The work of Barry Mazur

Henri Darmon

Abstract

Barry Mazur is awarded the 2022 Chern Medal “for his profound discoveries in topology, arithmetic geometry and number theory, and his leadership and generosity in forming the next generation." This *laudatio* surveys some of the highlights of Mazur’s remarkable mathematical career.

Mathematics Subject Classification 2020

01A70

Keywords

Schoenflies conjecture, primes, knots, elliptic curves, modular curves, modular forms, Eisenstein ideal, Galois representations, deformation theory, eigencurves, Fermat’s last theorem, Iwasawa theory, p-adic L-functions, Euler systems, rational points

ICM INTERNATIONAL CONGRESS OF MATHEMATICIANS 2022 JULY 6—14

Preliminary version, to appear in Proc. Int. Cong. Math. 2022, Vol. 1.
DOI 10.4171/ICM2022/217

Barry Mazur was born in 1937 in New York City. After graduating from the Bronx High School of Science in 1954, he completed his undergraduate studies at MIT in just two years, and his PhD at Princeton University in a further two years, during which he also spent a semester in Paris, attending, among others, the seminars of Cartan and Chevalley. After a one-year stint at the Institute for Advanced Study, he joined the faculty of the Mathematics Department at Harvard in 1959, first as a member of Harvard's Society of Fellows, and currently, as the Gerhard Gade University Professor.

Through a remarkable career spanning over six decades at Harvard alone, Barry Mazur has profoundly influenced the scientific outlooks of generations of graduate students, postdoctoral fellows, and colleagues. He has shaped the modern landscape of number theory by successfully tackling the most difficult problems in the area, laying the groundwork for important theories, and initiating legions of disciples to fertile new perspectives. His scientific achievements place him squarely among the greatest mathematicians of the 20th century. The following report touches on a few of the topics, in roughly chronological order, where Barry Mazur has had a transformative impact.

1. Geometric and differential topology

(References: [1]-[19], [15]).

Barry Mazur's earliest contributions were to the field of geometric topology and differential geometry. His 1959 PhD thesis at Princeton [4] caused a sensation by proving the *generalised Schoenflies conjecture*, a higher-dimensional generalisation of the Jordan curve theorem. It asserts that an $(n-1)$-sphere S embedded in the n-sphere S^n in a way that extends to an embedding of a small thickening of S can be mapped to the standard $n-1$ sphere by a homeomorphism of S^n [4–6]. The necessity of some regularity hypotheses on the embedding is illustrated by well-known counterexamples like the Alexander horned sphere. One of Mazur's ingenious ideas in the proof is the eponymous "swindle", which demonstrates that the connected sum of two non-trivial knots or manifolds is necessarily non-trivial. The seductively simple argument is based on the fact that infinite connected sums make rigorous sense in the setting of "wild knots"; if K_1 and K_2 are knots or manifolds for which $K_1 + K_2$ is trivial, then

$$K_1 = K_1 + (K_2 + K_1) + (K_2 + K_1) + \cdots = (K_1 + K_2) + (K_1 + K_2) + \cdots = 0,$$

and likewise for K_2. Mazur was awarded the Oswald Veblen Prize of the AMS with Morton Brown in 1966 for his work on the generalised Schoenflies conjecture.

Among other key notions, Mazur also discovered, independently and at roughly the same time as Valentin Poenaru, what are now commonly referred to in the literature as "Mazur manifolds" or "Poenaru-Mazur manifolds" [7]: compact, contractible, smooth four-manifolds with boundary which are not diffeomorphic to the standard four-ball.

Mazur's article [15] on dynamical systems, in collaboration with Michael Artin, studies the space $\mathcal{F}$ of k-differentiable self-maps on a compact differentiable manifold M, equipped with the suitable (C^k) topology, and proves that there is a dense subset of $\mathcal{F}$ consist-

ing of maps whose number of isolated periodic points of period n grows at most exponentially with n. The proof is obtained by invoking an approximation theorem of Nash to reduce to an analogous statement for real algebraic varieties, which can then be tackled with the methods of intersection theory of algebraic cycles.

2. Algebraic geometry

(References: [15], [20]-[29].)

With its appealing blend of differential and algebraic methods, [15] marked a gradual widening of Mazur's mathematical interests to encompass algebraic geometry at a time when the subject was experiencing a profound renewal under the impetus of the Grothendieck school. It is during this period, in the 60's and early 70's, that Mazur produced a number of seminal works in algebraic geometry, nourished by regular visits to the IHES.

His articles [20] and [21] study the interplay between the Frobenius operator and the Hodge filtration on the de Rham cohomology of a variety V over $\mathbb{Q}_p$ admitting a smooth model over $\mathbb{Z}_p$. It establishes the fundamental "Mazur inequality", originally conjectured by Nick Katz [132], asserting that "the Newton polygon lies above the Hodge polygon". The Newton polygon measures the slopes, or valuations at p, of the eigenvalues the frobenius endomorphism acting on the i-th cristalline cohomology of V, or equivalently, of the canonical lift of Frobenius to the de Rham cohomology of V over $\mathbb{Q}_p$. The Hodge polygon encodes the dimensions of the successive quotients of this de Rham cohomology relative to the Hodge filtration. The latter invariants were classically calculated via complex transcendental methods, by studying the Hodge decomposition on the de Rham cohomology of varieties over $\mathbb{C}$. Mazur's inequality captures a fundamental feature of the behaviour of the algebraic de Rham cohomology of a variety under "mod p reduction", and provides subtle p-adic information about the zeta-functions of varieties over finite fields of characteristic p.

Mazur's treatise [22] with Messing on cristalline cohomology represents a foundational contribution to the study of p-adic cohomology theories. This subject has gradually emerged as a powerful tool for understanding the p-adic representations of the Galois groups of p-adic fields that arise from the étale cohomology of algebraic varieties. It has been vigorously developed in the past decades and acquired a growing importance in number theory, notably in the theory of motives and in the Langlands program.

Some of Mazur's later contributions incorporating perspectives from p-adic Hodge theory shall be evoked in greater detail below, most notably, in §9, his celebrated conjecture with Jean-Marc Fontaine characterising the global p-adic Galois representations realised in the p-adic étale cohomology of varieties over number fields. The theory of p-adic periods also plays a key role in extending to higher weight modular forms the definition of the $\mathcal{L}$-*invariant* of Mazur, John Tate and Jeremy Teitelbaum arising in the leading terms of certain p-adic L-functions in the presence of an "exceptional zero" (cf. §8).

Another notable achievement from roughly this period is the article [28] with M. Artin laying the foundations for a homotopy theory for schemes, based on the étale topology

which had been introduced less than a decade earlier and has since come to play a central role in arithmetic geometry.

3. Arithmetic topology

(Reference: [30].)

In his gradual transition from topology and geometry to number theory, Mazur seems to have drawn guidance and inspiration from a suggestive analogy between knots and primes.

A knot is a copy of the circle S^1 embedded in a three-sphere S^3. Many invariants of knots arise from studying the fundamental group of the knot complement. There is a beautiful and tantalising parallel between this knot complement and the complement of a prime in the scheme $\mathrm{Spec}(\mathbb{Z})$. Namely, the latter space shares some of the same homological properties as S^3 insofar as its interesting cohomology is concentrated in degree 3, whereas $\mathrm{Spec}(\mathbb{F}_p)$ behaves like a circle since its fundamental group is (topologically pro-) cyclic.

The pursuit of this analogy leads to a beguiling dictionary between number theory and knot theory, in which quadratic reciprocity resonates with the symmetry of the linking number of two knots, and the higher quadratic residue symbols of Redei can be envisaged as analogues of the higher linking of knot configurations like the famous Borromean rings, both notions being manifestations of higher Massey products.

