Igor Rostislavovich Shafarevich

Ш (may we say "Shah"?) of Number Theory

B Sury

A magician from Moscow did stitch
a maze of Galois groups and abelian varieties which
led math to progress by leaps and bounds,
scale new heights and break new grounds.
It behoves us to thank Igor Shafarevich!

Shafarevich was an algebraist and geometer of the highest order who pioneered several topics in both. The fundamental results he proved, as well as the conjectures he made, were beacons for mathematical progress and universal landmarks. The first part Ш (pronounced "Sha") of his surname was borrowed to denote an intriguing, elusive object called the 'Tate–Shafarevich group'. Shafarevich held strong views on the philosophy of mathematics and wrote at length on it. Here, we pick out some of the mathematical gems resulting from Shafarevich-craft, so to say. In particular, we discuss his theorems and conjectures on Galois groups over **Q** and the role of his conjecture on curves and abelian varieties in the proof of Mordell's conjecture.

Sury likes interacting with talented high school students and writing for undergraduate students. At present, he is the National co-ordinator for the Mathematics Olympiad Programme in India.

Introduction

The previous mathematician featured in this journal was Hermann Weyl (December 2016 issue). Igor Rostislavovich Shafarevich who is featured here – while being a number theorist, algebraist and geometer of the highest order – was also someone who had strong ideas about the philosophy of mathematics and wrote at length to draw others to his point of view.

He begins his book *Basic Notions of Algebra* [1], with the words, "One can attempt a description of the place occupied by algebra in mathematics by drawing attention to the process for which

Keywords
Galois group, Shafarevich–Tate group, elliptic curves, abelian varieties, infinite-dimensional groups, Emmy Noether's problem.

"To Galileo is due the most extreme statement in his time of the idea of coordinatisation: Measure everything that is measurable and make measurable everything that is not yet so."

Hermann Weyl coined the unpronounceable word 'Coordinatisation'." He goes on later to say, "To Galileo is due the most extreme statement in his time of the idea of coordinatisation: Measure everything that is measurable and make measurable everything that is not yet so." He defines algebra as follows:

"Anything which is an object of mathematical study (curves and surfaces, symmetries, crystals, quantum mechanical quantities, and so on), can be 'coordinatised' or 'measured'. However, for such a coordinatisation, the 'ordinary' numbers are by no means adequate. Conversely, when we meet a new type of object, we are forced to construct (or discover) new types of quantities to coordinatise them. The construction and the study of the quantities arising in this way is what characterises the place of algebra in mathematics (of course, very approximately)."

In an article written in the *Mathematical Intelligencer* in 1991 [2], Shafarevich traces that the fundamental difficulties in mathematics arise due to a lack of generalization to a nonabelian situation facts in 'abelian' mathematics; for example, the duality theory of locally compact abelian groups. By means of several examples (which his mastery over several subjects allows him to come up with), Shafarevich manages to bring us to his point of view.

We briefly make a mention of Shafarevich's expositions and textbooks for students. It may not be well known among professional mathematicians that Shafarevich also wrote for high school students in his inimitable way – one of his books is being reviewed in this issue. Among his texts, the two books *Basic Algebraic Geometry* [3] and *Number theory* ([4] – written in collaboration with Borevich) are both regarded as classics. During the last three decades, it is not uncommon to find many graduate students who started learning algebraic geometry from Hartshorne's book, turn to Shafarevich's text when they were stuck. Whenever possible, Shafarevich would prefer to provide a simple, natural, geometric argument. It is a close call as to which of the two abovementioned books (geometry or number theory) is more revered. Both are beautifully crafted with a fine choice of language too.

In his book on basic algebra, it is remarkable that he begins with rings and fields and only later comes to groups (it is often done the other way around in modern algebra texts). He also says there: "This book makes no pretence to teach algebra: it is merely an attempt to talk about it." The book has a very large number of examples, and Shafarevich's mathematical writings in general seem to represent the thesis that a number of illustrative and penetrating examples detailing different aspects reveal much more than a proof (which he often finishes quite briefly). Even in his writings on advanced topics, his style is to start with small examples and then go on to generalize them in stages. For instance, his 180-page article on the foundations of algebraic geometry [5] follows the same style, and again an outstanding feature is the large (200 plus) number of examples. Shafarevich was an outstanding geometer as well as arithmetician. His contributions encompass a very wide spectrum, and his deep results and conjectures have contributed to the direction in which various subjects developed. We will attempt to give a brief outline of some of contributions which have given direction to subjects.

