterloo

The concept of randomness is an important but elusive one. Let N be a positive integer and let $E_N = (e_1, \ldots, e_N)$ be a sequence of terms from $\{-1, 1\}$. When does the sequence appear to be random? Such a question is fundamental and has applications to the study of pseudorandom sequences. Following on earlier work of Knuth on pseudorandomness of finite sequences, Mauduit and Sárközy introduced several measures of randomness for finite sequences.

In particular, they introduced measures of normality, well distribution in arithmetical progressions and multiple correlations.
Let k be a positive integer and let $X = (\varepsilon_1, \ldots, \varepsilon_k)$ be a sequence of terms from $\{-1, 1\}$. Let M be a positive integer and put

$$T(E_N, M, X) = \left|\{n : 0 \leq n < M, (e_{n+1}, \ldots, e_{n+k}) = X\}\right|,$$

where for any set Y, we denote its cardinality by $|Y|$.

The normality measure of order k, $N_k(E_N)$, is defined by

$$N_k(E_N) = \max_{X \varepsilon \{-1,1\}^k} \max_{0<M\leq N+1-k} \left| T(E_N, M, X) - M/2^k \right|.$$

The well distribution measure of E_N, $W(E_N)$, is defined by

$$W(E_N) = \max_{a,b,t} \left| \sum_{n=0}^{t-1} e_{a+nb} \right|,$$

where the maximum is taken over all positive integers a, b, t such that $1 \leq a < a + (t-1)b \leq N$.

Further, the correlation measure of order k of E_N, $C_k(E_N)$, is defined by

$$C_k(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|$$

where the maximum is taken over all k-tuples of distinct non-negative integers $D = (d_1, \ldots, d_k)$ and positive integers M for which $M + d_k \leq N$.

For each $\varepsilon > 0$ the probability exceeds $1 - \varepsilon$ that a randomly chosen sequence E_N from $\{-1, 1\}^N$ will have $W(E_N)$ between two positive multiples, depending on ε, of $N^{1/2}$ and will have $C_k(E_N)$ between two positive multiples, depending on ε, of $(kN \log N)^{1/2}$ for N sufficiently large.

Further, Mauduit and Sárközy , proved that the normality measure could be bounded from above by the correlation measures. They proved that for all N, E_N and $k < N$,

$$N_k(E_N) \leq \max_{1 \leq t \leq k} |C_t(E_N)| .$$

As a consequence they focussed on the measures W and C_k with the objective of proving upper bounds for them for various sequences E_N which approached in strength those for a typical random sequence and this work initiated much further study. In fact there has been an explosion of activity over the last quarter century in proving that various naturally occurring finite sequences behave like a typical sequence with respect to these measures. The decision by Mauduit and Sárközy to focus on these measures has proven to be very fruitful.

To fix ideas let p be an odd prime and consider the sequence of Legendre symbols $E(p) = ((\frac{1}{p}), (\frac{2}{p}), \ldots, (\frac{p-1}{p}))$. One half of the terms of $E(p)$ are 1 and the other half are -1 and, apart from a central symmetry, the distribution of 1's appears to be chaotic when $E(p)$ is calculated for various small primes p.

One might ask about the apparently random behaviour of the sequences $E(p)$ and a first step would be to check whether or not given patterns $(\varepsilon_1, \ldots, \varepsilon_k)$ with ε_i from $\{-1, 1\}$ occur with the expected frequency in $E(p)$. (Recall the definition of the Normality measure.) In 1906 Jacobstahl showed this to be the case when k is 2 or 3. In Davenport's first paper he treated the cases $k = 4$ or 5 and two years later, in 1933, he extended the work to cover all positive integers k less than 10.

Let $E_p(\varepsilon_1, \ldots, \varepsilon_k)$ denote the number of occurences of $(\varepsilon_1, \ldots, \varepsilon_k)$ as consecutive terms of $E(p)$. Further progress was made by Gelfond and Linnik in 1965, Bach in 1987 and Peralta in 1992 by means of the Weil bounds for exponential sums. In particular, it follows from their work that

$$E_p(\varepsilon_1, \ldots, \varepsilon_k) = \frac{p}{2^k} + O(kp^{1/2}).$$

Mauduit and Sárközy went much farther. They proved that there exist positive numbers c_1 and c_2 such that

$$W(E(p)) < c_1 p^{1/2} \log p$$

and

$$C_k(E(p)) < c_2 k p^{1/2} \log p.$$

Their proofs also made use of the Weil bounds.

András has constructed examples of pseudorandom binary sequences by means of various techniques. For example with Mauduit and Rivat in 2004 using additive characters, with Mauduit in 2005 using multiplicative inverses and with Gyarmati and Pethő in 2005 using linear recurrence sequences.

The notion of pseudorandom binary sequences has been generalized by András with Dartyge in 2007 to subsets of finite sets and to multidimensional binary lattices in a series of papers from 2006 to 2014 with Hubert, Mauduit and Gyarmati.