Mazur's unpublished but widely influential manuscript [30] enriches the number theory-knot theory lexicon by explicating the parallel between the Alexander polynomial of a knot and Iwasawa's conjectural algebraic description of the Kubota-Leopoldt p-adic zeta-function as the characteristic power series of a certain Iwasawa module constructed out of ideal class groups of p-power cyclotomic fields. The Iwasawa module in question can be identified via global class field theory with the maximal abelian (pro-p) extension of the maximal abelian extension of $\mathbb{Q}$ ramified only at p. It can then be understood as the second graded piece relative to a natural filtration on (the pro-solvable completion of) the fundamental group of the complement of $\mathrm{Spec}(\mathbb{F}_p)$ in $\mathrm{Spec}(\mathbb{Z})$. Iwasawa's interpretation of the p-adic zeta-function resembles the Alexander polynomial of a knot K, which encodes the characteristic polynomial of a generator of the homology of the knot complement acting on the next graded piece in the filtration of $\pi_1(S^3 - K)$ given by its derived central series.

The rich analogy between knots and primes which guided Mazur in his transition from topology to number theory has subsequently spawned an entire new field, known as *arithmetic topology*, which is elegantly described in the recent textbook of Masanori Morishita [138]. (See also [146] for further striking manifestations of the analogy.)

4. Torsion subgroups of elliptic curves

(References: [32]-[38], [122].)

The deep and systematic study of rational torsion points on elliptic curves carried out in roughly the decade from 1975 to 1985 stands among Mazur's landmark contributions to number theory.

An elliptic curve over a field F is a smooth projective curve E of genus one over F equipped with a distinguished rational point $O \in E(F)$. What makes these curves particularly rich arithmetically is that they are endowed with the structure of a projective *algebraic group*. In particular, the set $E(\mathbb{Q})$ of rational points on an elliptic curve over $\mathbb{Q}$ is an abelian group, known to be finitely generated by the Mordell-Weil theorem, and thus is isomorphic to

$$E(\mathbb{Q}) = \mathbb{Z}^r \times T,$$

where T is a finite group, called the *torsion subgroup* of E over $\mathbb{Q}$. Mazur's celebrated theorem [36] lists all the possibilities for the groups T that can arise in this way:

Theorem 4.1. *The torsion subgroup T of an elliptic curve over $\mathbb{Q}$ can only be isomorphic to one of the following* 15 *groups:*

$$\mathbb{Z}/n\mathbb{Z}, \text{ with } 1 \le n \le 10 \text{ or } n = 12, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ with } n = 2, 4, 6, \text{ or } 8.$$

This striking result was apparently anticipated by the Italian geometer Beppo Levi [142] in 1908. It became more widely known as a precise conjecture formulated by Andrew Ogg [139] and provides the backdrop for an active area of investigation to which mathematicians like Kamienny [130], Merel [135], and many others, have made important subsequent contributions. Indeed the study of rational points on modular curves remains a lively terrain of investigation to which a variety of approaches grounded in the pioneering insights of [36] have been applied (cf. for instance [133], [134] [136], [137], [128], [127], ...).

Beyond the appealing nature of the final statement "for its own sake", the perspectives that Mazur introduced into the subject in order to prove Theorem 4.1 also had a tremendous impact on other related developments. Both the statement and the proof of Theorem 4.1 are indispensable ingredients in the proof of the modularity of elliptic curves and of Fermat's Last Theorem, as will be explained further in Sections 5, 6, and 10.

In a subsequent article [37], Mazur also classifies the primes N for which there are elliptic curves over $\mathbb{Q}$ possessing a rational subgroup of order N, i.e., a non-trivial isogeny of degree N defined over $\mathbb{Q}$, simplifying his earlier proof of Theorem 4.1 at the same time:

Theorem 4.2. *Let N be a prime number such that some elliptic curve admits an isogeny of degree N defined over $\mathbb{Q}$. Then $N = 2, 3, 5, 7, 13$ (with infinitely many possible E for each N) or $N = 11, 17, 19, 37, 43, 67,$ or 163.*

The values $N = 11, 17, 19, \ldots, 163$ are primes for which the imaginary quadratic field $\mathbb{Q}(\sqrt{-N})$ has class number one. Elliptic curves with complex multiplication by the maximal orders of these fields admit models over $\mathbb{Q}$ and the kernel of multiplication by $\sqrt{-N}$ gives a cyclic subgroup of order N in E, defined over $\mathbb{Q}$. It is a measure of the delicacy of Mazur's

argument that it accounts for these arithmetically non-trivial exceptions while ruling out all other eventual occurrences.

Theorem 4.1 has been extended by Sheldon Kamienny, leading to the classification of possible torsion subgroups for elliptic curves defined over number fields of small degree over $\mathbb{Q}$ (cf. [130] and [38]). The most definitive result in this direction was then obtained by Loïc Merel [135], who showed that the torsion subgroups of elliptic curves defined over a number field K are bounded by a constant B_K depending only on K, and indeed, only on the degree of K over $\mathbb{Q}$.

5. Rational points on modular curves

Theorems 4.1 and 4.2 can be recast in terms of rational points on *modular curves*, which arise naturally as *moduli spaces* parametrising isomorphism classes of elliptic curves with auxiliary "level structures".

If E is an elliptic curve over a field F in which 6 is invertible, there are two rational functions x and y which are regular on $E - \{O\}$, have poles of order 2 and 3 respectively at O, and satisfy an equation of the form

$$y^2 = x^3 + ax + b, \qquad \text{with } a, b \in F.$$

The functions x and y are uniquely determined by these properties up to replacing (x, y) by (t^2x, t^3y) for some $t \in F^\times$, which has the effect of replacing the coefficients (a, b) by (t^4a, t^6b). In particular, the expression

$$j(E) := 1728\frac{4a^3}{4a^3 + 27b^2},$$

known as the j-invariant of E, depends only on (the $\bar{F}$-isomorphism class of) E and not on the choice of x and y. It is in fact a complete isomorphism invariant: two elliptic curves over F are isomorphic (over the algebraic closure of F) precisely when they have the same j-invariant. The affine j-line, viewed as an algebraic curve over $\mathbb{Q}$, is thus a (coarse) moduli space of elliptic curves: its points over any field F of characteristic zero are in bijection with the $\bar{F}$-isomorphism classes of elliptic curves over F. This affine j-line is the simplest instance of a *modular curve*.

More interesting examples can be obtained by classifying elliptic curves *with extra level structure*. A typical level N structure on E amounts to the datum of a subgroup or a point of order N on E, or eventually a basis for the full N-torsion of E. The curves that classify solutions of these problems are commonly denoted $Y_0(N)$, $Y_1(N)$, and $Y(N)$ respectively. They are affine curves over $\mathbb{Q}$, which can be completed to smooth projective curves by adjoining to them a finite set of cusps: the resulting projective curves are called $X_0(N)$, $X_1(N)$, and $X(N)$.

The following is merely a reformulation of Theorem 4.2 from the perspective of rational points on modular curves:

Theorem 5.1. *Let N be a prime number for which $Y_0(N)(\mathbb{Q})$ is non-empty. Then $N = 2, 3, 5, 7, 13$ (when $X_0(N)$ is isomorphic to the projective line, and has infinitely many rational points) or $N = 11, 17, 19, 37, 43, 67,$ or 163 (when $Y_0(N)$ contains a finite set of "sporadic" rational points).*

Concrete (but ultimately not very useful) equations for modular curves can be written down. If E and E' are related by a cyclic isogeny of degree N, then their j-invariants j and j' give rise to a root (j, j') of the so-called *modular polynomial* $\Phi_N(x, y)$, which is a rational polynomial of bidegree $N + 1$ when N is a prime number. The curve $Y_0(N)$ is birationally equivalent to the plane curve defined by this polynomial. These defining equations tend to be quite complicated. For instance,

$$\begin{aligned}\Phi_2(x, y) \quad = \quad & x^3 - x^2y^2 + 1488x^2y - 162000x^2 + 1488xy^2 + 40773375xy \\ & +8748000000x + y^3 - 162000y^2 + 8748000000y - 157464000000000,\end{aligned}$$

and tackling the associated diophantine equations through a direct elementary approach seems decidedly unpromising.

Mazur's opening gambit is to embed the modular curve — $X_0(N)$, say — in its *Jacobian* $J_0(N)$, an abelian variety whose rational points can then be studied through Fermat's method of infinite descent, in the conceptual modern framework given for it by André Weil, in which the consideration of explicit equations can largely be avoided.