Shafarevich's 180-page article on the foundations of algebraic geometry follows the same style, and again an outstanding feature is the large (200 plus) number of examples.

1. The Rule of The "Sha"

Shafarevich's contributions to number theory are outstanding and encompass manifold aspects. We discuss one aspect in this section. When we look for solutions to polynomial equations in integers, the first thing is to find if there are solutions modulo prime powers (this becomes a finite problem for each prime). Once these solutions modulo prime powers are known to exist, one would like to deduce the existence of a 'global' solution. The solutions modulo prime powers lead to so-called p-adic or 'local' solutions. However, the passing from 'local-to-global' is not always possible. For instance, the equation $x^4 = 17 + 2y^2$ has no rational (= global) solutions whereas it has solutions in p-adic numbers for all primes p and in the real numbers. Roughly speaking, the obstruction between having a global solution and local solutions for all primes, is measured by some object, usually an

Passing from 'local-to-global' is not always possible. For instance, the equation $x^4 = 17 + 2y^2$ has no rational (= global) solutions whereas it has solutions in p-adic numbers for all primes p and in the real numbers.

abelian group. Under fortuitous circumstances, one would expect to prove at least that the obstruction is a 'finite' group. Usually, solutions of a polynomial equation are thought of as points on a geometric object like a curve or a surface or a higher dimensional object. For instance, elliptic curves or abelian varieties[1] are geometric objects with a natural group structure defined on them, and that facilitates interpreting and solving corresponding polynomial equations using this group structure.

[1] Higher-dimensional analogues of elliptic curve.

It turns out that n is a congruent number if and only if there is a rational point of the curve with y-coordinate not zero.

An example is the classical 'congruent number' problem. A positive integer n that can be realized as the area of a right-angled triangle, all of whose sides are rational in length, is called a congruent number. The points of the 'elliptic curve'

$$y^2 = x^3 - n^2 x$$

can be 'added' to yield a natural group structure. Indeed, the degree 1 equation of the line joining two points and equation of the cubic curve have a third point in common, and one thinks of the sum of these three points to be zero. It turns out (and this is not difficult to see [6]) that n is a congruent number if and only if there is a rational point of the curve with y-coordinate not zero (equivalently, the point is of infinite order in this group). However, the existence of such a rational point is very non-trivial to check. If A is an abelian variety[2], then one calls the Tate–Shafarevich group of A, all those homogeneous spaces of A which have rational points over all completions of K, but have no rational point over K. The Tate-Shafarevich conjecture asserts that the Tate–Shafarevich group is finite. One denotes this group by the cyrillic letter Ш (as in Shafarevich). This nomenclature is due to Cassels who gives us the following interesting reason for it. The forerunner of the Tate–Shafarevich group of A over K is the so-called Weil–Chatêlet group of A over K, denoted by $WC(A/K)$ of which the Tate–Shafarevich group is a part. The notation WC (with its lavatorial connotation) was continued by the notation TS for Tate–Shafarevich group which was meant to indicate the Americanism 'tough shit' – for a part that is difficult to eliminate. Cassels mentions the above as the reason for his introduction of $Ш(A/K)$.

[2] Geometric object defined by equations with coefficients in an algebraic number field K with a group law as mentioned above.

If a, b, c are square-free and pairwise coprimes, and if the equation has real solutions (equivalently, a, b, c are not all of the same sign), then the form has integer roots if and only if $-ab$ is a square modulo c, $-bc$ is a square modulo a and $-ca$ is a square modulo b.

We mentioned the Tate–Shafarevich group $Ш(A/K)$ of abelian varieties in relation to the congruent number problem. Here is a more detailed version of the role of this group in the congruent number problem. The role is *via* a(n open) million dollar prize problem called the 'Birch–Swinnerton Dyer conjecture'. We already talked about the local-to-global nature of many number theoretic problems. For instance if we have a 'quadratic form' $ax^2 + by^2 + cz^2$ with a, b, c non-zero integers, then the question of existence of integer roots is solved by reducing it to local conditions. More precisely, Legendre solves this problem as follows. If a, b, c are square-free and pairwise coprimes, and if the equation has real solutions (equivalently, a, b, c are not all of the same sign), then the form has integer roots if and only if $-ab$ is a square modulo c, $-bc$ is a square modulo a and $-ca$ is a square modulo b.

