❙ Elemente der Mathematik

The Abel Prize – the new coronation of mathematical careers

Norbert Hungerbühler, University of Fribourg, Switzerland
Jürg Kramer, Humboldt-Universität zu Berlin, Germany
Yngvar Reichelt, University of Oslo, Norway

On August 23, 2001 the Norwegian Prime Minister Jens Stoltenberg proposed the establishment of a Niels Henrik Abel Memorial Fund of 200'000'000 NOK (27 million USD), with the purpose of creating an international prize for outstanding scientific work in mathematics. The prize is named after the famous Norwegian mathematician Niels Henrik Abel (1802–1829), who died at the early age of 26 leaving behind a great and lasting scientific heritage.

The following public statement from the Norwegian Academy of Science and Letters describes the criteria for the award of the Abel Prize:

> *The prize is to recognize contributions to mathematics and its applications of extraordinary depth and influence. Such work may have resolved fundamental problems, created powerful new techniques, introduced unifying principles or opened up new areas. The intent is to award prizes over the course of time in a wide range of areas of mathematics and its applications.*

The Abel Prize was first proposed in 1902 – the centenary of Abel's birth – by King Oscar II of Sweden and Norway. However, the plan was dropped when the union between the two countries ceased in 1905. It has now being revived for the bicentenary of Abel's birth, through the generosity of the Norwegian Parliament (Storting), and with the enthusiastic support of the International Mathematical Union (IMU) and the European Mathematical Society (EMS).

The Fields Medal, which is awarded every four years, endowed with 15'000 Canadian Dollars (about 10'000 Euro) and which is only awarded to researchers under 40 years, went often unnoticed by the broader public. The Abel Price is awarded annually, endowed with approximately 6 million NOK (750'000 Euro) and will be presented by the King of Norway in a ceremony in Oslo. It has the potential to become an equivalent to the Nobel Prize, and will therefore fill the gap arising from the lack of a Nobel Prize in mathematics. The prize will increase interest among young people for the study of science, strengthening the research in the field of mathematics and increase awareness of the important rôle of mathematics in culture, technology and applications.

The annual return of the fund capital is allocated to the Norwegian Academy of Science and Letters, which awards the prize on the recommendation of an Abel committee, formed by five outstanding mathematicians, one proposed by the EMS, three proposed by the IMU, and one Norwegian. This year, the committee consists of Erling Størmer (University of Oslo, Chair), John Ball (University of Oxford), Friedrich Hirzebruch (Max Planck Institute for Mathematics, Bonn), David Mumford (Brown University, Providence RI) and Jacob Palis (IMPA). The name of the first Abel laureate has been announced on April 3, 2003 and the prize will be presented on June 3, 2003.

The first Abel laureate is **Jean-Pierre Serre**, one of the great mathematicians of our time. He is an Emeritus Professor at the Collège de France in Paris. Serre has been made a Commander Légion d'Honneur and High Officer Ordre National du Mérite. He has been elected to many national academies, was awarded the Fields Medal in 1954 (the youngest recipient ever), the Prix Gaston Julia in 1970, the Balzan Prize in 1985, the Steele Prize in 1995, and the Wolf Prize in 2000. He has been awarded honorary degrees from many universities. Serre has made profound contributions to the progress of mathematics for over half a century, and is continuing to do so. He has been of major influence in shaping the modern form of many parts of mathematics, including

- *Topology*, which treats the question: what remains the same in geometry even when the length is distorted?
- *Algebraic Geometry*, which treats the question: what is the geometry of the solutions of polynomial equations?
- *Number Theory*, the study of basic properties of numbers; for example prime numbers and rational or integer solutions of polynomial equations as in Fermat's Last Theorem.

Many of the fundamental theorems in the above mentioned disciplines are due to Serre. He developed revolutionary algebraic methods for studying topology, and in particular studied the transformations between spheres of higher dimensions. He is responsible for a spectacular clarification of the work of the Italian algebraic geometers by introducing and developing the right algebraic machinery for determining when their geometric construction worked. This powerful technique of Serre, with its new language and viewpoint, ushered in a golden age for Algebraic Geometry. For the past four decades Serre's work in Number Theory, and his vision, have brought that subject to its current glory. His work has been vital in setting the stage for many of the most celebrated recent breakthroughs, including the work of Wiles on Fermat's Last Theorem. Serre's contribution here is so vast that it hardly is possible to give a sense of its immensity, but let us try to explain a bit of the background to appreciate just one of Serre's fundamental results in Number Theory.

As mentioned above, a central focus of Number Theory consists in the understanding of the zeroes of polynomial equations with rational coefficients; for simplicity, let us concentrate on the case of polynomials $f = f(X)$ in one variable. When the degree of the polynomial in question is one, the zeroes are rational numbers, which are well understood. If we consider a quadratic polynomial, we know from high school algebra that the zeroes of such a polynomial are given in terms of square roots involving the coefficients of the polynomial. Sixteenth century Italian algebraists used cube roots, and

fourth roots to express the solutions of polynomial equations of degrees three and four. Niels Henrik Abel then showed that this simple tool of extracting suitable roots is not sufficient to solve arbitrary polynomial equations of degree bigger than or equal to five; this asked for the development of additional tools to understand the arithmetic nature of the solutions of such polynomial equations. In the next paragraph we will discuss a simple example explaining this conceptual point of view.

