THE
ABEL
PRIZE
2020

Two number theory problems solved by ergodic theory methods, Szemerédi's theorem and Oppenheim's conjecture.

The first problem is about arithmetic progressions. An arithmetic progression is a sequence of integers with fixed difference. The sets $\{5, 8, 11, 14, 17\}$ and $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$ are two examples of arithmetic progressions. The first one has length 5 and difference 3, and the second one has infinite length and difference 2. Now, consider a subset A of the integers $\mathbb{Z}$. Based on a paper from 1936 by the two Hungarian mathematicians Paul Erdős and Pál Turán it has been conjectured that if the subset A has positive density, then it contains arithmetic progressions of arbitrary length.

The density of a set A reflects the probability that an arbitrary chosen integer is a member of A. The formal definition is as follows;

Definition. A set A of integers has positive upper density if

$$\limsup_{N\to\infty} \frac{|A \cap \{-N, \dots, N\}|}{2N+1} > 0$$

The set $2\mathbb{Z}$ has density 2, a finite set has density 0. Also infinite sets can have 0 density, as is the case of the set of primes.

The Erdős-Turán conjecture was first proved in 1975 by the 2012 Abel Prize Laureate Endre Szemerédi, using combinatorial arguments.

Theorem (Szemerédi, 1975). Let $k \geq 1$ be an integer, and let A be a set of integers of positive upper density. Then A contains a non-trivial arithmetic progression of length k.

In 1977 Furstenberg gave another proof of the conjecture, by establishing what is now called the Furstenberg multiple recurrence theorem:

Theorem (Furstenberg, 1977). Let $k \geq 1$ be an integer, $(\mathbb{Z}, \chi, \mu, T)$ a measure-preserving system on $\mathbb{Z}$ and $E \subset \mathbb{Z}$ a set of positive measure. Then there exists an $r > 0$ such that

$$E \cap T^{-r}E \cap \cdots \cap T^{-(k-1)r}E \neq \emptyset$$

To see that Furstenberg's multiple recurrence theorem implies Szemerédi's theorem (avoiding some deeper technicalities) we let E correspond to the set A and view T as the shift operator $x \to x+1$ on $\mathbb{Z}$. Then if A contains no arithmetic progression of length k, the intersection

$$A \cap T^{-r}A \cap \cdots \cap T^{-(k-1)r}A = \emptyset \quad \text{for all } r > 0$$

In fact, if the intersection is non-empty we can find elements $a_0, \dots, a_{k-1}$ in A such that

$$a_0 = a_1 - r = a_2 - 2r = \cdots = a_{k-1} - (k-1)r$$

but then

$$a_{k-1}, a_{k-2} = a_{k-1} + r, \dots, a_0 = a_{k-1} + (k-1)r$$

is an arithmetic progression in A, of length k, contradicting the conclusion of the multiple recurrence theorem.

The second problem is known as Oppenheim's conjecture, named after the British mathematician Alexander Oppenheim. The conjecture is about solutions of quadratic equations in rational numbers. An old result by A. Meyer from 1884 states that a huge class of quadratic equations (corresponding to indefinite quadratic forms) in 5 or more variables and with integer coefficients have rational solutions.

Theorem (A. Meyer, 1884). Let Q be an indefinite quadratic form in 5 or more variables over the rational numbers $\mathbb{Q}$. If

$$Q(x) = 0$$

has a non-zero solution in $\mathbb{R}$, then it also has a non-zero solution in $\mathbb{Z}$.

The theorem is sharp in the number of variables; Consider the quadratic form

$$Q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 - p(x_3^2 + x_4^2),$$

where p is a prime number congruent to 3 modulo 4. The equation $Q = 0$ has obviously real solutions, but no integer solutions. In fact, a perfect square is congruent to 0 modulo 4 or congruent to 1 modulo 8. Suppose x_1, x_2, x_3, x_4 have no common factor. Then at least one of them is congruent to 1 modulo 8, and one can show that there are no solutions of the congruence $Q(x_1, x_2, x_3, x_4) = 0$, modulo 8. But then it is impossible that there exixts any integer solutions.

Oppenheim conjectured that quadratic equations in the same class, but with more general coefficients and only in three or more variables, can be approximated by rational numbers. The precise formulation of Oppenheim's conjecture is as follows:

Conjecture (Oppenheim, 1929). Let Q be a real non-degenerated indefinite quadratic form in 3 or more variables. Suppose Q is not a multiple of a form with rational coefficients. Then for any $\epsilon > 0$ there exist a non-zero rational vector $\mathbf{x}$ such that $|Q(\mathbf{x})| < \epsilon$.

The conjecture is not true for quadratic equations in two variables. In fact, it is known that for an algebraic number α which is a solution of a quadratic equation with integer coefficients, there exists a real number C such that $|\alpha - \frac{p}{q}| \geq \frac{C}{q^2}$ for any rational number $\frac{p}{q}$. Consider the quadratic form $Q(x, y) = \alpha^2 x^2 - y^2$. For integers p, q we then have

$$\begin{aligned} |Q(p,q)| &= |\alpha^2 p^2 - q^2| \\ &= |(\alpha x - y)(\alpha x + y)| \\ &\geq \frac{C}{x}|\alpha x + y| \\ &\geq C|\alpha| \end{aligned}$$

which shows that the conjecture is not true for quadratic forms in two variables.

Oppenheim's conjecture was proved in 1987 by Margulis in complete generality using methods of ergodic theory.