Mazur is able to show that if N is a prime for which $J_0(N)$ is non-trivial (i.e., if $N = 11$ or $N > 13$) then this jacobian admits non-trivial quotients with finite Mordell-Weil group over $\mathbb{Q}$, which he calls *Eisenstein quotients*. This immediately implies, a decade before Faltings' proof of the Mordell conjecture, that $X_0(N)$ has finitely many rational points whenever it has genus ≥ 1, and, with more care, can be used to derive bounds on the set of rational points sufficiently precise to deduce Theorem 4.1, and, with even greater care, Theorem 4.2.

The Eisenstein quotients of $J_0(N)$ are attached to the different primes p dividing the numerator of $(N - 1)/12$, and denoted $J^{(p)}_{\text{eis}}(N)$. The Mordell-Weil group $J^{(p)}_{\text{eis}}(N)(\mathbb{Q})$ contains an element of order p, and it becomes natural to calculate this Mordell-Weil group by a p-descent argument involving the Selmer group for a p-torsion module on which the Galois group of $\mathbb{Q}$ acts through an abelian quotient. The "Eisenstein descent" which Mazur developed for this purpose thus places the study of $J^{(p)}_{\text{eis}}(\mathbb{Q})$ in proximity with more classical questions surrounding the class groups of cyclotomic fields.

In constructing $J^{(p)}_{\text{eis}}$ and establishing the finiteness of its Mordell-Weil group, Mazur is able to marshal several special features of modular curves that make their diophantine properties more amenable to analysis. Most critically, modular curves are endowed with a plentiful supply of algebraic correspondences over $\mathbb{Q}$, which emerge naturally from their moduli description and are geometric incarnations of *Hecke operators*. The resulting endomorphisms break up $J_0(N)$ into arithmetically simpler pieces with a large endomorphism algebra, whose Tate modules give rise to (compatible systems of) two-dimensional ℓ-adic representations of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. These abelian variety quotients "of $\mathbf{GL}(2)$ type" offer a fertile testing ground for the general program of understanding linear representations of the Galois

groups of number fields, a cornerstone of the Langlands program. The two-dimensional representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ represent a prototypical first step in this program, going beyond the abelian setting of global class field theory. It is partly for this reason that Mazur's Eisenstein descent has largely transcended in importance the diophantine application for which it was originally designed. The ideas Mazur introduced into the subject have played a key role, notably, in Andrew Wiles' proof [148] almost 20 years later of the Taniyama-Weil conjecture on the modularity of elliptic curves over $\mathbb{Q}$, as will be explained further below.

The non-trivial point of order p on $J_0(N)$ which Mazur so spectacularly exploits in his proofs of Theorems 4.1 and 4.2 arises from the image of a divisor supported on the cusps of $X_0(N)$. In addition to the cusps, the modular curve $X_0(N)$ is also endowed with a plentiful supply of points defined over various ring class fields of imaginary quadratic fields – the *Heegner points* arising from the moduli of suitable elliptic curves with complex multiplication. A formula of Benedict Gross and Don Zagier connects the heights of these points to the first derivatives of the Hasse-Weil L-series of abelian variety quotients of $J_0(N)$. In the late 1980's, Victor Kolyvagin parlayed this connection into a proof of the finiteness of the Mordell-Weil group of any quotient of $J_0(N)$ whose Hasse-Weil L-series does not vanish at the center, consistent with the Birch and Swinnerton-Dyer conjecture for these quotients. The somewhat larger quotient of $J_0(N)$ with finite Mordell-Weil group that emerges from Kolyvagin's theorem is called the *winding quotient* (a terminology that can be traced back to Mazur's "winding element" [42]). The winding quotient was later exploited to great effect by Merel in his extension of Theorem 4.1 to number fields of arbitrary degree [135].

6. Fermat's Last Theorem

Mazur's theorem 5.1 on rational points on modular curves asserts that an infinite collection of curves, of increasing genus and arithmetic complexity – the modular curves $X_0(N)$ indexed by the parameter N – have no rational points except the trivial ones when N is large enough. This statement is reminiscent of Fermat's Last Theorem, which makes the same assertion for the Fermat curves F_N with equation

$$F_N : x^N + y^N = z^N.$$

The relation between the two statements goes far beyond a superficial analogy. Theorem 5.1 turns out to be a critical ingredient – indeed, the key diophantine ingredient – in the proof of Fermat's Last Theorem.

The tight connection between the diophantine properties of modular curves and Fermat curves can seem surprising at first, since only rarely are there explicit maps between the two types of curves. A charming exception to this statement is the modular curve $X(7)$ with full level 7 structure, a genus 3 curve having a maximal size automorphism group for its genus, the group $\mathbf{PSL}(2,7)$ of order 168. This property determines it uniquely up to isomorphism over $\bar{\mathbb{Q}}$, and a model for it is provided by the famous *Klein quartic* with equation

$$X(7) : u^3v + v^3w + w^3u = 0.$$

It turns out that $X(7)$ is the image of the Fermat curve

$$F_7 : x^7 + y^7 + z^7 = 0$$

under the degree 7 map $\pi : F_7 \to X(7)$ sending $(x, y, z) \in F_7$ to

$$(u, v, w) = \pi(x, y, z) := (x^3 z, y^3 x, z^3 y).$$

A non-trivial solution to Fermat's Last Theorem would thus give rise to a non-trivial rational point on $X(7)$, and the assertion that this modular curve has no non-trivial rational points (satisfying $uvw \neq 0$) therefore implies Fermat's last theorem for exponent 7. More interesting is the converse implication that was first proved by Hurwitz, namely, that $X(7)$ has no non-trivial rational points because the same is true for F_7. (At the time, Fermat's last theorem for exponent 7 was already known through the work of Lamé.) Hurwitz notes that if (u, v, w) is a point on the Klein quartic with integer coordinates, satisfying $\gcd(u, v, w) = 1$, then these coordinates need not be pairwise coprime. Setting

$$x = \gcd(u, v), \quad y = \gcd(v, w), \quad z = \gcd(w, u),$$

a direct reasoning involving the fundamental theorem of arithmetic shows (after changing the signs of x, y, and/or z if necessary) that (x, y, z) lies on the Fermat curve F_7 and that $\pi(x, y, z) = (u, v, w)$. Through this argument, Hurwitz shows that the map $\pi : F_7 \to X(7)$ is surjective on rational points. Unlike the purely algebraic implication

$$F_7 \text{ has a non-trivial rational point} \quad \Rightarrow \quad X(7) \text{ has a non-trivial rational point,} \qquad (6.1)$$

the reverse implication is more genuinely arithmetic, resting on ingredients like unique factorisation. Essential for this implication is the fact that the degree 7 map π (viewed as a map of Riemann surfaces, on the complex points of the curves, say) is *everywhere unramified*.

The proof of Fermat's last theorem for the general (prime) exponent p rests on an analogous but substantially more general geometric relation between the modular curve $X(2p)$ and the p-th Fermat curve F_p. Namely, both are equipped with natural surjective maps

$$F_p \xrightarrow{\pi_1} \mathbb{P}_1 \xleftarrow{\pi_2} X(2p)$$

to the projective line $\mathbb{P}_1$ with "common local features". The map π_1 sends the Fermat triple (x, y, z) to x^p/y^p, and the map π_2 is simply the one that "forgets about the level p structure", sending a point on $X(2p)$ to its natural image in $X(2)$, identified with the projective line by viewing $\lambda \in \mathbb{P}_1$ as the parameter in the Legendre family of elliptic curves

$$y^2 = x(x - 1)(x - \lambda).$$

Although they have different degrees and are defined on different curves, the maps π_1 and π_2 exhibit the following striking affinity: they are both ramified only at 0, 1 and ∞, and their ramification degrees at these three points are equal to p. This suggests that, if $(a, b, c) \in F_p(\mathbb{Q})$ is a non-trivial solution to Fermat's last theorem, then the image $\pi_1(a, b, c) = a^p/b^p \in \mathbb{P}_1(\mathbb{Q})$ ought to lift to a point of $X(2p)$ whose field of definition exhibits a *limited amount*

of ramification, bounded independently of the solution (a, b, c). One is led to study the field generated by the p-division points of the "Frey elliptic curve"

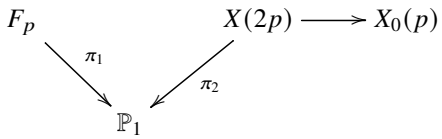
$$E_{a,b,c} \ : \ y^2 = x(x - a^p)(x + b^p),$$

which is indeed (after eventually re-ordering a, b and c appropriately, and modifying their signs) unramified outside of 2 and p.