It is clear that the original paper of Mauduit and Sárközy has led to the development of a rich and interesting area of study.

FIGURE: Ice fishing with Carl Pomerance ,who has two fishing poles

In the next slide I am proudly displaying our catch after a full day of fishing on the ice at Lake Simcoe.

In a series of papers András investigated the arithmetical character of sumsets. Let N be a positive integer and let A and B be subsets of $\{1, \ldots, N\}$. In 1984 Balog and Sárközy proved, by means of the large sieve inequality, that if

$$|A| >> N \quad \text{and} \quad |B| >> N$$

then there exist a in A and b in B and a prime p dividing $a + b$ with

$$p >> N/\log N.$$

They also proved, under the same assumption, that there exist a_1 in A and b_1 in B and a prime p such that $p^2 \mid a_1 + b_1$ and

$$p^2 >> N/(\log N)^7.$$

For the proof they employed the circle method.

In 1986 and 1988 András and I used the circle method to sharpen these results. We proved that if k is a positive integer then there exist a in A and b in B and a prime p such that p^k divides $a+b$ and

$$p^k >>_k N.$$

In 1992 Ruzsa gave a new proof of this result for the case when $k = 1$.

The general philosophy behind results of this sort is that if A and B are sufficiently dense subsets of $\{1, \ldots, N\}$ then arithmetical properties of the sums $a + b$ should mirror those of the first $2N$ integers. With this in mind, it is reasonable to ask if an Erdős-Kac theorem holds for the sums $a + b$.

In 1987 Erdős, Maier and Sárközy established such a result. For any positive integer n let $\omega(n)$ denote the number of prime factors of n. They proved that

$$\frac{1}{|A||B|}\left|\left\{(a,b) : \frac{\omega(a+b)-\log\log N}{(\log\log N)^{1/2}} < x,\ a\in A,\ b\in B\right\}\right|$$

is asymptotic to

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-u^2/2}du,$$

provided that

$$\frac{|A||B|}{N^2/(\log\log N)^{1/2}} \to \infty \quad \text{as } N\to\infty.$$

Elliott and Sárközy and also Tenenbaum have extended this result.

Erdős, Pomerance, Sárközy and I considered several problems connected with large values of $\omega(a+b)$. I would like to mention one of the results that András and I proved. Let θ be a real number with $1/2 < \theta \leq 1$ and let N be a positive integer. We proved that there is a positive number C, which is effectively computable in terms of θ, such that if A and B are subsets of $\{1, \ldots, N\}$ with N greater than C and

$$(|A||B|)^{1/2} \geq N^{\theta},$$

then there exists an integer a from A and an integer b from B for which

$$\omega(a+b) > \frac{1}{6}(\theta - \frac{1}{2})^2 (\log N)/\log\log N.$$

The dependence on N is best possible. The proof is an unusual iterative construction where at each stage we appeal to a variant of the large sieve inequality.

In 2014 Balog, Sárközy and Rivat tackled sums for which the number of distinct prime factors is small. Let N be a positive integer and let A and B be subsets of $\{1, \ldots, N\}$. Put

$$R = \frac{3N}{(|A||B|)^{1/2}}.$$

They proved that for N sufficiently large there exist a in A and b in B with

$$\omega(a+b) << \frac{\log R}{\log\log R}.$$

FIGURE: Aux Baies des Singes restaurant, outside of Marseille, 1999

A set of positive integers A is said to be reducible if there exist sets B and C of positive integers with cardinality at least 2 for which

$$A = B + C,$$

and otherwise it is said to be irreducible.

We say that two sets of positive integers A and B are asymptotically equal, denoted by $A \sim B$, if all sufficiently large elements are the same.

An infinite set of positive integers is said to be totally irreducible if every A' with $A \sim A'$ is irreducible.

In 1956 Ostmann conjectured that the set of primes is totally irreducible, a conjecture which is still open.

Erdős conjectured that if one changes $o(n^{1/2})$ elements up to n in the set S of squares that the resulting set is totally irreducible.

In 1965 Sárközy and Szemerédi proved a slightly weaker version of the conjecture where for each $\epsilon > 0$ one is allowed to make $n^{(1/2)-\epsilon}$ changes up to n.

In a series of three papers from 2018 to 2020 Hajdu and Sárközy have considered multiplicative analogues of these questions.

Here we find new phenomena since, for instance,

$$S = SS$$

so the squares are multiplicatively reducible.

On the other hand Hajdu and Sárközy prove that the set S' of squares shifted by 1 is multiplicatively irreducible.

What about the set P of pure powers of positive integers?

In 2020 Hajdu and Sárközy proved that P is multiplicatively totally irreducible.

FIGURE: Fishing for salmon on Georgian Bay

Let me conclude by wishing András good health, many more theorems and many successful fishing expeditions.

Thank you for your attention.