The above example corresponds to a curve of genus 0 over the rational numbers. The curves of genus > 1 have only finitely many rational solutions (as conjectured by Mordell and proved by Faltings – we will talk about another conjecture of Shafarevich on this aspect later). The tricky case is that of curves of genus 1. This is the case that relates the congruent number problem. There is no known (= proved) way of deciding when an equation of the form $y^2 = x^3 + ax + b$ (with a, b rational and discriminant non-zero) has rational roots, and if it does, to decide whether it has infinitely many rational roots. Luckily, these curves E have a group law and the group $E(\mathbf{Q})$ of rational points is known (by Mordell) to be a finitely generated abelian group (isomorphic to) $\mathbf{Z}^r \oplus$ {a finite abelian group}, the latter consisting of points of finite order. In particular:

n is a congruent number if and only if $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{tors}$ *with* $r > 0$ *where E is the curve* $y^2 = x^3 - n^2 x$.

However, deciding when $r \neq 0$ is an unsolved question. The conjecture of Birch and Swinnerton-Dyer relates the above algebraic information r (the rank of the group of rational points) to analytic information coming from the generating function of

The conjecture of Birch and Swinnerton-Dyer relates the algebraic information r (the rank of the group of rational points) to analytic information coming from the generating function of E, called the L-function of E.

E, called the L-function of E. Using analytic information about such generating functions to deduce concrete facts is a fundamental theme in analytic number theory. For instance, the Riemann zeta function $\zeta(s)$ defined by the series $\sum_{n\geq 1} 1/n^s$ for $Re(s) > 1$, contains deep information about prime numbers. Indeed, the fact that an analytic continuation of the above series does not vanish on the whole vertical line $Re(s) = 1$ is essentially equivalent to the prime number theorem which asserts that the number of primes $\leq x$ is asymptotic to $x/\log(x)$. Even at the more basic level, the fact that the above series can be expressed as an 'Euler product' $\prod_{p\ prime}(1-1/p^s)^{-1}$ for $Re(s) > 1$ re-expresses the basic fact that every positive integer is a unique product of primes. For elliptic curves $E : y^2 = x^3 + ax + b$ with a, b integers and discriminant $\Delta(E) := -4a^3 - 27b^2 \neq 0$, one defines an L-function by means of local data. For every odd prime p not dividing $\Delta(E)$, one looks at the equation modulo p [3] If N_p is the number of solutions modulo p, then one considers the product,

$$\prod_{(p,2\Delta(E))=1} (1 - (p - N_p)p^{-s} + p^{1-2s})^{-1}.$$

[3] The condition on p means the polynomial has distinct roots modulo p.

This is the partial L-function of E and one puts in some suitable factors for the finitely many leftover primes to define the full L-function $L(E, s)$. Akin to the Riemann zeta function, the product defining $L(E, s)$ is known to converge when $Re(s) > 3/2$. It was conjectured to be analytically continuable to the whole complex plane as an analytic function and this has now been proved. The conjecture of Birch and Swinnerton-Dyer (often called BSD conjecture) predicts (in a more precise form) that $L(E, s) = c(s-1)^r +$ higher order terms, where r is the rank of $E(\mathbf{Q})$. Further, the non-zero constant c is given explicitly where, apart from local factors coming from various primes, a prominent factor is our 'Sha' $Ш(E/\mathbf{Q})$. Thereby, Sha plays a role in the BSD conjecture, and one must remember that it is not even known to be finite yet. The BSD conjecture implies that positive integers n which are $5, 6$ or 7 modulo 8 are congruent numbers. Incidentally, Fibonacci was challenged in the court of Frederic II to exhibit a right-angled triangle with rational sides and area 5 which he succeeded in do-

Incidentally, Fibonacci was challenged in the court of Frederic II to exhibit a right-angled triangle with rational sides and area 5 which he succeeded in doing.

ing. The reader could do the same (or look up the article [6]). The most striking result is due to Tunnell who showed that BSD implies the following criterion for an odd, square-free number to be a congruent number: such a natural number is a congruent number if and only if the number of ways of writing n in the form $2x^2 + y^2 + 8z^2$ is twice the number of writing it in the form $2x^2 + y^2 + 32z^2$. He also proved a similar criterion for even n (of course, assuming the BSD). The nice thing is, this is checkable and would answer the congruent number problem satisfactorily.