The ultimate proof of Fermat's Last theorem rests on a supremely delicate analysis of this field, or, better yet, of the $\mathbb{Z}/p\mathbb{Z}$- linear representation

$$\varrho_{a,b,c} \ : \ G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E_{a,b,c}[p]) \simeq \mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

of the absolute Galois group of $\mathbb{Q}$ acting on the p-torsion points of $E_{a,b,c}$. The startling insight that emerged from the work of Gerhard Frey, Jean-Pierre Serre [143], and Kenneth Ribet [141], is that the modularity of $E_{a,b,c}$, which was ultimately proved by Wiles [148], can be parlayed into the conclusion that $\varrho_{a,b,c}$ is necessarily *reducible*. Because of this, any non-trivial solution $(a, b, c) \in F_p(\mathbb{Q})$ to Fermat's last theorem can be transferred to a non-trivial rational point on $X_0(p)$, by chasing it through the following diagram of maps of curves:



Thanks to the implication

$$F_p \text{ has a non-trivial rational point} \quad \Rightarrow \quad X_0(p) \text{ has a non-trivial rational point,} \tag{6.2}$$

(which is reminiscent of (6.1), is even closer in spirit to its converse, and is considerably deeper than either statement), a Diophantine question about the Fermat curves F_p is reduced to the same question about the modular curves $X_0(p)$: precisely the question that is answered in Mazur's Theorem 5.1.

As will be further explained in Section 10, the ideas that Mazur introduced to prove Theorem 5.1 are also instrumental in the the proof of (6.2): they are thus woven into the very fabric of Wiles' extraordinary proof of the Taniyama-Weil conjecture and of Fermat's last theorem.

7. Iwasawa Main conjectures

(References: [45], [47], [51].)

The proof of the main conjecture of Iwasawa theory by Mazur and Wiles [47] is another milestone of number theory, occurring roughly a decade before the proof of Fermat's last theorem. Iwasawa theory starts with the fact that the p-parts of the ideal class groups of the p-power cyclotomic fields, obtained by adjoining to $\mathbb{Q}$ the p^n-th roots of unity, exhibit a remarkably regular growth as a function of n. The main conjecture of Iwasawa theory ties this behaviour to the zeroes of the Kubota-Leopoldt p-adic zeta-function. It grew

out of an analogy with Weil's formulation of the Riemann hypothesis for varieties over finite fields, and can be envisaged as its counterpart in a p-adic setting, insofar as it assigns to the mysterious zeroes of the p-adic zeta function a *spectral interpretation*. Namely these zeroes are the eigenvalues of a certain operator – a topological generator of the Galois group of the cyclotomic $\mathbb{Z}_p$-extension generated by all p-power roots of unity – acting on an Iwasawa module formed by piecing together the ideal class groups of the finite layers of this $\mathbb{Z}_p$-extension. A remarkable feature of the proof of Mazur and Wiles is that it rests on a careful study of the two-dimensional Galois representations arising from the quotients of the jacobians of modular curves, particularly those that are *reducible*, to prove a statement that is ostensibly part of the more classical abelian theory of class groups of cyclotomic fields. Global class field theory is used to convert questions about class groups into ones about constructing unramified abelian extensions of cyclotomic fields, and the extensions that are predicted to arise from the zeroes of the p-adic zeta function are ultimately shown to be cut out by the Galois representations arising from the p-power torsion points of these modular jacobians.

The proof of the Iwasawa Main conjecture — justifying the analogy between the p-adic zeta function of Kubota-Leopoldt and the Alexander polynomial of a knot which Mazur had perceived decades earlier — stands as one of the notable achievements in number theory in the latter half of the 20th century. Its method has been vastly generalised, notably by Wiles for totally real fields **[147]**, and by Chris Skinner and Eric Urban **[144]** in the setting of elliptic curves, a framework which also owes much to Mazur's vision and will be discussed in the following section.

8. Elliptic curves and the Birch and Swinnerton-Dyer conjecture

(References: **[40]** — **[44]**, **[46]**, **[48]**, **[50]**, **[52]**, **[56]**, **[58]**, **[101]**.)

Throughout the 1970's and 1980's, Mazur reflected extensively on the arithmetic of elliptic curves, focusing on the most notoriously difficult and central open problem in the area: the Birch and Swinnerton-Dyer conjecture. Rather than tackling the problem head-on, he initiated a parallel study in the p-adic setting, opening up a new terrain of investigation which has been remarkably fruitful and witnessed decades of sustained progress.

The article **[41]** champions the introduction of Iwasawa-theoretic ideas in the arithmetic study of elliptic curves and abelian varieties. The relevant Iwasawa modules are obtained by replacing the p-parts of ideal class groups with relevant p-Selmer groups over the finite layers of a $\mathbb{Z}_p$-extension, appropriately pieced together. The importance of this new perspective can hardly be overstated: entire mathematical careers (the author's among them) have been enjoyably spent fleshing out Mazur's vision for the Iwasawa theory of abelian varieties over towers of number fields.

Mazur's article **[42]** with Peter Swinnerton-Dyer introduces what has since come to be known as the Mazur–Swinnerton-Dyer p-adic L-function of an elliptic curve over $\mathbb{Q}$, the direct counterpart of the Hasse-Weil L-function in the p-adic world. Relating analytically

defined p-adic L-functions like this one to the characteristic power series of Mazur's Iwasawa modules leads to a rich variety of "Iwasawa main conjectures" for elliptic curves.

The foundations that are laid in [41] and [42] lead naturally to a *p-adic analogue* of the Birch and Swinnerton-Dyer conjecture, which was formulated roughly ten years later in a profoundly influential article [50] by Mazur, Tate and Teitelbaum.

The p-adic Birch and Swinnerton Dyer conjecture is more tractable than its archimedean precursor, because of the tight connection one can hope to establish between p-adic L-functions and Mazur's Iwasawa modules, as expressed in the main conjecture. The main conjecture explains why elliptic curves of large rank, for example, ought to exhibit high order zeroes in their associated p-adic L-functions: it is because the Mordell-Weil group provides a subspace of the relevant Iwasawa module that is fixed by Galois and thus contributes to the multiplicity of the trivial character as a zero of the p-adic L-function.

Such a spectral interpretation is sorely lacking for the zeroes of the Hasse Weil L-function in the archimedean setting, and indeed there is not a single elliptic curve over $\mathbb{Q}$ whose L-series can be shown to vanish to order > 3 at $s = 1$, although elliptic curves of rank > 3 (and even > 23) are known to exist in relative abundance.

In the non-archimedean framework that Mazur pioneered, the situation is better understood. The requisite divisibility in the main conjecture for elliptic curves over $\mathbb{Q}$ was shown by Kazuya Kato in the early 1990's by exploiting, much as Kolyvagin with Heegner points, special elements in the K-theory of modular curves arising from pairs of Siegel units and (crucially) their p-adic deformations [131]. Thanks to Kato's result, the Mazur–Swinnerton-Dyer p-adic L-function of an elliptic curve is known to vanish to order at least the rank of the Mordell-Weil group.

The opposite divisibility in the main conjecture for elliptic curves was established by Skinner and Urban [144], by building on the very different circle of ideas that arose in the proof of the original Iwasawa main conjecture by Mazur and Wiles. Significant mysteries relating to the finiteness of the Shafarevich-Tate group and non-degeneracies in p-adic heights (and the eventual non-semisimplicity of the relevant Iwasawa modules) still prevent this divisibility in the main conjecture from leading to the correct upper bound on the order of vanishing of the p-adic L-function. So the p-adic Birch and Swinnerton-Dyer conjecture of Mazur, Tate and Teitelbaum still offers alluring mysteries in spite of its relative accessibility compared to the original archimedean conjecture.