Gauß realized the complex numbers as elements of the (x, y)-plane. Complex numbers of absolute value one can then be interpreted as elements of the unit circle S^1, i.e., elements $z = x + iy \in \mathbb{C}$ satisfying $x^2 + y^2 = 1$. Parametrizing S^1 by means of $z = e^{i\varphi}$ ($\varphi \in \mathbb{R}$), we immediately see that S^1 carries the structure of an abelian group with group law given by $e^{i\varphi_1} \cdot e^{i\varphi_2} = e^{i(\varphi_1 + \varphi_2)}$. For an algebraist it is now quite natural to ask for the elements of finite order in this group, i.e., for the elements $\zeta \in S^1$ satisfying $\zeta^m = 1$ for some positive natural number m. It is known that the set of these elements is nothing but the finite subgroup $\mu_m = \{\zeta = e^{2\pi in/m} \mid n = 0, \dots, m-1\}$ of m-th roots of unity. We observe that μ_m is a cyclic subgroup generated by a primitive m-th root of unity $e^{2\pi in/m}$ $\big((n, m) = 1\big)$, e.g., $\zeta_1 = e^{2\pi i/m}$. With regard to our original problem, we note that in case $m = \ell$ a prime number, there are $(\ell - 1)$ different primitive ℓ-th roots of unity, which are the zeroes of the irreducible polynomial

$$X^{\ell-1} + X^{\ell-2} + X^{\ell-3} + \cdots + X^2 + X + 1 = 0, \tag{1}$$

a so-called cyclotomic polynomial. All the (primitive) ℓ-th roots of unity are contained in the simple algebraic extension

$$\mathbb{Q}(\zeta_1) = \left\{ \sum_{j=0}^{\ell-1} a_j \cdot \zeta_1^j \;\middle|\; a_0, \dots, a_{\ell-1} \in \mathbb{Q} \right\},$$

over $\mathbb{Q}$ generated by ζ_1. The so-called cyclotomic field $\mathbb{Q}(\zeta_1)$ is a Galois extension of $\mathbb{Q}$ of degree $(\ell - 1)$ with Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_1)/\mathbb{Q})$ isomorphic to the group $(\mathbb{Z}/\ell\mathbb{Z})^\times$ of invertible elements of the ring of integers modulo ℓ. The Galois group acts by sending ζ_1 to the other primitive ℓ-th roots of unity. In this way, we fully understand the arithmetic nature of the zeroes of the cyclotomic polynomial (1). We emphasize that Kummer studied the cyclotomic extensions comprehensively, which lead him to a proof of Fermat's Last Theorem for exponents less than 100 (up to a few exceptions).

In order to decribe Serre's result, we now replace the unit circle described by the quadratic equation $x^2 + y^2 = 1$ by a curve given by a cubical equation in the (x, y)-plane of the form

$$E : \; y^2 = 4x^3 - g_2 x - g_3,$$

where g_2, g_3 are rational numbers satisfying $g_2^3 - 27g_3^2 \neq 0$. If we view this curve in the projective plane, it can be completed by adding a distinguished point O at infinity. The curve E together with its point O is called an elliptic curve. As it was possible to parametrize S^1 using the exponential function (or, equivalently, the trigonometric sine and cosine functions), it turns out that (the complex points of) the elliptic curve E can be parametrized by means of Weierstraß' elliptic function $\wp(\cdot)$, namely we have

$$E(\mathbb{C}) = \{(\wp(z), \wp'(z)) \mid z \in \mathbb{C}\}.$$

The Weierstraß $\wp$-function is doubly periodic and emerges from the study of elliptic integrals, which themselves arise as expressions for the arc lengths of ellipses. It was the idea of Gauß, Legendre, Abel, and Jacobi to invert certain of these arc length expressions giving rise to elliptic functions and generalizing the exponential function, which has only one period. We also note that elliptic curves play nowadays an important rôle in public-key cryptography.

The additive group structure underlying the field of complex numbers $\mathbb{C}$ induces via the $\wp$-function the structure of an abelian group on E, which has the following geometrical description: Given two points P and Q on E, we first construct the straight line joining the two points and intersecting the curve E in a third point R; the sum $P + Q$ is then given by the mirror image of R with respect to the x-axis. If P and Q coincide, one has to replace the secant by the tangent; the point O is the neutral element for this group structure. Using elementary analytical geometry, one can easily compute the coordinates of $P + Q$ in terms of rational functions of the coordinates of P and Q.

As in the case of the unit circle, one can now investigate the points of finite order on E, i.e., the points $P = (x_P, y_P)$ satisfying $m \cdot P = O$ for some positive $m \in \mathbb{N}$. There are m^2 points of order m; the formulas describing the coordinates of $m \cdot P$ show that the x_P's are the zeroes of a certain polynomial (depending on E and m). Fixing a prime ℓ, Serre studied the algebraic extension K_ℓ obtained by adjoining the x-coordinates of all the points of order ℓ^n ($n = 1, 2, \ldots$) to $\mathbb{Q}$. He found that the Galois group $\mathrm{Gal}(K_\ell/\mathbb{Q})$ of this extension generically contains the group $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for almost all primes ℓ, i.e., it contains at least $\ell(\ell^2 - 1)$ elements. "Generically" here means: with the exception of elliptic curves having "complex multiplication".

This result of Serre represents of course a vast generalization of the corresponding result for cyclotomic fields discussed above. It marks the beginning of a fruitful modern epoch in Number Theory, in which the arithmetic of elliptic curves is connected with other classical objects such as modular forms.

ABEL
PRISEN