2. Shafarevich's Perspective on Galois Riches

The study of roots of polynomial equations was dramatically transformed by Galois. It lead to resolutions of classical Greek problems and explain the existing facts with a renewed perspective, and has continued to be a basic theme in all of mathematics. The state of the art is that many problems in number theory are related to properties of the so-called absolute Galois group – the group of automorphisms of $\overline{\mathbf{Q}}$, the field of algebraic numbers (and its subgroups). In a talk in 1994 in Oberwolfach, Shafarevich conjectured that the subgroup of this automorphism group which fixes all roots of unity is free (as a profinite group) of countable rank. Formally:

Conjecture. $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}^{ab})$ *is free profinite, of countably infinite rank.*

Here, $\mathbf{Q}^{ab}$ is the maximal abelian extension of $\mathbf{Q}$ and is generated by all roots of unity. This conjecture has been generalized by others to general algebraic number fields K (the fields K^{ab} are more mysterious than $\mathbf{Q}^{ab}$). In fact, the conjecture can be formulated for fields of rational functions over finite and other fields. In this set-up, the conjecture has been proved by Harbater when the function field is considered over an algebraically closed field. We recall that many number-theoretic results have counterparts in the set-up of function fields (especially over finite fields). The freeness of the Galois group as conjectured by Shafarevich and as

In a talk in 1994 in Oberwolfach, Shafarevich conjectured that the subgroup of this automorphism group which fixes all roots of unity is free (as a profinite group) of countable rank.

proved in the function field case by Harbater is equivalent to the freeness of a certain fundamental group.

In the Oberwolfach talk where Shafarevich made the above conjecture, he was actually talking about one of his other celebrated results obtained in collaboration with Golod. This addressed the so-called 'class field tower' problem which is about so-called Hilbert class fields of algebraic number fields. The Hilbert class field $H(K)$ contains a large amount of information about the number field K. It is, by definition, the maximal unramified, abelian extension and has the property that its Galois group $Gal(H(K)/K)$ – the group of automorphisms of $H(K)$ which reduce to the identity map on K – is isomorphic to the ideal class group of K, a very important arithmetical invariant. All ideals of the ring of algebraic integers in K become principal in the corresponding ring of $H(K)$. To point out a concrete application, if n is a positive integer and one is interested in prime numbers expressible in the form $x^2 + ny^2$ for some integers x, y, then this can be completely deciphered by going to $H(\mathbf{Q}(\sqrt{-n}))$ (more correctly, the ring class field $H(\mathbf{Z}[\sqrt{-n}])$, a slight generalization of the Hilbert class field). Here, $\mathbf{Q}(\sqrt{-n})$ is the quadratic field consisting of all complex numbers of the form $a + b\sqrt{-n}$ where a, b are rational numbers, and $\mathbf{Z}[\sqrt{-n}]$ is made up of those numbers where a, b are integers. The criterion is a prime p not dividing n, is expressible as $p = x^2 + ny^2$ for integers x, y if and only if, $-n$ is a square modulo p and the smallest degree polynomial with top coefficient 1 of α has a root modulo p, where α generates $H(\mathbf{Z}[\sqrt{-n}])$ over the quadratic field $\mathbf{Q}(\sqrt{-n})$. Having motivated that the Hilbert class field is an important invariant, we describe what the class field tower problem is. Furtwangler who made fundamental contributions to class field theory conjectured in 1925 that for a number field K, the tower of finite field extensions,

$$K_0 = K, K_1 = H(K_0), K_2 = H(K_1), \cdots,$$

always stabilizes; that is, just a finite tower. However, in 1965, Shafarevich (in collaboration with Golod) showed this to be false. They showed for instance that the field $K = \mathbf{Q}(\sqrt{-3.5.7.11.13.17})$ has an infinite tower!