Another appealing feature of the p-adic Birch and Swinnerton-Dyer conjecture is the appearance of new phenomena that seem to have no immediate counterpart in the archimedean setting, most notably, the phenomenon of *exceptional zeroes* of p-adic L-functions that can arise, for instance, from the vanishing of an Euler factor at p that needs to be inserted to ensure the interpolation of the special values.This phenomenon was first observed and explored in [50]. While they may appear somewhat specialised to the uninitiated, leading terms of p-adic L-functions at points where there is an exceptional zero encode rich arithmetic information, and their careful examination is often rewarded with fruitful new insights. The original "exceptional zero conjecture" of Mazur, Tate and Teitelbaum involved the Tate p-adic period of an elliptic curve with multiplicative reduction. A series

of suggestive proposals have been formulated to extend this conjecture to modular forms of higher weight, notably by Jeremy Teitelbaum [145] in terms of the Cerednik-Drinfeld theory of p-adic uniformisation of Shimura curves, and by Fontaine and Mazur [67], exploiting the filtered frobenius monodromy module which p-adic Hodge theory attaches to the local p-adic Galois representation of a modular form of higher weight. As a further instance of the importance of exceptional zeros, let us mention that they also sometimes arise in p-adic L-series attached to totally odd characters of totally real fields at $s = 0$, where they are central to Gross's p-adic variant of the Stark conjectures.

Towards the end of the 1980's, Mazur also introduced, in collaboration with John Tate, a *tame refinement* of the p-adic Birch and Swinnerton-Dyer conjecture which consists, roughly speaking, in replacing the Iwasawa algebra – the completed group ring of the Galois group of a $\mathbb{Z}_p$ extension – by the group ring of the Galois group of a finite abelian extension [52]. The more refined conjectures that emerge from the tame framework turn out to offer a congenial setting in which to study and organise the behaviour of Euler systems, and these ideas have undergone something of a recent revival, notably through their connections with conjectures of Harris and Venkatesh concerning Venkatesh's "derived Hecke operators" acting on the cohomology of coherent sheaves on modular curves attached to modular forms of weight one [129].

9. The Fontaine-Mazur conjecture

Like many of the great number theorists of the 20th century, Mazur has contributed significantly to the study of Galois representations and their connection with automorphic forms. These ideas are central to a number of the achievements of Mazur that have already been recounted.

One of Mazur's important contributions in this direction is the deep conjecture, formulated in [71] with Jean-Marc Fontaine, which has widely come to be known as the *Fontaine-Mazur conjecture*. It aims to characterise the global p-adic Galois representations that arise from the p-adic étale cohomology of varieties over number fields. The characterisation is via their restriction to the decomposition group at p (one demands that these p-adic representations of the Galois groups of p-adic fields be *potentially semistable*, a notion based on comparison functors between p-adic étale cohomology over p-adic fields and the p-adic cohomologies studied by Mazur in earlier decades) combined with a natural requirement of otherwise being ramified at finitely many primes other than p. This conjecture provides an elegant framework in which much of the recent progress on the Langlands program can be understood and conceptualised.

10. Deformations of Galois representations

(References: [53], [54], [61], [73], [75], [76], [78], [108].)

The p-adic variation of modular forms and Galois representations is a theme that underlies much of Mazur's work in number theory, starting with his early work on the Eisenstein ideal. His fundamental article [53] formalizes this notion on the Galois theory side by introducing the *universal deformation ring* attached to a Galois representation with coefficients in a complete local ring. With this idea, Mazur launched the new field of Galois deformation theory, which almost immediately after its inception found a spectacular application in Wiles' proof of the Taniyama-Weil conjecture. This proof proceeds by constructing a natural map from one of Mazur's universal Galois deformation rings to a suitably completed ring of Hecke operators, and showing this map is an isomorphism. The deep study of the ring theoretic structure of completed Hecke algebras had already been initiated, more than a decade earlier, in Mazur's work on the Eisenstein ideal. With the introduction of universal deformation rings, Mazur can be credited for a substantial part of the theoretical infrastructure that enabled the proof of the Taniyama-Weil conjecture. Mazur's ideas are thus present in the very foundations of the remarkably successful strategy for establishing the modularity of Galois representations that has been extensively developed and generalized in the wake of Wiles' breakthrough on the modularity of elliptic curves.

Mazur's subsequent work [73], [78] with Robert Coleman represents an attempt to partially globalise the study of deformation spaces of Galois representations, leading to the fundamental notion of Coleman-Mazur "eigencurves" and "eigenvarieties". The framework initiated by Coleman and Mazur in these foundational papers has been extensively developed in the past decades, spawning a fruitful area that underlies much of the recent progress in the Langlands program via p-adic methods.

11. Diophantine geometry

(References: [49], [62], [68], [70], [72], [79], [86], [95], [100].)

Mazur's work on diophantine geometry distinguishes itself by insights that are often stunning in their audacity. The article [62] ventures the striking conjecture that if the rational points of a variety V are Zariski dense, then their topological closure in $V(\mathbb{R})$ for the real topology is a union of connected components of $V(\mathbb{R})$.

Just as far reaching are the celebrated conjectures Mazur formulated with Lucia Caporaso and Joe Harris [70], [72], asserting that the number of rational points on a curve of genus g over a number field K is *uniformly bounded* by a constant that depends only on g and K, and even just on g if one tolerates a finite number of exceptions. In [70] it is shown that this conjecture, which is both remarkably strong and pleasingly concrete, follows from the earlier, and at the time more widely accepted, conjecture of Lang that the set of rational points on a variety of general type can never be Zariski dense.

Such fearless conjectures, applying to all varieties at once or to the number of points on all curves of given genus, shine an unexpected light on venerable questions about rational points and have guided a lot of subsequent efforts by other researchers.

Many of Mazur's articles devoted to diophantine topics reveal unexpected connections to other mathematical themes. This is the case, notably, for [109] and [114], which study the variation in 2-Selmer ranks of elliptic curves over number fields, revealing a surprising connection between the notion of "Diophantine stability" and Hilbert's tenth problem concerning the undecidability of diophantine questions over certain number fields.

12. Euler systems and related areas

(References. [92] [99], [104], [106], [110], [115], [117], [118], [119], [120].)

The method of *Euler systems* is a powerful technique that emerged in the late 1980's from the works of mathematicians like Francisco Thaine, Karl Rubin, Victor Kolyvagin, and Kazuya Kato. It parlays the presence of special elements in the global Galois cohomology of (a compatible system of) p-adic Galois representations into a proof of at least one inequality in the associated main conjecture. The existence of the global elements making up an Euler system is still poorly understood, and their construction remains as much an art as a science.

The articles [92] [99], [104], [110], [119], and [120], all joint with Karl Rubin, are part of a systematic attempt to formalise (via the notion of what the authors call a "Kolyvagin system") the procedure whereby such norm-compatible collections of global classes with ties to L-function behaviour can be exploited to obtain results in the direction of a main conjecture, or possibly a tame counterpart in the spirit of [52]. The perspectives introduced by Mazur and Rubin have had a decisive influence on an entire generation of researchers who are currently exploring the ramifications of the Euler system method.

13. Exposition

(References. [59], [63], [75], [83], [87], [89], [93], [97], [105], [107], [112], [113], [116], [121], [124], [126].)

Mazur is a master expositor who revels in the joy of mathematical and philosophical ideas. He is the author of a fascinating, eclectic collection of essays in which his erudition and intellectual curiosity range far and wide. Some of these essays are devoted to broad mathematical topics like local-global principles in number theory [63], the deformation theory of Galois representations [75], diophantine questions related to perfect powers [83], the general idea of deformation in various parts of mathematics [93], the notion of a motive [97], the Sato-Tate conjecture [105], and the Riemann hypothesis [121]. Others examine ideas through the lense of their historical development, treating complex numbers as they were envisioned in the 16th Century [87], or Hermann Weyl's foundational article on spectral theory [112]. Mazur also ventures into more philosophical topics like dreams in mathematics told through an evocation of Kronecker's *Jugendtraum* [113], the concept of number and mathematical abstraction [89], the subtle and elusive concept of equality in mathematics [107], the notion of plausiblity [116],

the overarching unity of mathematics [124], and thoughts on doing mathematics during the pandemic [126]. Mazur's infectious enthusiasm easily transmits itself to the reader, and his reflections on a diverse range of mathematical, historical and philosophical subjects never fail to delight, uplift, and enlighten. (The range and depth of Mazur's intellectual interests are vividly evoked in the engaging documentary movie "Barry Mazur and the infinite cheese of knowledge" directed by Oliver Ralfe [140].)

14. Mentorship

According to the Mathematics genealogy website, Mazur has had (at least) 57 students and 325 descendants, figures that are bound to be obsolete by the time this *laudatio* goes to press. Beyond the direct impact he has had on his students, Mazur has shaped the views of an entire generation of number theorists who have been enriched by his ideas and enjoyed the privilege of pursuing his capacious intellectual legacy. This legacy, which is now being recognised through the awarding of the Chern medal, is a central and integral part of modern number theory and its influence will be felt for a very long time.

References

[1] B. Mazur. The definition of equivalence of combinatorial imbeddings. *Inst. Hautes Etudes Sci. Publ. Math.* **1959** (1959), 97–109.

[2] B. Mazur, On the structure of certain semi-groups of spherical knot classes. *Inst. Hautes Etudes Sci. Publ. Math.* **1959** (1959), 111–119.

[3] B. Mazur, Orthotopy and spherical knots. *Inst. Hautes Etudes Sci. Publ. Math.* **1959** (1959), 121–140.

[4] B. Mazur, *On embeddings of spheres*. Ph.D. thesis Princeton University, 1959.

[5] B. Mazur, On embeddings of spheres. *Bull. Amer. Math. Soc.* **65** (1959), 59–65.

[6] B. Mazur, On embeddings of spheres. *Acta Math.* **105** (1961), 1–17.

[7] B. Mazur, A note on some contractible 4-manifolds. *Ann. of Math.* (2) **73** (1961), 221–228.

[8] B. Mazur, Stable equivalence of differentiable manifolds. *Bull. Amer. Math. Soc.* **67** (1961), 377–384.

[9] B. Mazur, Simple neighborhoods. *Bull. Amer. Math. Soc.* **68** (1962), 87–92.

[10] B. Mazur, Symmetric homology spheres. *Illinois J. Math.* **6** (1962), 245–250.

[11] B. Mazur, Relative neighborhoods and the theorems of Smale. *Ann. of Math.* (2) **77** (1963), 232–249.

[12] B. Mazur, Differential topology from the point of view of simple homotopy theory. *Inst. Hautes Etudes Sci. Publ. Math.* No. **15** (1963), 93 pp.

[13] B. Mazur, The method of infinite repetition in pure topology. I. *Ann. of Math. (2)* **80** (1964), 201–226.

[14] B. Mazur, Combinatorial equivalence versus topological equivalence. *Trans. Amer. Math. Soc.* **111** (1964), 288–316.

[15] M. Artin and B. Mazur, On periodic points. *Ann. of Math. (2)* **81** (1965), 82–99.

[16] B. Mazur, Morse theory. *1965 Differential and Combinatorial Topology* (A Symposium in Honor of Marston Morse) pp. 145–165, Princeton Univ. Press, Princeton, N.J.

[17] M. Artin and B. Mazur, On the van Kampen theorem. *Topology* **5** (1966), 179–189.

[18] B. Mazur, The method of infinite repetition in pure topology. II. Stable applications. *Ann. of Math. (2)* **83** (1966), 387–401.

[19] M.W. Hirsch and B. Mazur, Smoothings of piecewise linear manifolds. *Annals of Mathematics Studies*, No. **80**. Princeton University Press, Princeton, N. J.; University of Tokyo Press, Tokyo, 1974.

[20] B. Mazur, Frobenius and the Hodge filtration. *Bull. Amer. Math. Soc.* **78** (1972), 653–667.

[21] B. Mazur, Frobenius and the Hodge filtration (estimates). *Ann. of Math.* (2) **98** (1973), 58–95.

[22] B. Mazur and W. Messing, *Universal extensions and one dimensional crystalline cohomology.* Lecture Notes in Mathematics, Vol. 370. Springer-Verlag, Berlin-New York, 1974.

[23] B. Mazur, *Eigenvalues of Frobenius acting on algebraic varieties over finite fields.* in Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974), pp. 231–261. Amer. Math. Soc., Providence, R.I., 1975.

[24] M. Artin and B. Mazur, Formal groups arising from algebraic varieties. *Ann. Sci. Ecole Norm. Sup.* (4) 10 (1977), no. 1, 87–131.

[25] M. Artin and B. Mazur, Homotopy of varieties in the etale topology. in *1967 Proc. Conf. Local Fields (Driebergen, 1966)* pp. 1–15 Springer, Berlin.

[26] B. Mazur and L. Roberts, Local Euler characteristics. *Invent. Math.* **9** (1969/70), 201–234.

[27] B. Mazur, Finite flat structures. in *1970 Applications of Categorical Algebra* (Proc. Sympos. Pure Math., Vol. XVII, New York, 1968) pp. 219–225 Amer. Math. Soc., Providence, R.I.

[28] M. Artin and B. Mazur, *Etale homotopy.* Reprint of the 1969 original. Lecture Notes in Mathematics, 100. Springer-Verlag, Berlin, 1986.

[29] B. Mazur, Local flat duality. *Amer. J. Math.* **92** (1970), 343–361.

[30] B. Mazur. *Remarks on the Alexander Polynomial*. Unpublished. Available at https://people.math.harvard.edu/ mazur/papers/alexander_polynomial.pdf.

[31] B. Mazur, Notes on étale cohomology of number fields. *Ann. Sci. École Norm. Sup. (4)* **6** (1973), 521–552 (1974).

[32] B. Mazur and J. Vélu, Courbes de Weil de conducteur 26. *C. R. Acad. Sci. Paris Sér. A-B* **275** (1972), A743–A745.

[33] B. Mazur and J. Tate, Points of order 13 on elliptic curves. *Invent. Math.* **22** (1973/74), 41–49.

[34] B. Mazur and J.-P. Serre, Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg). *Séminaire Bourbaki* (1974/1975), Exp. No. 469, pp. 238–255. Lecture Notes in Math., Vol. 514, Springer, Berlin, 1976.

[35] B. Mazur, Rational points on modular curves. *Modular functions of one variable, V* (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107–148. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977.

[36] B. Mazur, Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* No. **47** (1977), 33–186 (1978).

[37] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), no. 2, 129–162.

[38] S. Kamienny and B. Mazur, Rational torsion of prime order in elliptic curves over number fields. Columbia University Number Theory Seminar (New York, 1992). *Astérisque* No. **228** (1995), 3, 81–100.

[39] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985.

[40] B. Mazur, Courbes elliptiques et symboles modulaires. in *Séminaire Bourbaki, 24ème année (1971/1972),* Exp. No. **414**, pp. 277–294. Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973.

[41] B. Mazur, Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* **18** (1972), 183–266.

[42] B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves. *Invent. Math.* **25** (1974), 1–61.

[43] B. Mazur, p-adic analytic number theory of elliptic curves and Abelian varieties over $\mathbb{Q}$. *Proceedings of the International Congress of Mathematicians* (Vancouver, B. C., 1974), Vol. 1, pp. 369–377.

[44] B. Mazur, On the arithmetic of special values of L-functions. *Invent. Math.* **55** (1979), no. 3, 207–240.

[45] B. Mazur and A. Wiles, Analogies between function fields and number fields. *Amer. J. Math.* **105** (1983), no. 2, 507–521.

[46] B. Mazur and J. Tate, Canonical height pairings via biextensions. *Arithmetic and geometry,* Vol. I, 195–237, Progr. Math., 35, Birkhäuser Boston, Boston, MA, 1983.

[47] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$. *Invent. Math.* **76** (1984), no. 2, 179–330.