The criterion is a prime p not dividing n, is expressible as $p = x^2 + ny^2$ for integers x, y if and only if, $-n$ is a square modulo p and the smallest degree polynomial with top coefficient 1 of α has a root modulo p, where α generates $H(\mathbf{Z}[\sqrt{-n}])$ over the quadratic field $\mathbf{Q}(\sqrt{-n})$.

To say something about how such a result is obtained, we mention that the problem about extension fields is converted, by standard procedures, into one on groups *via* Galois theory. Thus, Golod and Shafarevich proved a group-theoretic result. Recall that a presentation of a group is a set of elements which generate it and a set of relations between them which imply all the relations between the generators. They showed that if G is a finite group of p-power order for a prime p, then the minimal number d of generators and the corresponding number r of relations between them in a presentation of the group must satisfy $r > d^2/4$. In other words, when we run through a sequence of such p-groups where the number of generators goes to infinity, the number of relations also goes to infinity quadratically. Two years earlier (in 1963), Shafarevich had shown that, for a prime p, if one runs through the so-called p-parts of the Hilbert class field tower, the minimal number d_p of generators and the number r_p of relations for the corresponding pro-p groups (these are built out of a tower of finite p-groups), the numbers $r_p - d_p$ remain bounded; in particular, if the d_p's go to infinity, r_p's go to infinity not faster than d_p. Thus, the later theorem of Golod–Shafarevich shows that the corresponding pro-p groups cannot be finite; from this they deduce the infiniteness of the class field tower.

As is usual when one solves a problem by generalizing or abstractifying its setting, it yields other unrelated consequences. In fact, Golod used the Golod–Shafarevich theorem to deduce the first general examples of infinite Burnside groups[4]. We already mentioned Shafarevich's 1994 Oberwolfach talk. The talk was about the Golod–Shafarevich theorem, but Shafarevich made the conjecture on freeness of the profinite group $Gal(\overline{Q}/\mathbf{Q}^{ab})$ referred to above.

[4] Groups that are finitely generated of a given exponent.

Another outstanding gem that originated from Shafarevich's indulgence with Galois groups was his proof that every finite, solvable group occurs as a Galois group over $\mathbf{Q}$. Students, while learning basic Galois theory, realize that for the roots of a polynomial to be expressible as algebraic expressions in the radicals in the coefficients, it is necessary and sufficient (as proved by Ga-

Another outstanding gem that originated from Shafarevich's indulgence with Galois groups was his proof that every finite, solvable group occurs as a Galois group over $\mathbf{Q}$.

lois) that the corresponding Galois group (of permutations of the roots of the polynomial) has an algebraic property that has been dubbed as 'solvability'. Thus, it is of immediate interest to know if every solvable group can be realized as such a Galois group. Shafarevich proved this in 1954; a gap was pointed out in the treatment of the case of the prime 2 and a rectification was provided by Shafarevich in 1989. See [7] for a modern treatment. When we recall the famous theorem that all groups of odd order are solvable, it is remarkable that Shafarevich proved already in 1954 that all groups of odd order are Galois groups of polynomials over $\mathbf{Q}$. As a matter of fact, it is expected that all finite groups are realizable as Galois groups over $\mathbf{Q}$. This is called (a weaker version of) 'Emmy Noether's problem'.

3. Shafarevich's Extension to Groups of Infinite-Dimension

In collaboration with Kostrikin, Rudakov and others, Shafarevich studied several aspects of Lie theory, including that of Cartan pseudogroups and Lie algebras in positive characteristic. We shall only mention one topic which originated with Shafarevich. In 1965, Shafarevich introduced, for the first time, a theory of infinite-dimensional groups [8]. His model was the group of automorphisms of the polynomial ring in n variables over a field. For $\mathbf{C}[X, Y]$, the group of automorphisms was analyzed by Jung and van der Kulk who showed that this group is a so-called 'amalgamated' free product of two groups L and B amalgamated along their intersection. The group L is the group of all affine linear transformations, and B consists of the 'Joinquiére' transformations consisting of the maps $aX + f(Y)$ and $g(X) + bY$ for polynomials f, g and constants $a, b \neq 0$. To determine the group of automorphisms for general n and any field K, Shafarevich developed a theory of infinite-dimensional algebraic groups for the first time. Roughly, Shafarevich thinks of an infinite-dimensional algebraic variety to be a union $\cup_n X_n$ of finite-dimensional algebraic varieties X_n such that each X_n is closed in the successive X_{n+1}. He defines a morphism of infinite-dimensional varieties to be a map