[48] B. Mazur, Modular curves and arithmetic. *Proceedings of the International Congress of Mathematicians,* Vol. 1, 2 (Warsaw, 1983), 185–211, PWN, Warsaw, 1984.

[49] B. Mazur, Arithmetic on curves. *Bull. Amer. Math. Soc.* (N.S.) **14** (1986), no. 2, 207–259.

[50] B. Mazur, J. Tate, and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.* **84** (1986), no. 1, 1–48.

[51] B. Mazur and A. Wiles, On p-adic analytic families of Galois representations. *Compositio Math.* **59** (1986), no. 2, 231–264.

[52] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type". *Duke Math. J.* **54** (1987), no. 2, 711–750.

[53] B. Mazur, Deforming Galois representations. in *Galois groups over* $\mathbb{Q}$, 385–437, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.

[54] N. Boston and B. Mazur, Explicit universal deformations of Galois representations. in *Algebraic number theory*, 1–21, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.

[55] B. Mazur, Two-dimensional p-adic Galois representations unramified away from p. *Compositio Math.* **74** (1990), no. 2, 115–133.

[56] B. Mazur and J. Tilouine, Représentations galoisiennes, différentielles de Kähler et "conjectures principales". *Inst. Hautes Etudes Sci. Publ. Math.* **71** (1990), 65–103.

[57] F. Gouvêa and B. Mazur, The square-free sieve and the rank of elliptic curves. *J. Amer. Math. Soc.* **4** (1991), no. 1, 1–23.

[58] B. Mazur and J. Tate, The p-adic sigma function. *Duke Math. J.* **62** (1991), no. 3, 663–688.

[59] B. Mazur, Number theory as gadfly. *Amer. Math. Monthly* **98** (1991), no. 7, 593–610.

[60] B. Mazur and K. Ribet, Two-dimensional representations in the arithmetic of modular curves. in *Courbes modulaires et courbes de Shimura* (Orsay, 1987/1988). Astérisque No. 196-197 (1991), 6, 215–255 (1992).

[61] F. Gouvêa and B. Mazur, Families of modular eigenforms. *Math. Comp.* **58** (1992), no. 198, 793–805.

[62] B. Mazur, The topology of rational points. *Experiment. Math.* **1** (1992), no. 1, 35–45.

[63] B. Mazur, On the passage from local to global in number theory. *Bull. Amer. Math. Soc. (N.S.)* **29** (1993), no. 1, 14–50.

[64] F.Q. Gouvêa and B. Mazur, On the characteristic power series of the U operator. *Ann. Inst. Fourier (Grenoble)* **43** (1993), no. 2, 301–312.

[65] E.M. Friedlander and B. Mazur, Filtrations on the homology of algebraic varieties. With an appendix by Daniel Quillen. *Mem. Amer. Math. Soc.* **110** (1994), no. 529.

[66] B. Mazur, Questions of decidability and undecidability in number theory. *J. Symbolic Logic* **59** (1994), no. 2, 353–371.

[67] B. Mazur, On monodromy invariants occurring in global arithmetic, and Fontaine's theory. in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture* (Boston, MA, 1991), 1–20, Contemp. Math., 165, Amer. Math. Soc., Providence, RI, 1994.

[68] B. Mazur, Speculations about the topology of rational points: an update. Columbia University Number Theory Seminar (New York, 1992). *Astérisque* No. **228** (1995), 4, 165–182.

[69] F.Q. Gouvêa and B. Mazur, Searching for p-adic eigenfunctions. *Math. Res. Lett.* **2** (1995), no. 5, 515–536.

[70] L. Caporaso, J. Harris, and B. Mazur, How many rational points can a curve have? The moduli space of curves (Texel Island, 1994), 13–31, Progr. Math., **129**, Birkhäuser Boston, Boston, MA, 1995.

[71] J.-M. Fontaine and B. Mazur, Geometric Galois representations. in *Elliptic curves, modular forms, & Fermat's last theorem*, (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[72] L. Caporaso,J. Harris, and B. Mazur, Uniformity of rational points. *J. Amer. Math. Soc.* **10** (1997), no. 1, 1–35.

[73] B. Mazur, An "infinite fern" in the universal deformation space of Galois representations. *Journées Arithmétiques* (Barcelona, 1995). Collect. Math. **48** (1997), no. 1-2, 151–193.

[74] D. Eisenbud and B. Mazur, Evolutions, symbolic squares, and Fitting ideals. *J. Reine Angew. Math.* **488** (1997), 189–201.

[75] B. Mazur, An introduction to the deformation theory of Galois representations. in *Modular forms and Fermat's last theorem* (Boston, MA, 1995), 243–311, Springer, New York, 1997.

[76] F.. Gouvêa and B. Mazur, On the density of modular representations. in *Computational perspectives on number theory* (Chicago, IL, 1995), 127–142, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.

[77] J. Harris, B. Mazur, and R. Pandharipande, Hypersurfaces of low degree. *Duke Math. J.* **95** (1998), no. 1, 125–160.

[78] R. Coleman and B. Mazur, The eigencurve. in *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, 1–113, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[79] B. Mazur, Open problems regarding rational points on curves and varieties. in *Galois representations in arithmetic algebraic geometry*, (Durham, 1996), 239–265, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[80] B. Mazur, Open problems in number theory. in *Current developments in mathematics, 1997* (Cambridge, MA), 199–203, Int. Press, Boston, MA, 1999.

[81] B. Mazur, Visualizing elements of order three in the Shafarevich-Tate group. in *Sir Michael Atiyah: a great mathematician of the twentieth century*. Asian J. Math. 3 (1999), no. 1, 221–232.

[82] D. Kazhdan, B. Mazur, and C.-G. Schmidt, Relative modular symbols and Rankin-Selberg convolutions. *J. Reine Angew. Math.* **519** (2000), 97–141.

[83] B. Mazur, Questions about powers of numbers. *Notices Amer. Math. Soc.* **47** (2000), no. 2, 195–202.

[84] B. Mazur, The theme of p-adic variation. in *Mathematics: frontiers and perspectives,* 433–459, Amer. Math. Soc., Providence, RI, 2000.

[85] J. E. Cremona and B. Mazur, Visualizing elements in the Shafarevich-Tate group. *Experiment. Math.* **9** (2000), no. 1, 13–28.

[86] B. Mazur, Abelian varieties and the Mordell-Lang conjecture. in *Model theory, algebra, and geometry,* 199–227, Math. Sci. Res. Inst. Publ., **39**, Cambridge Univ. Press, Cambridge, 2000.

[87] F. La Nave and B. Mazur, Reading Bombelli. *Math. Intelligencer* **24** (2002), no. 1, 12–21.

[88] B. Mazur and K. Rubin, Elliptic curves and class field theory. *Proceedings of the International Congress of Mathematicians,* Vol. II (Beijing, 2002), 185–195, Higher Ed. Press, Beijing, 2002.

[89] B. Mazur, *Imagining numbers. Particularly the square root of minus fifteen*. Farrar, Straus and Giroux, New York, 2003.

[90] B. Mazur and K. Rubin, Studying the growth of Mordell-Weil. in *Kazuya Kato's fiftieth birthday.* Doc. Math. 2003, Extra Vol., 585–607.

[91] T. Graber, J. Harris, B. Mazur, and J. Starr, Jumps in Mordell-Weil rank and arithmetic surjectivity. in *Arithmetic of higher-dimensional algebraic varieties* (Palo Alto, CA, 2002), 141–147, Progr. Math., 226, Birkhäuser Boston, Boston, MA, 2004.

[92] B. Mazur and K. Rubin, Kolyvagin systems. *Mem. Amer. Math. Soc.* **168** (2004)

[93] B. Mazur, Perturbations, deformations, and variations (and "near-misses") in geometry, physics, and number theory. *Bull. Amer. Math. Soc. (N.S.)* **41** (2004), no. 3, 307–336.

[94] B. Mazur and K. Rubin, Pairings in the arithmetic of elliptic curves. in *Modular curves and abelian varieties*, 151–163, Progr. Math., 224, Birkhäuser, Basel, 2004.

[95] T. Graber, J. Harris, B. Mazur, and J. Starr, Arithmetic questions related to rationally connected varieties. in *The legacy of Niels Henrik Abel*, 531–542, Springer, Berlin, 2004.