$f : \cup_n X_n \to \cup_m Y_m$ such that the restriction of f to any X_n is a morphism to some Y_m where m is obtainable from n. In this manner, Shafarevich shows that the automorphisms of $\mathbf{C}[X_1, \cdots, X_n]$ form a group which is also an infinite-dimensional algebraic variety as above. Interestingly, in his reasoning, he assumes the truth of the as-yet unproven Jacobian conjecture[5]. In the *60th Birthday Volume I of Shafarevich*, we recall the interesting sentence with which André Weil ends his article; he says "this completes the solution found in 1765 by Euler for a problem first formulated in 1954!"

[5] This is pointed out by Hyman Bass in his article in the *60th Birthday Volume II of Shafarevich* – see [9], p.68.

4. Shafarevich's Conjecture – A Billion Variety

Shafarevich's towering presence in algebraic geometry cannot be overemphasized. His work encompasses the theory of principal homogeneous spaces of abelian varieties, elliptic surfaces, the classification of algebraic surfaces (re-proving the theorems of the Italian school in a different way), periods and arithmetic of $K3$ surfaces, theory of $K3$ surfaces of positive characteristic [10]. Here too, we discuss only one particular conjecture due to him and its special place in the developments that followed.

André Weil ends his article in the Shafarevich volume with, "this completes the solution found in 1765 by Euler for a problem first formulated in 1954!"

While discussing the BSD, we mentioned that curves have a notion of a genus and Mordell had conjectured that curves of genus > 1 have only finitely many rational points. As we said in passing, Faltings proved Mordell's conjecture in 1983. Faltings's theorem implies that equations like $x^p + y^p = 1$ for prime $p > 3$ and like $y^2 = x^5 + 2017$ have only finitely many solutions in $\mathbf{Q}$. Of course, we know now the stronger assertion that the former equation has NO non-zero solutions in $\mathbf{Q}$ (Fermat's last theorem). Writing the equation of a curve as $f(x, y) = 0$, the genus is a number which is at the most $(d-1)(d-2)/2$ where d is the degree of f. The precise expression for genus is obtained by subtracting from the above number certain numbers corresponding to all singular points (points where the three partial derivatives of the homogenized polynomial $F(X, Y, Z)$ vanish. In the case of Fermat curves, there are no singular points.

The curve $y^2 = x^3 - 17$ has 2, 3, and 17 as the primes of bad reduction.

In the method of attacking Mordell conjecture, a conjecture of Shafarevich naturally plays a role. Firstly, let us assume that the polynomial $F(X, Y, Z)$ has integer coefficients which have no common factors > 1. One may reduce the equation $F(X, Y, Z) = 0$ modulo p; that is, consider the coefficients as integers modulo p and look at solutions in the finite field of integers modulo p. We already saw this when we wrote the L-function of an elliptic curve. If the three partial derivatives of F have no common roots modulo p, the prime p is said to be of good reduction. For example, the prime 3 is a prime of bad reduction for the curve $X^3 + Y^3 = Z^3$. The curve $y^2 = x^3 - 17$ has $2, 3$, and 17 as the primes of bad reduction. Shafarevich made the following conjecture:

For a fixed genus and a fixed finite set of primes (in a number field) there are only finitely many curves over that field with good reduction outside this finite set of primes, up to isomorphism.

It enters Mordell's conjecture in the following way. Start with a curve C of genus $g \geq 2$ defined over a number field K and a point P on C with co-ordinates in K. Let S be a fixed set of primes of K. Parshin proved that one can find a bigger number field K', a curve C' defined over K' of some genus g' and a finite set S' of primes K' (where both g', S' depend only on g, S and not on the point P) and a mapping from C' to C which is unramified outside the point P. By a map being unramified over a point Q, we mean that the number of points which map to Q equals the degree of the map (if it is ramified over Q if this inverse image has less number of points). Shafarevich's conjecture would imply that such curves C' are finite in number. Therefore, if the curve C were to have infinitely many rational points, then infinitely many of the C' would be mutually isomorphic to a common curve C_0. Thus, from C_0 to C there would be infinitely many maps from C_0 to C (both of genera > 1), which is contradicted by the classical Riemann surface theory. Hence, Shafarevich's conjecture implies Mordell conjecture. What Faltings proved is Shafarevich's conjecture in a stronger form – for abelian varieties, higher-dimensional analogues of elliptic curves. We mention in

passing that although generally curves do not have group structures, one can pass to a $2g$-dimensional object called the Jacobian of a curve which has the natural structure of an abelian group. In fact, given the curve C over K (thought of over complex numbers as a Riemann surface), there is a natural $2g$-dimensional real vector space (formed by the so-called 1-forms $f(z)dz$ on C) and a lattice obtained by integrating paths such that the Jacobian is the quotient, which is a torus of dimension $2g$. More precisely, the construction of the Jacobian can be done algebraically, yielding an abelian variety defined over the number field K. The version of Shafarevich's conjecture over abelian varieties asserts that there are only finitely many (principally polarized) abelian varieties in a given dimension which have good reduction outside a given finite set of primes. Faltings proved this version of Shafarevich's conjecture (and hence the Mordell conjecture) which implies the earlier version by the so-called Torelli theorem. On the way to his proof of Shafarevich's conjecture for abelian varieties, Faltings proved the so-called Tate conjecture which he used, along with Weil conjectures to deduce his results.

Shafarevich's conjecture implies Mordell conjecture. What Faltings proved is Shafarevich's conjecture in a stronger form – for abelian varieties, higher-dimensional analogues of elliptic curves.

5. Conclusion

In this article, we have talked only about a certain selection of Shafarevich's mathematical results. It is clear from this brief introduction already that he was a true master of algebraic geometry, and number theory. Each of his results and visionary conjectures were landmarks which solved important problems and pinpointed directions in which the subject moved. Shafarevich's writings for high school students have been touched upon in another article in this issue and something of his philosophy of mathematics is described in the beginning of this note as well. On his political views, we leave the readers to follow their own Shafarevich hunt!

Suggested Reading

[1] I R Shafarevich (translated from the Russian by M Reid), *Basic Notions of Algebra*, Encyclopaedia of Mathematics, Vol.11, (258 pages), Springer-Verlag 2005.

[2] I R Shafarevich, (Translated from the Russian by Smilka Zdravkovska), Abelian and Nonabelian Mathematics, *Math. Intelligencer* Vol.13, No.1, p.67–75, 1991.

[3] I R Shafarevich, *Basic Algebraic Geometry I*, *Basic algebraic geometry II*, Springer 2013.

[4] Z I Borevich & I R Shafarevich, (Translated from the Russian by Newcomb Greenleaf), *Number Theory*, Pure and Applied Mathematics, Vol.20, Academic Press, New York-London 1966.

[5] I R Shafarevich, Foundations of Algebraic Geometry, *Russian Math Surveys*, Vol.24, pp.3–184, 1969.

[6] B Sury, A Walk Which Must Be Irrational For the Same Reason That $\sqrt{1}$ Is Not Congruent, Classroom Notes, *Resonance*, Vol.17, No.1 pp.76–82, January 2012.

[7] J Neukirch, K Schmidt & K Wingberg, *Cohomology of Number Fields*, Springer-Verlag 2000.

[8] I R Shafarevich, On Some Infinite-Dimensional Groups, *Rend. Mat. e Appl.*, Vol.25, No.1–2, pp.208–212, 1966.

[9] H Bass, The Jacobian Conjecture and Inverse Degrees, *Arithmetic and Geometry*, Papers dedicated to I R Shafarevich on the occasion of his sixtieth birthday, Vol.II, Michael Artin & John Tate (editors), Birkhauser 1983.

[10] I R Shafarevich, *Lectures on Minimal Models and Birational Transformations of Two Dimensional Schemes*, Notes by C P Ramanujam, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, No.37, Bombay, 1966.

Address for Correspondence
B Sury
Stat-Math Unit
Indian Statistical Institute
8th Mile Mysore Road
Bangalore 560 059 India.
Email: surybang@gmail.com