[96] B. Mazur and K. Rubin, Introduction to Kolyvagin systems. in *Stark's conjectures: recent work and new directions*, 207–221, Contemp. Math., 358, Amer. Math. Soc., Providence, RI, 2004.

[97] B. Mazur, What is … a motive? *Notices Amer. Math. Soc.* **51** (2004), no. 10, 1214–1216.

[98] B. Mazur, and K. Rubin, Organizing the arithmetic of elliptic curves. *Adv. Math.* **198** (2005), no. 2, 504–546.

[99] B. Mazur and K. Rubin, Finding large Selmer groups. *J. Differential Geom.* **70** (2005), no. 1, 1–22.

[100] T. Graber, J. Harris, B. Mazur, and J. Starr, Rational connectivity and sections of families over curves. *Ann. Sci. Ecole Norm. Sup.* (4) **38** (2005), no. 5, 671–692.

[101] B. Mazur, W. Stein, and J. Tate, Computation of p-adic heights and log convergence. *Doc. Math.* 2006, Extra Vol., 577–614.

[102] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, Average ranks of elliptic curves: tension between data and conjecture. *Bull. Amer. Math. Soc.* (N.S.) **44** (2007), no. 2, 233–254.

[103] B. Mazur, K. Rubin, K, and A. Silverberg, Twisting commutative algebraic groups. *J. Algebra* **314** (2007), no. 1, 419–438.

[104] B. Mazur and K. Rubin, Finding large Selmer rank via an arithmetic theory of local constants. *Ann. of Math.* (2) **166** (2007), no. 2, 579–612.

[105] B. Mazur, Finding meaning in error terms. *Bull. Amer. Math. Soc. (N.S.)* **45** (2008), no. 2, 185–228.

[106] B. Mazur and K. Rubin, Growth of Selmer rank in nonabelian extensions of number fields. *Duke Math. J.* **143** (2008), no. 3, 437–461.

[107] B. Mazur, When is one thing equal to some other thing? in *Proof and other dilemmas*, 221–241, MAA Spectrum, Math. Assoc. America, Washington, DC, 2008.

[108] F. Calegari and B. Mazur, Nearly ordinary Galois deformations over arbitrary number fields. *J. Inst. Math. Jussieu* **8** (2009), no. 1, 99–177.

[109] B. Mazur and K. Rubin, Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.* **181** (2010), no. 3, 541–575.

[110] B. Mazur and K. Rubin, Refined class number formulas and Kolyvagin systems. *Compos. Math.* **147** (2011), no. 1, 56–74.

[111] B. Mazur, How can we construct abelian Galois extensions of basic number fields? *Bull. Amer. Math. Soc. (N.S.)* **48** (2011), no. 2, 155–209.

[112] B. Mazur, About Hermann Weyl's "Ramifications, old and new, of the eigenvalue problem", *Bull. Amer. Math. Soc. (N.S.)* **49** (2012), no. 2, 325–326.

[113] B. Mazur, Visions, dreams, and mathematics. in *Circles disturbed*, 183–210, Princeton Univ. Press, Princeton, NJ, 2012.

[114] Z. Klagsbrun, B. Mazur, K. Rubin, Disparity in Selmer ranks of quadratic twists of elliptic curves. *Ann. of Math. (2)* **178** (2013), no. 1, 287–320.

[115] J.B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin, The spin of prime ideals. *Invent. Math.* **193** (2013), no. 3, 697–749.

[116] B. Mazur, Is it plausible? *Math. Intelligencer* **36** (2014), no. 1, 24–33.

[117] Z. Klagsbrun, B. Mazur, and K. Rubin, A Markov model for Selmer ranks in families of twists. *Compos. Math.* **150** (2014), no. 7, 1077–1106.

[118] B. Mazur and K. Rubin, Selmer companion curves. *Trans. Amer. Math. Soc.* **367** (2015), no. 1, 401–421.

[119] B. Mazur and K. Rubin, Controlling Selmer groups in the higher core rank case. *J. Théor. Nombres Bordeaux* **28** (2016), no. 1, 145–183.

[120] B. Mazur and K. Rubin, Refined class number formulas for G_m, *J. Théor. Nombres Bordeaux* **28** (2016), no. 1, 185–211.

[121] B. Mazur, W. Stein, *Prime numbers and the Riemann hypothesis*. Cambridge University Press, Cambridge, 2016. xi+142 pp.

[122] M. Derickx, B. Mazur, and S. Kamienny, Rational families of 17-torsion points of elliptic curves over number fields. in *Number theory related to modular curves—Momose memorial volume*, 81–104, Contemp. Math., 701, Amer. Math. Soc., 2018.

[123] B. Mazur and K. Rubin, Diophantine stability. *Amer. J. Math.* **140** (2018), no. 3, 571–616.

[124] B. Mazur, Grand unity. *ICCM Not.* **7** (2019), no. 1, 76.

[125] B. Mazur and K. Rubin, Big fields that are not large. *Proc. Amer. Math. Soc.* Ser. B **7** (2020), 159–169.

[126] B. Mazur, Math in the time of plague. *Math. Intelligencer* **42** (2020), no. 4, 1–6.

[127] J. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, and J. Vonk, Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math.* (2) **189** (2019), no. 3, 885–944.

[128] Y. Bilu, P. Parent, and M. Rebolledo, Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier* (Grenoble) **63** (2013), no. 3, 957–984.

[129] M. Harris and A. Venkatesh, Derived Hecke algebra for weight one forms. *Exp. Math.* **28** (2019), no. 3, 342–361.

[130] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.* **109** (1992), no. 2, 221–229.

[131] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms.* Cohomologies p-adiques et applications arithmétiques. III. *Astérisque* No. **295** (2004), ix, 117–290.

[132] N.M. Katz, Slope filtration of F-crystals. *Journées de Géométrie Algébrique de Rennes* Vol. I, pp. 113–163, *Astérisque*, **63**, Soc. Math. France, Paris, 1979.

[133] M.A. Kenku, Rational torsion points on elliptic curves defined over quadratic fields. *J. Nigerian Math. Soc.* **2** (1983), 1–16.

[134] M.A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.* **109** (1988), 125–149.

[135] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124** (1996), no. 1–3, 437–449.

[136] F. Momose, Rational points on the modular curves $X_{\mathrm{split}}(p)$. *Compositio Math.* **52** (1984), no. 1, 115–137.

[137] F. Momose, Rational points on the modular curves $X_0^+(p^r)$. *J. Fac. Sci. Univ. Tokyo* Sect. IA Math. **33** (1986), no. 3, 441–466.

[138] M. Morishita, *Knots and primes. An introduction to arithmetic topology.* Universitext. Springer, London, 2012. 191 pp.

[139] A.P. Ogg, Rational points of finite order on elliptic curves. *Invent. Math.* **12** (1971), 105–111.

[140] Oliver Ralfe, *Barry Mazur and the infinite cheese of knowledge*, Sheepstreet films.

[141] K.A. Ribet, On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.* **100** (1990), no. 2, 431–476.

[142] N. Schappacher and R. Schoof, Beppo Levi and the arithmetic of elliptic curves. *Math. Intelligencer* **18** (1996), no. 1, 57–69.

[143] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}\bar{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.* **54** (1987), no. 1, 179–230.

[144] C. Skinner and E. Urban, The Iwasawa main conjectures for GL_2 *Invent. Math.* **195** (2014), no. 1, 1–277.

[145] J. Teitelbaum, Values of p-adic L-functions and a p-adic Poisson kernel. *Invent. Math.* **101** (1990), no. 2, 395–410.

[146] A. Venkatesh, Primes and Knots, *Public Lecture, IAS, Princeton*, video online at https://www.youtube.com/watch?v=jvoYgNYKyk0

[147] A. Wiles, The Iwasawa conjecture for totally real fields. *Ann. of Math. (2)* **131** (1990), no. 3, 493–540.

[148] A. Wiles, Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* (2) **141** (1995), no. 3, 443–551.

Henri Darmon

McGill University, Montreal, Canada, henri.darmon@mcgill.ca